Зміст

Перелік умовних позначень, символів, одиниць і термінів ……..….. 9

Вступ ……..….. 20

Розділ 1. Законодавча та нормативно-правова база України в галузі інформаційної та /або кібербезпеки ……..…… 22
Закон України «Про освіту». Стаття 42. Академічна доброчесність ... 22
1.1. Закон України «Про інформацію» ……... 26
1.2. Закон України «Про науково-технічну інформацію» ……..... 30
1.3. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» …..……..... 35
1.4. Закон України «Про основні засади забезпечення кібербезпеки України» …… 39
1.5. Закон України «Про державну таємницю» ……. 46
1.6. Закон України «Про захист персональних даних» ……. 59
1.7. Постанова КМУ від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» …. 70
1.8. ДСТУ 3396.0,1,2-97 ……... 72
1.9. ДСТУ ISO/IEC 15408-1:2017 ……. 73
1.10. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» ……... 73
1.11. НД ТЗІ 2.5-004-99. «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» …….. 74
1.12. Закон України «Про доступ до публічної інформації» ……. 74
1.13. Загрози, яким підлягає інформація …….. 82
1.14. Стратегії реалізації загроз ..…….. 82
1.15. Основні міри протидії загрозам безпеці, принципи побудови систем захисту, основні механізми захисту …….. 83
1.16. Перелік основних задач, які повинні вирішуватися системою комп'ютерної безпеки …….. 84
1.17. Основні принципи побудови систем захисту інформаційно-комунікаційних систем (ІКС) …….. 85

Розділ 2. Міжнародні стандарти в галузі інформаційної та /або кібербезпеки …… 89
2.1. Регламенти ЄС в галузі кібербезпеки: Регламент Європейського Парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року «Про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій» ……... 89
2.2. ДСТУ ISO 27001, ISO 27002, ISO 27003 ……..…. 95
2.3. ISO/IEC 15408- 2, ISO/IEC 15408-3 …… 103
2.4. Стек протоколів ДСТУ ISO/IEC 27000 …….. 108

Розділ 3. Інструментальні та прикладні застосунки в інформаційній та/або кібербезпеці …….. 126
3.1. Мережева модель OSI …….…… 126
3.2. Основні протоколи стеку TCP/IP …… 130
3.3. Віртуалізація (принципи, гіпервізори) ……... 138
3.4. Архітектура комп'ютерів …… 146

Розділ 4. Методи і засоби обробки інформації ……..……. 148
4.1. Економне кодування. Префіксний код та його дерево. Алгоритм Шеннона-Фано. Алгоритм Хаффмана. Основні методи економного кодування без втрат послідовної дискретної інформації ……. 148
4.2. Принципи завадостійкого кодування. Основні характеристики завадостійких кодів. Класифікація завадостійких кодів. Математичний опис процесу кодування і декодування …….. 160
4.3. Блочні лінійні коди. Коректуючи властивості блочних кодів. Коди з перевіркою на парність. Коди Хеммінга ……. 167
4.4. Циклічні коди. Засоби опису циклічних кодів. Властивості циклічних кодів по виявленню помилок. Укорочені циклічні коди. Коди Боуза-Чоудхурі-Хоквінгема. Коди Ріда-Соломона. Код Файра …..... 173

Розділ 5. Операційні системи ……..…. 182
5.1 Архітектура операційних систем …..……..… 182
5.2. Процеси і потоки в операційних системах …….……. 187
5.3. Керування пам'яттю в операційних системах ……. 196
5.4. Файлові системи ……. 202
5.5. Захисні механізми операційних систем (Unix, Windows Server 2022, Windows 10/11) ……... 204

Розділ 6. Моделі безпеки в інформаційній та/або кібербезпеці ……..… 262
6.1. ДСТУ ISO/IEC 15408 ……..... 262
6.2. Модель порушника ……..…. 275
6.3. Модель загроз ……..……..……. 276
6.4. Модель вразливостей ……..…… 283

Розділ 7. Захист інформації, що обробляється та зберігається в інформаційно-телекомунікаційних системах (ІКС) ……..... 293
7.1. Процедури ідентифікації, автентифікації, авторизації користувачів ……. 293
7.2. Захист ресурсів і процесів в інформаційно-телекомунікаційних системах на основі моделей безпеки (кінцевих автоматів, управління потоками, Bell-LaPadula, Biba, Clark-Wilson, та інші) ……..…… 302
7.3. Резервування інформації та компонентів інформаційно-телекомунікаційних системах ……. 310

Розділ 8. Програмні та програмно-апаратні комплекси засобів захисту інформації (ЗЗІ) …… 316
8.1. Антивіруси …… 316
8.2. Міжмережеві екрани …… 318
8.3. IDS, IPS …… 325
8.4. Системи контролю та управління доступом у мережі (Active Directory, ACL) …… 331
8.5. Системи контролю та управління фізичним доступом (СКУД) …… 336

Розділ 9. Відновлення функціонування інформаційно-комунікаційних систем (ІКС) після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження …… 343
9.1. Організаційно-технічні заходи відновлення функціонування ІКС … 343
9.2. Журнал аудиту подій …… 346
9.3. Політики резервного копіювання даних …… 352

Розділ 10. Моніторинг процесів функціонування інформаційно-комунікаційних систем (ІКС) …… 358
10.1. Джерела інформації про події та типи подій, що аналізуються в системах моніторингу …… 358
10.2. Система візуалізації та управління подіями (SIEM) …… 359
10.3. Аналіз подій SIEM …… 363

Розділ 11. Механізми безпеки комп'ютерних мереж …… 367
11.1. Віртуальні приватні мережі (VPN) …… 367
11.2. Протоколи автентифікації RADIUS …… 371
11.3. Протоколи SSL/TLS …… 378

Розділ 12. Проектування, створення, супровід комплексних систем захисту інформації (КСЗІ) …… 398
12.1. Дослідження середовищ функціонування ІС – середовища користувачів, обчислювальної системи, фізичного середовища, інформаційного середовища та побудова моделі загроз …… 398
12.2. Проведення аудиту інформаційної безпеки (ІБ) та визначення її рівня на основі звіту з аудиту ризиків ІБ …… 405
12.3. Вибір методів та засобів забезпечення необхідного рівня ІБ …… 412

Розділ 13. Моделі загроз та моделі порушника …… 417
13.1. Загальні визначення й поняття моделі загроз та моделі порушника . 417
13.2. Загрози цілісності …… 429
13.3. Загрози доступності …… 431
13.4. Загрози конфіденційності …… 433
13.5. Загрози автентичності …… 435
13.6. Загрози через технічні канали …… 447
13.7. Загрози через соціальну інженерію …… 453

Розділ 14. Оцінка захищеності інформації в інформаційно-телекомунікаційних системах (ІКС) ……..……. 456
14.1. Оцінка захищеності інформації в інформаційно-телекомунікаційних системах згідно НД ТЗІ 2.5-004-99. «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» …. 456
14.2. Концептуальна схема оцінки безпеки інформації ……..…….. 466
14.3. Кількісна та якісна оцінки безпеки інформації ……..…….. 470

Розділ 15. Управління інформаційною та/або кібербезпекою 477
15.1. Управління кіберінцидентами: Поняття кіберінцидента/кібератаки. Розслідування кіберінцидентів/кібератак ……..….. 477
15.2. Управління ризиками в інформаційній та/або кібербезпеці: Загальна концепція управління ризиками ІБ. ISO/IEC 27005:2018, IEC 31010:2019, NIST SP 800-39, NIST SP 800-37, NIST SP 800-30, NIST SP 800-137 (Ризики інформаційної безпеки. Аналіз та оцінка ризику. Прийняття ризику. Зменшення ризику. Страхування (перекладання) ризику). Системи класу Incident Response Platform ……..……. 484

Розділ 16. Аудит інформаційної та/або кібербезпеки ……..…… 517
16.1. Етапи проведення аудиту ……..……. 517
16.2. Аудит на основі аналізу ризиків …… 523
16.3. Аудит на основі стандартів інформаційної безпеки (ІБ) ……. 526
16.4. Аудит на основі експертних досліджень інформаційних систем (ІС). 528
16.5. Забезпечення безперервності бізнес-процесів: Поняття бізнес-процесу. Модель бізнес-процесу …… 528
16.6. Розробка політик інформаційної безпеки під час забезпечення бізнес-процесів ……. 532
16.7. Дотримання політик інформаційної безпеки під час забезпечення бізнес-процесів …… 547

Розділ 17. Симетричні криптосистеми ……... 551
17.1. Модель симетричної криптосистеми……. 551
17.2. Класичні методи шифрування: Шифр Цезаря, Вернама. Квадрат Полібія. Шифр гамування ……... 553
17.3. Блокові шифри: DES. ДСТУ ГОСТ 28147:2009. AES. Калина (ДСТУ 7624:2014) (режими роботи, довжина ключів, довжина блоку вхідного тексту, кількість раундів, крипостійкість згідно з ДСТУ ISO/IEC 10116:2019) ……..…….. 558
17.4. Потокові шифри: RC4, STRUMOK. (ДСТУ 8845:2019) (довжина ключів, криптостійкість) ……..……. 585

Розділ 18. Несиметрична (асиметрична, з відкритим ключем) криптографія 601
18.1. Модель асиметричної криптосистеми 601
18.2. Шифр RSA 605
18.3. Алгоритм Ель-Гамаля (EG) 609
18.4. Генерація спільних секретів Діффі-Хеллмана (DH) 610
18.5. Електронний цифровий підпис DSA 611
18.6. Криптографія на еліптичних кривих 613
18.7. Електронний цифровий підпис згідно ДСТУ 4145-2002 615
18.8. EC-DSA згідно ISO/IEC 15946-2 618

Розділ 19. Криптографічні протоколи 620
19.1. Протоколи захисту мережевого трафіку IPSec 620
19.2. Протоколи безпечної передачі даних прикладного рівня: https 633

Розділ 20. Цифрова стеганографія 636
20.1. Поняття цифрової стеганографії 636
20.2. Модель стеганосистеми та класифікація методів стеганографічного захисту 637
20.3. Основні вимоги до стеганосистеми 646
20.3. Відкриті, напівзакриті, закриті стеганосистеми 648
20.4. Поняття ЦВЗ, класифікація 649
20.5. Метод модифікації найменшого значущого біта та інші методи приховання даних у зображенні, відео та аудіо 652
20.6. Атаки на стеганосистеми 659

Розділ 21. Технічний захист інформації 672
21.1. Технічні канали витоку інформації: Акустичний (мовний) канал витоку інформації. Електричний канал витоку інформації. Електромагнітний канал витоку інформації. Методи прослуховування мобільного зв'язку. Оптичний та оптоелектронний канал витоку інформації. Параметричний канал витоку інформації 672
21.2.Методи та засоби технічного захисту інформації: Пасивні та активні методи і засоби захисту інформації від витоку технічними каналами. Захист від прослуховування мобільного зв'язку. Система контролю та управління доступом (СКУД). Системи відеоспостереження. Пожежна сигналізація 687

Додаток А. Тексти Законів та стандартів України щодо забезпечення кібербезпеки 712
А.1. Закон України «Про інформацію» 713
А.2. Закон України «Про науково-технічну інформацію» 725
А.3. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» 735

А.4. Закон України «Про основні засади забезпечення кібербезпеки України» ……..…….. 742
А.5. Закон України «Про державну таємницю» ……. 759
А.6. Закон України «Про захист персональних даних» …… 789
А.7. Постанова КМУ від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури ……..…... 804
А.8. ДСТУ 3396.0,1,2-97 ……... 823
А.9. ДСТУ ISO/IEC 15408-1:2017 ……..……. 839
А.10. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» …… 840
А.11. НД ТЗІ 2.5-004-99. «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» ……. 849
А.12. Закон України «Про доступ до публічної інформації» …….. 889

Додаток Б. Розширена нормативно-правова база щодо захисту інформації в Україні та стандарти у галузі захисту інформації …..…. 903
Б.1 Нормативно-правова база щодо захисту інформації в Україні ….…… 903
Б.2. Статі Кримінального кодексу, які передбачують покарання за розголошення таємниці ……... 906
Б.3. Нормативно-правові акти, що регламентують діяльність Держспецзв'язку за сферами ……... 907
Б.4. Стандарти у галузі захисту інформації ……... 916

Список використаних джерел …….. 930
Перелік законів, нормативних актів, стандартів та специфікацій ….. 946

Розділ 1. Законодавча та нормативно-правова база України в галузі інформаційної та /або кібербезпеки

Закон України «Про освіту». Стаття 42. Академічна доброчесність.

1.1. Закон України «Про інформацію».

1.2. Закон України «Про науково-технічну інформацію».

1.3. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».

1.4. Закон України «Про основні засади забезпечення кібербезпеки України».

1.5. Закон України «Про державну таємницю».

1.6. Закон України «Про захист персональних даних».

1.7. Постанова КМУ від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури.

1.8. ДСТУ 3396.0,1,2-97

1.9. ДСТУ ISO/IEC 15408-1:2017

1.10. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу»

1.11. НД ТЗІ 2.5-004-99. «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»

1.12. Закон України «Про доступ до публічної інформації».

1.13. Загрози, яким підлягає інформація.

1.14. Стратегії реалізації загроз.

1.15. Основні міри протидії загрозам безпеці, принципи побудови систем захисту, основні механізми захисту.

1.16. Перелік основних задач, які повинні вирішуватися системою комп'ютерної безпеки.

1.17. Основні принципи побудови систем захисту інформаційно-комунікаційних систем (ІКС).

Закон України «Про освіту»

Стаття 42. Академічна доброчесність

1. **Академічна доброчесність** – це сукупність етичних принципів та визначених законом правил, якими мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової (творчої) діяльності з метою забезпечення довіри до результатів навчання та/або наукових (творчих) досягнень.

2. **Дотримання академічної доброчесності педагогічними, науково-педагогічними та науковими працівниками передбачає:**

– посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;

– дотримання норм законодавства про авторське право і суміжні права;

– надання достовірної інформації про методики і результати досліджень, джерела використаної інформації та власну педагогічну (науково-педагогічну, творчу) діяльність;

– контроль за дотриманням академічної доброчесності здобувачами освіти;

– об'єктивне оцінювання результатів навчання.

3. **Дотримання академічної доброчесності здобувачами освіти передбачає**:

– самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей);

– посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;

– дотримання норм законодавства про авторське право і суміжні права;

– надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

4. **Порушенням академічної доброчесності вважається**:

– **академічний плагіат –** оприлюднення (частково або повністю) наукових (творчих) результатів, отриманих іншими особами, як результатів власного дослідження (творчості) та/або відтворення опублікованих текстів (оприлюднених творів мистецтва) інших авторів без зазначення авторства;

– **самоплагіат** – оприлюднення (частково або повністю) власних раніше опублікованих наукових результатів як нових наукових результатів;

– **фабрикація –** вигадування даних чи фактів, що використовуються в освітньому процесі або наукових дослідженнях;

– **фальсифікація –** свідома зміна чи модифікація вже наявних даних, що стосуються освітнього процесу чи наукових досліджень;

– **списування –** виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання, зокрема під час оцінювання результатів навчання;

– **обман –** надання завідомо неправдивої інформації щодо власної освітньої (наукової, творчої) діяльності чи організації освітнього процесу; формами обману є, зокрема, академічний плагіат, самоплагіат, фабрикація, фальсифікація та списування;

– **хабарництво –** надання (отримання) учасником освітнього процесу чи пропозиція щодо надання (отримання) коштів, майна, послуг, пільг чи будь-яких інших благ матеріального або нематеріального характеру з метою отримання неправомірної переваги в освітньому процесі;

– **необ'єктивне оцінювання –** свідоме завищення або заниження оцінки результатів навчання здобувачів освіти;

– надання здобувачам освіти під час проходження ними оцінювання результатів навчання допомоги чи створення перешкод, не передбачених умовами та/або процедурами проходження такого оцінювання;

– вплив у будь-якій формі (прохання, умовляння, вказівка, погроза, примушування тощо) на педагогічного (науково-педагогічного) працівника з метою здійснення ним необ'єктивного оцінювання результатів навчання.

5. **За порушення академічної доброчесності педагогічні, науково-педагогічні та наукові працівники закладів освіти можуть бути притягнені до такої академічної відповідальності:**

– відмова у присудженні ступеня освітньо-наукового чи освітньо-творчого рівня чи присвоєнні вченого звання;

– позбавлення присудженого ступеня освітньо-наукового чи освітньо-творчого рівня чи присвоєного вченого звання;

– відмова в присвоєнні або позбавлення присвоєного педагогічного звання, кваліфікаційної категорії;

– позбавлення права брати участь у роботі визначених законом органів чи займати визначені законом посади.

6. **За порушення академічної доброчесності здобувачі освіти можуть бути притягнені до такої академічної відповідальності**:

– повторне проходження оцінювання (контрольна робота, іспит, залік тощо);

– повторне проходження відповідного освітнього компонента освітньої програми;

– відрахування із закладу освіти (крім осіб, які здобувають загальну середню освіту);

– позбавлення академічної стипендії;

– позбавлення наданих закладом освіти пільг з оплати навчання.

7. **Види академічної відповідальності** (у тому числі додаткові та/або деталізовані) учасників освітнього процесу за конкретні порушення академічної доброчесності визначаються спеціальними законами та/або внутрішніми положеннями закладу освіти, що мають бути затверджені (погоджені) основним колегіальним органом управління закладу освіти та погоджені з відповідними органами самоврядування здобувачів освіти в частині їхньої відповідальності.

8. **Порядок виявлення та встановлення фактів порушення академічної доброчесності** визначається уповноваженим колегіальним органом управління закладу освіти з урахуванням вимог цього Закону та спеціальних законів.

Кожна особа, стосовно якої порушено питання про порушення нею академічної доброчесності, має такі права:

– ознайомлюватися з усіма матеріалами перевірки щодо встановлення факту порушення академічної доброчесності, подавати до них зауваження;

– особисто або через представника надавати усні та письмові пояснення або відмовитися від надання будь-яких пояснень, брати участь у дослідженні доказів порушення академічної доброчесності;

– знати про дату, час і місце та бути присутньою під час розгляду питання про встановлення факту порушення академічної доброчесності та притягнення її до академічної відповідальності;

– оскаржити рішення про притягнення до академічної відповідальності до органу, уповноваженого розглядати апеляції, або до суду.

9. **Форми та види академічної відповідальності закладів освіти** визначаються спеціальними законами.

10. **За дії (бездіяльність), що цим Законом визнані порушенням академічної доброчесності, особа може бути притягнута до інших видів відповідальності з підстав та в порядку, визначених законом**.

Інформаційна безпека (англ. *Information Security*, а також – англ. *InfoSec*) – Практика запобігання несанкціонованого доступу, використання, розкриття, спотворення, зміни, дослідження, запису або знищення інформації. Це універсальне поняття застосовується незалежно від форми, яку можуть набувати дані (електронна або, наприклад, фізична). Основне завдання інформаційної безпеки – збалансований захист конфіденційності, цілісності та доступності даних, з урахуванням доцільності застосування і без будь-яких збитківпродуктивності організації. Це досягається, в основному, за допомогою багатоетапного процесу управління ризиками, який дозволяє ідентифікувати основні засоби та нематеріальні активи, джерела загроз, уразливості, потенційний ступінь впливу та можливості управління ризиками. Цей процес супроводжується оцінкою ефективності плану управління ризиками.

Комп'ютерна безпека – розділ інформаційної безпеки, що характеризує неможливість виникнення шкоди комп'ютера, що перевищує величину прийнятної шкоди для нього від усіх виявлених та вивчених джерел його відмов у певних умовах роботи та на заданому інтервалі часу. Комп'ютерна безпека – заходи безпеки для захисту обчислювальних пристроїв (комп'ютери, смартфони та інші), а також комп'ютерних мереж (приватних та публічних мереж, включаючи Інтернет). Поле діяльності системних адміністраторів охоплює всі процеси та механізми, за допомогою яких цифрове обладнання, інформаційне поле та послуги захищаються від випадкового чи несанкціонованого доступу, зміни або знищення даних, і набуває все більшого значення у зв'язку з зростаючою залежністю від комп'ютерних систем у розвиненій спільноті.

Кібербезпека – розділ інформаційної безпеки, в рамках якого вивчають процеси формування, функціонування та еволюції кібероб'єктів, для виявлення джерел кібернебезпеки, що утворюються при цьому, визначення їх характеристик, а також їх класифікацію та формування нормативних документів, виконання яких має гарантувати захист кібероб'єктів від усіх виявлених і вивчених джерел кібернебезпеки. Кібербезпека – процес використання заходів безпеки для забезпечення конфіденційності, цілісності та доступності даних. Системний адміністратор забезпечує захист активів, включаючи дані локальної мережі комп'ютерів та серверів. Крім того, під охорону беруться безпосередньо будівлі та, найголовніше, персонал. Метою забезпечення кібербезпеки є захист даних (як у процесі передачі та/або обміну так і тих, що знаходяться на зберіганні). З метою безпеки даних можуть бути застосовані і контрзаходи. Деякі

з цих заходів включають (але не обмежуються) контроль доступу, навчання персоналу, аудит та звітність, оцінку ймовірних ризиків, тестування на проникнення та вимогу авторизації.

1.1. Закон України «Про інформацію»

Цей Закон регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації, та складається з наступних розділів і статей.

Розділ I. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення термінів

Стаття 2. Основні принципи інформаційних відносин

Стаття 3. Державна інформаційна політика

Стаття 4. Суб'єкти і об'єкт інформаційних відносин

Стаття 5. Право на інформацію

Стаття 6. Гарантії права на інформацію

Стаття 7. Охорона права на інформацію

Стаття 8. Мова інформації

Стаття 9. Основні види інформаційної діяльності

Розділ II. ВИДИ ІНФОРМАЦІЇ

Стаття 10. Види інформації за змістом

Стаття 11. Інформація про фізичну особу

Стаття 12. Інформація довідково-енциклопедичного характеру

Стаття 13. Інформація про стан довкілля (екологічна інформація)

Стаття 14. Інформація про товар (роботу, послугу)

Стаття 15. Науково-технічна інформація

Стаття 16. Податкова інформація

Стаття 17. Правова інформація

Стаття 18. Статистична інформація

Стаття 19. Соціологічна інформація

Стаття 19. Критична технологічна інформація

Стаття 20. Доступ до інформації

Стаття 21. Інформація з обмеженим доступом

Розділ III. ДІЯЛЬНІСТЬ ЖУРНАЛІСТІВ, ЗАСОБІВ МАСОВОЇ ІНФОРМАЦІЇ, ЇХ ПРАЦІВНИКІВ

Стаття 22. Масова інформація та її засоби

Стаття 23. Інформаційна продукція та інформаційна послуга

Стаття 24. Заборона цензури та заборона втручання в професійну діяльність журналістів і засобів масової інформації

Стаття 25. Гарантії діяльності засобів масової інформації та журналістів

Стаття 26. Акредитація журналістів, працівників засобів масової інформації

Розділ IV. ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА ПРО ІНФОРМАЦІЮ

Стаття 27. Відповідальність за порушення законодавства про інформацію
Стаття 28. Неприпустимість зловживання правом на інформацію
Стаття 29. Поширення суспільно необхідної інформації
Стаття 30. Звільнення від відповідальності
Стаття 31. Відшкодування матеріальної та моральної шкоди

Розділ I. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення термінів

1. У цьому Законі наведені нижче терміни вживаються в такому значенні:

– документ – матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі;

– захист інформації – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї;

– інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;

– суб'єкт владних повноважень – орган державної влади, орган місцевого самоврядування, інший суб'єкт, що здійснює владні управлінські функції відповідно до законодавства, у тому числі на виконання делегованих повноважень.

Стаття 2. Основні принципи інформаційних відносин

1. Основними принципами інформаційних відносин є:

– гарантованість права на інформацію;

– відкритість, доступність інформації, свобода обміну інформацією;

– достовірність і повнота інформації;

– свобода вираження поглядів і переконань;

– правомірність одержання, використання, поширення, зберігання та захисту інформації;

– захищеність особи від втручання в її особисте та сімейне життя.

Стаття 3. Державна інформаційна політика

1. Основними напрямами державної інформаційної політики є:

– забезпечення доступу кожного до інформації;

– забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації;

– створення умов для формування в Україні інформаційного суспільства;

– забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень;

– створення інформаційних систем і мереж інформації, розвиток електронного урядування;

– постійне оновлення, збагачення та зберігання національних інформаційних ресурсів;

– забезпечення інформаційної безпеки України;

– сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору.

Стаття 4. Суб'єкти і об'єкт інформаційних відносин

1. Суб'єктами інформаційних відносин є:

– фізичні особи;

– юридичні особи;

– об'єднання громадян;

– суб'єкти владних повноважень.

2. Об'єктом інформаційних відносин є інформація.

Стаття 5. Право на інформацію

1. Кожен має право на інформацію, що передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів.

Реалізація права на інформацію не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб.

Стаття 6. Гарантії права на інформацію

1. Право на інформацію забезпечується:

– створенням механізму реалізації права на інформацію;

– створенням можливостей для вільного доступу до статистичних даних, архівних, бібліотечних і музейних фондів, інших інформаційних банків, баз даних, інформаційних ресурсів;

– обов'язком суб'єктів владних повноважень інформувати громадськість та засоби масової інформації про свою діяльність і прийняті рішення;

– обов'язком суб'єктів владних повноважень визначити спеціальні підрозділи або відповідальних осіб для забезпечення доступу запитувачів до інформації;

– здійсненням державного і громадського контролю за додержанням законодавства про інформацію;

– встановленням відповідальності за порушення законодавства про інформацію.

2. Право на інформацію може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку, з метою запобігання заворушенням чи кримінальним правопорушенням, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.

Стаття 7. Охорона права на інформацію

1. Право на інформацію охороняється законом. Держава гарантує всім суб'єктам інформаційних відносин рівні права і можливості доступу до інформації.

2. Ніхто не може обмежувати права особи у виборі форм і джерел одержання інформації, за винятком випадків, передбачених законом.

Суб'єкт інформаційних відносин може вимагати усунення будь-яких порушень його права на інформацію.

3. Забороняється вилучення і знищення друкованих видань, експонатів, інформаційних банків, документів з архівних, бібліотечних, музейних фондів, крім встановлених законом випадків або на підставі рішення суду.

4. Право на інформацію, створену в процесі діяльності фізичної чи юридичної особи, суб'єкта владних повноважень або за рахунок фізичної чи юридичної особи, Державного бюджету України, місцевого бюджету, охороняється в порядку, визначеному законом.

Стаття 9. Основні види інформаційної діяльності

1. Основними видами інформаційної діяльності є створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації.

Розділ II. ВИДИ ІНФОРМАЦІЇ

Стаття 10. Види інформації за змістом

За змістом інформація поділяється на такі види:

– інформація про фізичну особу;

– інформація довідково-енциклопедичного характеру;

– інформація про стан довкілля (екологічна інформація);

– інформація про товар (роботу, послугу);

– науково-технічна інформація;

– податкова інформація;

– правова інформація;

– статистична інформація;

– соціологічна інформація;

– критична технологічна інформація;

– інші види інформації.

Стаття 11. Інформація про фізичну особу

1. Інформація про фізичну особу (персональні дані) – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

2. Не допускаються збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини. До конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження.

Стаття 15. Науково-технічна інформація

1. Науково-технічна інформація – будь-які відомості та/або дані про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, одержані в ході науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

3. Науково-технічна інформація є відкритою за режимом доступу, якщо інше не встановлено законами України.

Стаття 19. Критична технологічна інформація

1. **Критична технологічна інформація** – дані, що обробляються (приймаються, передаються, зберігаються) в системах управління технологічними процесами об’єктів критичної інфраструктури.

2. Правовий режим критичної технологічної інформації визначається законами України та міжнародними договорами України, згода на обов’язковість яких надана Верховною Радою України.

3. Критична технологічна інформація за режимом доступу належить до інформації з обмеженим доступом та підлягає захисту згідно із законом.

Стаття 20. Доступ до інформації

1. За порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом.

2. Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом.

Стаття 21. Інформація з обмеженим доступом

1. Інформацією з обмеженим доступом є **конфіденційна, таємна та службова інформація.**

2. Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом.

Відносини, пов'язані з правовим режимом конфіденційної інформації, регулюються законом.

Розділ IV. ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА ПРО ІНФОРМАЦІЮ

Стаття 27. Відповідальність за порушення законодавства про інформацію

1. Порушення законодавства України про інформацію тягне за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність згідно із законами України.

1.2. Закон України «Про науково-технічну інформацію»

Цей Закон визначає основи державної політики в галузі науково-технічної інформації, порядок її формування і реалізації в інтересах науково-технічного, економічного і соціального прогресу країни та складається з наступних розділів і статей.

Розділ I. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення термінів

Стаття 2. Об’єкт відносин у сфері науково-технічної інформації

Стаття 3. Суб’єкти відносин у сфері науково-технічної інформації

Стаття 4. Законодавство України у сфері науково-технічної інформації

Розділ II. ПРАВОВИЙ РЕЖИМ НАУКОВО-ТЕХНІЧНОЇ ІНФОРМАЦІЇ

Стаття 5. Право на науково-технічну інформацію

Стаття 6. Права на науково-технічну інформацію

Стаття 7. Відносини між особами, яким належать права на науково-технічну інформацію, її споживачами і посередниками

Розділ III. НАЦІОНАЛЬНА СИСТЕМА НАУКОВО-ТЕХНІЧНОЇ ІНФОРМАЦІЇ

Стаття 8. Визначення та склад національної системи науково-технічної інформації

Стаття 9. Основні завдання національної системи науково-технічної інформації

Стаття 10. Інформаційні ресурси національної системи науково-технічної інформації

Стаття 11. Державна реєстрація, облік і використання результатів науково-технічної діяльності

Стаття 12. Організація надходження та використання зарубіжної науково-технічної інформації

Розділ IV. РИНОК НАУКОВО-ТЕХНІЧНОЇ ІНФОРМАЦІЇ

Стаття 13. Науково-технічна інформація як об'єкт товарних відносин

Стаття 14. Формування ринку науково-технічної інформації

Стаття 15. Умови надання інформаційної продукції та послуг

Стаття 16. Відносини виробників і споживачів науково-технічної інформації

Розділ V. ДЕРЖАВНА ПОЛІТИКА У СФЕРІ НАУКОВО-ТЕХНІЧНОЇ ІНФОРМАЦІЇ

Стаття 17. Державна підтримка науково-інформаційної діяльності

Стаття 18. Державне управління у сфері науково-технічної інформації

Стаття 19. Відповідальність за порушення законодавства України про науково-технічну інформацію

Розділ VI. МІЖНАРОДНЕ СПІВРОБІТНИЦТВО У СФЕРІ НАУКОВО-ТЕХНІЧНОЇ ІНФОРМАЦІЇ

Стаття 20. Міжнародна інформаційна діяльність

Стаття 21. Міждержавний обмін науково-технічною інформацією

Стаття 22. Діяльність іноземних фізичних та юридичних осіб в Україні у сфері науково-технічної інформації

Стаття 23. Забезпечення суверенітету України у сфері науково-технічної інформації

Метою Закону є створення в Україні правової бази для одержання та використання науково-технічної інформації.

Законом регулюються правові і економічні відносини громадян, юридичних осіб, держави, що виникають при створенні, одержанні, використанні та поширенні науково-технічної інформації, а також визначаються правові форми міжнародного співробітництва в цій галузі.

Дія Закону поширюється на підприємства, установи, організації незалежно від форм власності, а також громадян, які мають право на одержання, використання та поширення науково-технічної інформації. Дія Закону не поширюється на інформацію, що містить державну та іншу охоронювану законом таємницю.

Розділ І. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення термінів

У цьому Законі наведені нижче терміни вживаються в такому значенні:

– науково-технічна інформація – будь-які відомості та/або дані про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, одержані в ході науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;

– науково-інформаційна діяльність – це сукупність дій, спрямованих на задоволення потреб громадян, юридичних осіб і держави у науково-технічній інформації, що полягає в її збиранні, аналітично-синтетичній обробці, фіксації, зберіганні, пошуку і поширенні;

– інформаційні ресурси науково-технічної інформації – це систематизоване зібрання науково-технічної літератури і документації (книги, брошури, періодичні видання, патентна документація, нормативно-технічна документація, промислові каталоги, конструкторська документація, звітна науково-технічна документація з науково-дослідних і дослідно-конструкторських робіт, депоновані рукописи, переклади науково-технічної літератури і документації), зафіксовані на паперових чи інших носіях;

– довідково-інформаційний фонд – це сукупність упорядкованих первинних документів і довідково-пошукового апарату, призначених для задоволення інформаційних потреб;

– довідково-пошуковий апарат – це сукупність упорядкованих вторинних документів, створюваних для пошуку першоджерел;

– інформаційні ресурси спільного користування – це сукупність інформаційних ресурсів державних органів науково-технічної інформації, наукових, науково-технічних бібліотек, а також комерційних центрів, фірм, організацій, які займаються науково-технічною діяльністю і з власниками яких укладено договори про їх спільне використання;

– аналітично-синтетична обробка науково-технічної інформації – це процес обробки інформації шляхом аналізу і синтезу змісту документів з метою одержання необхідних відомостей, а також шляхом їх класифікації, оцінки, співставлення і узагальнення;

– інформаційний ринок – це система економічних, організаційних і правових відносин щодо продажу і купівлі інформаційних ресурсів, технологій, продукції та послуг.

Стаття 2. Об’єкт відносин у сфері науково-технічної інформації

Об’єктом відносин у сфері науково-технічної інформації є вітчизняна і зарубіжна науково-технічна інформація.

Стаття 3. Суб’єкти відносин у сфері науково-технічної інформації

1. Суб’єктами відносин, що регулюються цим Законом, є державні органи, органи місцевого і регіонального самоврядування, юридичні особи та громадяни України, міжнародні організації, іноземні юридичні особи і громадяни та особи без громадянства.

2. Фізичні та юридичні особи у сфері дії цього Закону виступають як творці і накопичувачі науково-технічної інформації, власники, виробники, зберігачі і споживачі інформаційної продукції та послуг, а також як посередники у сфері науково-інформаційної діяльності.

Розділ ІІ. ПРАВОВИЙ РЕЖИМ НАУКОВО-ТЕХНІЧНОЇ ІНФОРМАЦІЇ

Стаття 5. Право на науково-технічну інформацію

1. Усі громадяни України, юридичні особи, державні органи, органи місцевого і регіонального самоврядування відповідно до Конституції України і цього Закону мають право на відкриту науково-технічну інформацію, яке передбачає можливість вільного її одержання, зберігання, використання і поширення під час здійснення наукової, науково-дослідної, виробничої, громадської та іншої діяльності, що не забороняється чинним законодавством.

2. Режим доступу до відкритої науково-технічної інформації та інформації з обмеженим доступом регулюється чинним законодавством.

Стаття 6. Права на науково-технічну інформацію

1. Права на науково-технічну інформацію охороняються відповідно до закону.

2. Підставою виникнення прав на науково-технічну інформацію є створення науково-технічної інформації своїми силами і за свій рахунок; виконання договору про створення науково-технічної інформації; виконання будь-якого договору, що містить умови переходу прав на інформацію до іншої особи.

3. Права на науково-технічну інформацію, створену кількома особами, визначаються договором, укладеним між творцями цієї інформації.

4. Права на науково-технічну інформацію, створену за рахунок коштів державного бюджету, визначаються державою шляхом прийняття загальних рішень і шляхом укладення договорів між державним органом, що здійснює фінансування, і виконавцем робіт із створення науково-технічної інформації.

Права на науково-технічну інформацію, що належали фізичним та юридичним особам, можуть переходити до держави в разі передачі її до відповідних державних банків даних, фондів або архівів на договірній основі.

Розділ ІІІ. НАЦІОНАЛЬНА СИСТЕМА НАУКОВО-ТЕХНІЧНОЇ ІНФОРМАЦІЇ

Стаття 8. Визначення та склад національної системи науково-технічної інформації

1. Основною метою національної системи науково-технічної інформації є задоволення потреб громадян, юридичних осіб і держави в науково-технічній інформації.

Національна система науково-технічної інформації – це організаційно-правова структура, за допомогою якої формується державна інформаційна політика, а також здійснюється координація робіт по створенню, користуванню, зберіганню та поширенню національних ресурсів науково-технічної інформації з урахуванням інтересів національної безпеки.

2. Національна система науково-технічної інформації складається з:

– спеціалізованих державних підприємств, установ, організацій, державних органів науково-технічної інформації, наукових і науково-технічних бібліотек, об'єднаних загальносистемними зв'язками та обов'язками;

– підприємств будь-яких організаційно-правових форм, заснованих на приватній чи колективній власності, предметом діяльності яких є інформаційне забезпечення народного господарства і громадян України.

Діяльність складових частин національної системи науково-технічної інформації здійснюється на основі договірно-обумовленого поділу праці в її збиранні, накопичуванні, переробці, зберіганні, поширенні та використанні.

Стаття 10. Інформаційні ресурси національної системи науково-технічної інформації

1. Інформаційні ресурси національної системи науково-технічної інформації становлять сукупність довідково-інформаційних фондів з необхідним довідково-пошуковим апаратом і відповідними технічними засобами зберігання, обробки і передачі, що є у володінні, розпорядженні, користуванні державних органів і служб науково-технічної інформації, наукових і науково-технічних бібліотек, комерційних центрів, підприємств, установ і організацій.

2. Інформаційні ресурси науково-технічної інформації, що є власністю держави, визнаються державними ресурсами науково-технічної інформації. Їх розподіл між різними державними органами, службами, установами та порядок обміну може регулюватися на рівні загальнодержавних та відомчих рішень через уповноважені на те структури.

Розділ V. ДЕРЖАВНА ПОЛІТИКА У СФЕРІ НАУКОВО-ТЕХНІЧНОЇ ІНФОРМАЦІЇ

Стаття 17. Державна підтримка науково-інформаційної діяльності

1. Держава з метою створення та розвитку національної системи науково-технічної інформації забезпечує:

– створення державних мереж первинного збирання, обробки та зберігання усіх видів науково-технічної інформації;

– проведення заходів для поширення і підвищення якісного рівня інформаційної продукції та послуг;

– фінансову, в тому числі валютну, підтримку надходження науково-технічної інформації до державних органів і служб науково-технічної інформації, наукових і науково-технічних бібліотек, створення їх мереж і відповідного технічного забезпечення;

– підготовку кадрів у сфері інформатики і науково-інформаційної діяльності через систему навчальних закладів вищої та середньої освіти, підвищення рівня інформаційної підготовки спеціалістів народного господарства;

– вільну конкуренцію між органами науково-технічної інформації, іншими підприємствами та організаціями усіх форм власності, які здійснюють науково-інформаційну діяльність;

– захист суб'єктів відносин в галузі науково-технічної інформації від прояву недобросовісної конкуренції та монополізму в будь-яких сферах науково-інформаційної діяльності.

2. Держава сприяє відкритості та загальнодоступності науково-технічної інформації.

Обмеження щодо доступу, поширення та використання інформації, яка є державною або іншою таємницею, що охороняється законом, визначаються законами України.

1.3. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»

Цей Закон регулює відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах (далі – система) та складається з наступних статей.

Стаття 1. Визначення термінів

Стаття 2. Об'єкти захисту в системі

Стаття 3. Суб'єкти відносин

Стаття 4. Доступ до інформації в системі

Стаття 5. Відносини між володільцем інформації та власником системи

Стаття 6. Відносини між власником системи та користувачем

Стаття 7. Відносини між власниками систем

Стаття 8. Умови обробки інформації в системі

Стаття 9. Забезпечення захисту інформації в системі

Стаття 10. Повноваження державних органів у сфері захисту інформації в системах

Стаття 11. Відповідальність за порушення законодавства про захист інформації в системах

Стаття 12. Міжнародні договори

Стаття 1. Визначення термінів

У цьому Законі наведені нижче терміни вживаються в такому значенні:

– блокування інформації в системі – дії, внаслідок яких унеможливлюється доступ до інформації в системі;

– виток інформації – результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї;

– володілець інформації – фізична або юридична особа, якій належать права на інформацію;

– власник системи – фізична або юридична особа, якій належить право власності на систему;

– доступ до інформації в системі – отримання користувачем можливості обробляти інформацію в системі;

– захист інформації в системі – діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі;

– знищення інформації в системі – дії, внаслідок яких інформація в системі зникає;

– інформаційна (автоматизована) система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;

– інформаційно-комунікаційна система – сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле;

– комплексна система захисту інформації – взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації;

– користувач інформації в системі (далі – користувач) – фізична або юридична особа, яка в установленому законодавством порядку отримала право доступу до інформації в системі;

– криптографічний захист інформації – вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

– несанкціоновані дії щодо інформації в системі – дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства;

– обробка інформації в системі – виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів;

– порушення цілісності інформації в системі – несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст;

– порядок доступу до інформації в системі – умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації;

– електронна комунікаційна система – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання та/або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;

– технічний захист інформації – вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації;

– резервна копія державних інформаційних ресурсів – копія інформації, яка міститься в державних інформаційних ресурсах, що перебувають у володінні або розпорядженні органів державної влади, органів місцевого самоврядування,

військових формувань, утворених відповідно до законів України, державних підприємств, установ та організацій, та є критичною для їх сталого функціонування, створюється, записується, обробляється або зберігається у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів з метою подальшого відновлення цієї інформації;

– резервування державних інформаційних ресурсів та систем – сукупність заходів, спрямованих на забезпечення створення резервної копії (резервних копій) та зберігання державних інформаційних ресурсів та систем з метою забезпечення безперервності їх роботи та подальшого відновлення інформації, що міститься в державних інформаційних ресурсах та системах, а також інсталяційних копій програмного забезпечення та операційних систем (та/або їх образів), в яких здійснюється їх обробка. Перелік видів державних інформаційних ресурсів та систем, щодо яких може здійснюватися резервне копіювання, визначається Кабінетом Міністрів України.

Стаття 2. Об'єкти захисту в системі

Об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

Стаття 3. Суб'єкти відносин

Суб'єктами відносин, пов'язаних із захистом інформації в системах, є:

– володільці інформації;

– власники системи;

– користувачі;

– спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації і підпорядковані йому регіональні органи;

На підставі укладеного договору або за дорученням власник системи може надати право розпоряджатися системою іншій фізичній або юридичній особі – розпоряднику системи.

Стаття 4. Доступ до інформації в системі

Порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються володільцем інформації.

Порядок доступу до державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, перелік користувачів та їх повноваження стосовно цієї інформації визначаються законодавством.

У випадках, передбачених законом, доступ до інформації в системі може здійснюватися без дозволу її володільця в порядку, встановленому законом.

Стаття 5. Відносини між володільцем інформації та власником системи

Власник системи забезпечує захист інформації в системі в порядку та на умовах, визначених у договорі, який укладається ним із володільцем інформації, якщо інше не передбачено законом.

Власник системи на вимогу володільця інформації надає відомості щодо захисту інформації в системі.

Протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування володільці інформації – власники (держателі) державних інформаційних ресурсів можуть укладати договори про технічне адміністрування відповідних реєстрів з іноземними компаніями, організаціями – постачальниками послуг з надання хмарних ресурсів (надавачами хмарних послуг), утвореними відповідно до законодавства інших держав, та/або їх зареєстрованими (акредитованими або легалізованими) відповідно до законодавства України філіями, представництвами та іншими відокремленими підрозділами з місцезнаходженням на території України в порядку, встановленому Кабінетом Міністрів України.

Стаття 6. Відносини між власником системи та користувачем

Власник системи надає користувачеві відомості про правила і режим роботи системи та забезпечує йому доступ до інформації в системі відповідно до визначеного порядку доступу.

Стаття 7. Відносини між власниками систем

Власник системи, яка використовується для обробки інформації з іншої системи, забезпечує захист такої інформації в порядку та на умовах, що визначаються договором, який укладається між власниками систем, якщо інше не встановлено законодавством. Власник системи, яка використовується для обробки інформації з іншої системи, повідомляє власника зазначеної системи про виявлені факти несанкціонованих дій щодо інформації в системі.

Стаття 8. Умови обробки інформації в системі

Умови обробки інформації в системі визначаються власником системи відповідно до договору з володільцем інформації, якщо інше не передбачено законодавством. Державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності комплексної системи захисту інформації здійснюється за результатами державної експертизи, яка проводиться з урахуванням галузевих вимог та норм інформаційної безпеки у порядку, встановленому законодавством.

Стаття 9. Забезпечення захисту інформації в системі

Відповідальність за забезпечення захисту інформації в системі покладається на власника системи. Власник системи, в якій обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним.

Про спроби та/або факти несанкціонованих дій у системі щодо державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, власник системи повідомляє відповідно спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкований йому регіональний орган.

Стаття 10. Повноваження державних органів у сфері захисту інформації в системах

Вимоги до забезпечення захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, встановлюються Кабінетом Міністрів України.

Стаття 11. Відповідальність за порушення законодавства про захист інформації в системах

Особи, винні в порушенні законодавства про захист інформації в системах, несуть відповідальність згідно із законом.

1.4. Закон України «Про основні засади забезпечення кібербезпеки України»

Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки, та складається з наступних статей.

Стаття 1. Визначення термінів

Стаття 2. Принципи застосування Закону

Стаття 3. Правові основи забезпечення кібербезпеки України

Стаття 4. Об’єкти кібербезпеки та кіберзахисту

Стаття 5. Суб’єкти забезпечення кібербезпеки

Стаття 6. Об’єкти критичної інфраструктури

Стаття 7. Принципи забезпечення кібербезпеки

Стаття 8. Національна система кібербезпеки

Стаття 9. Урядова команда реагування на комп’ютерні надзвичайні події України CERT-UA

Стаття 10. Державно-приватна взаємодія у сфері кібербезпеки

Стаття 11. Сприяння суб’єктам забезпечення кібербезпеки України

Стаття 12. Відповідальність за порушення законодавства у сфері кібербезпеки

Стаття 13. Фінансове забезпечення заходів кібербезпеки

Стаття 14. Міжнародне співробітництво у сфері кібербезпеки

Стаття 15. Контроль за законністю заходів із забезпечення кібербезпеки України

Стаття 1. Визначення термінів

У цьому Законі наведені нижче терміни вживаються в такому значенні:

– **індикатори кіберзагроз –** показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози;

– **інформація про інцидент кібербезпеки –** відомості про обставини кіберінциденту, зокрема про те, які об'єкти кіберзахисту і за яких умов зазнали кібератаки, які з них успішно виявлені, нейтралізовані, яким запобігли за допомогою яких засобів кіберзахисту, у тому числі з використанням яких індикаторів кіберзагроз;

– **інцидент кібербезпеки (далі – кіберінцидент) –** подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів;

– **кібератака** – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту;

– **кібербезпека** – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі;

– **кіберзагроза** – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів;

– **кіберзахист** – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем;

– **кіберзлочин (комп'ютерний злочин)** – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України;

– **кіберзлочинність** – сукупність кіберзлочинів;

– **кібероборона** – сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії;

– **кіберпростір** – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних;

– **кіберрозвідка** – діяльність, що здійснюється розвідувальними органами у кіберпросторі або з його використанням;

– **кібертероризм** – терористична діяльність, що здійснюється у кіберпросторі або з його використанням;

– **кібершпигунство** – шпигунство, що здійснюється у кіберпросторі або з його використанням;

– **критична інформаційна інфраструктура** – сукупність об'єктів критичної інформаційної інфраструктури;

– **Національна телекомунікаційна мережа** – сукупність спеціальних телекомунікаційних систем (мереж), систем спеціального зв'язку, інших комунікаційних систем, які використовуються в інтересах органів державної влади та органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону, призначена для обігу (передавання, приймання, створення, оброблення, зберігання) та захисту національних інформаційних ресурсів, забезпечення захищених електронних комунікацій, надання спектра сучасних захищених інформаційно-комунікаційних (мультисервісних) послуг в інтересах здійснення управління державою у мирний час, в умовах надзвичайного стану та в особливий період, та яка є мережею (системою) подвійного призначення з використанням частини її ресурсу для надання послуг, зокрема з кіберзахисту, іншим споживачам;

– **національні електронні інформаційні ресурси (далі – національні інформаційні ресурси)** – систематизовані електронні інформаційні ресурси, які містять інформацію незалежно від виду, змісту, форми, часу і місця її створення (включаючи публічну інформацію, державні інформаційні ресурси та іншу інформацію), призначену для задоволення життєво важливих суспільних потреб громадянина, особи, суспільства і держави. Під електронними інформаційними ресурсами розуміється будь-яка інформація, що створена, записана, оброблена або збережена у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів;

– **Національний центр резервування державних інформаційних ресурсів** – організована сукупність об'єктів, створених з метою забезпечення надійності та безперебійності роботи державних інформаційних ресурсів, кіберзахисту, зберігання національних електронних інформаційних ресурсів, резервного копіювання інформації та відомостей національних електронних

інформаційних ресурсів державних органів, військових формувань, утворених відповідно до законів, підприємств, установ та організацій;

– **об'єкт критичної інформаційної інфраструктури** – комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури;

– **система управління технологічними процесами (далі – технологічна система)** – автоматизована або автоматична система, яка є сукупністю обладнання, засобів, комплексів та систем обробки, передачі та приймання, призначена для організаційного управління та/або управління технологічними процесами (включаючи промислове, електронне, комунікаційне обладнання, інші технічні та технологічні засоби) незалежно від наявності доступу системи до мережі Інтернет та/або інших глобальних мереж передачі даних;

– **системи електронних комунікацій (далі – комунікаційні системи)** – системи передавання, комутації або маршрутизації, обладнання та інші ресурси (включаючи пасивні мережеві елементи, які дають змогу передавати сигнали за допомогою проводових, радіо-, оптичних або інших електромагнітних засобів, мережі мобільного, супутникового зв'язку, електричні кабельні мережі в частині, в якій вони використовуються для цілей передачі сигналів), що забезпечують електронні комунікації (передачу електронних інформаційних ресурсів), у тому числі засоби і пристрої зв'язку, комп'ютери, інша комп'ютерна техніка, інформаційно-телекомунікаційні системи, які мають доступ до мережі Інтернет та/або інших глобальних мереж передачі даних;

– **система активної протидії агресії у кіберпросторі** – сукупність організаційних, правових, наукових та технічних заходів, спрямованих на підвищення рівня кіберзахисту держави шляхом здійснення впливу на інформаційні (автоматизовані), електронно-комунікаційні, інформаційно-комунікаційні системи держави-агресора, джерела походження кіберзагроз та кібератак;

– **активна протидія агресії у кіберпросторі** – дії, спрямовані на підвищення рівня кіберзахисту шляхом нейтралізації кібератак держави-агресора, його систем і мереж, а також джерел походження кіберзагроз та кібератак, які використовуються для завдання шкоди національній безпеці України.

Стаття 4. Об'єкти кібербезпеки та кіберзахисту

1. **Об'єктами кібербезпеки** є:

– конституційні права і свободи людини і громадянина;

– суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;

– держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;

– національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;

– об'єкти критичної інфраструктури.

2. **Об’єктами кіберзахисту** є:

– комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;

– об’єкти критичної інформаційної інфраструктури;

– комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

3. Порядок формування переліку об’єктів критичної інформаційної інфраструктури, перелік таких об’єктів та порядок їх внесення до державного реєстру об’єктів критичної інформаційної інфраструктури, а також порядок формування та забезпечення функціонування державного реєстру об’єктів критичної інформаційної інфраструктури затверджуються Кабінетом Міністрів України.

Повноваження щодо формування та забезпечення функціонування реєстру об’єктів критичної інформаційної інфраструктури у банківській системі України покладаються на Національний банк України.

Стаття 5. Суб’єкти забезпечення кібербезпеки

4. **Суб’єктами,** які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є:

– міністерства та інші центральні органи виконавчої влади;

– місцеві державні адміністрації;

– органи місцевого самоврядування;

– правоохоронні, розвідувальні і контррозвідувальні органи, суб’єкти оперативно-розшукової діяльності;

– Збройні Сили України, інші військові формування, утворені відповідно до закону;

– Національний банк України;

– підприємства, установи та організації, віднесені до об’єктів критичної інфраструктури;

– суб’єкти господарювання, громадяни України та об’єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов’язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

5. Суб’єкти забезпечення кібербезпеки у межах своєї компетенції:

– здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях;

– здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;

– здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз;

– розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту;

– забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об’єктах та об’єктах, що належать до сфери їх управління;

– здійснюють інші заходи із забезпечення розвитку та безпеки кіберпростору.

Стаття 6. Об’єкти критичної інфраструктури

1. Віднесення об’єктів до об’єктів критичної інфраструктури та формування Реєстру об’єктів критичної інфраструктури здійснюються відповідно до Закону України "Про критичну інфраструктуру".

2. Критерії та порядок віднесення об’єктів до об’єктів критичної інфраструктури, перелік таких об’єктів, загальні вимоги до їх кіберзахисту, у тому числі щодо застосування індикаторів кіберзагроз, та вимоги до проведення незалежного аудиту інформаційної безпеки затверджуються Кабінетом Міністрів України, а щодо банків, інших осіб, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг – Національним банком України.

Стаття 7. Принципи забезпечення кібербезпеки

1. **Забезпечення кібербезпеки в Україні ґрунтується на принципах**:

– верховенства права, законності, поваги до прав людини і основоположних свобод та їх захисту в порядку, визначеному законом;

– забезпечення національних інтересів України;

– відкритості, доступності, стабільності та захищеності кіберпростору, розвитку мережі Інтернет та відповідальних дій у кіберпросторі;

– державно-приватної взаємодії, широкої співпраці з громадянським суспільством у сфері кібербезпеки та кіберзахисту, зокрема шляхом обміну інформацією про інциденти кібербезпеки, реалізації спільних наукових та дослідницьких проектів, навчання та підвищення кваліфікації кадрів у цій сфері;

– пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам, реалізації невід’ємного права держави на самозахист відповідно до норм міжнародного права у разі вчинення агресивних дій у кіберпросторі;

– пріоритетності запобіжних заходів;

– невідворотності покарання за вчинення кіберзлочинів;

– пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу;

– міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в терористичних, воєнних, інших протиправних цілях;

– забезпечення демократичного цивільного контролю за утвореними відповідно до законів України військовими формуваннями та правоохоронними органами, що провадять діяльність у сфері кібербезпеки.

Стаття 8. Національна система кібербезпеки

1. Національна система кібербезпеки є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури.

2. Основними **суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України.**

Стаття 9. Урядова команда реагування на комп'ютерні надзвичайні події України **CERT-UA**

1. **Завданнями CERT-UA** є:

– накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів;

– надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об'єктів;

– організація та проведення практичних семінарів з питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту;

– підготовка та розміщення на своєму офіційному веб-сайті рекомендацій щодо протидії сучасним видам кібератак та кіберзагроз;

– взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки;

– взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамках участі у Форумі команд реагування на інциденти безпеки FIRST із сплатою щорічних членських внесків;

– взаємодія з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору;

– опрацювання отриманої від громадян інформації про кіберінциденти щодо об'єктів кіберзахисту;

– сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам.

2. Забезпечення функціонування CERT-UA здійснює Державна служба спеціального зв’язку та захисту інформації України у межах штатної чисельності та виділених обсягів фінансування.

Стаття 12. Відповідальність за порушення законодавства у сфері кібербезпеки

Особи, винні у порушенні законодавства у сферах національної безпеки, електронних комунікацій та захисту інформації, якщо кіберпростір є місцем та/або способом здійснення кримінального правопорушення, іншого винного діяння, відповідальність за яке передбачена цивільним, адміністративним, кримінальним законодавством, несуть відповідальність згідно із законом.

1.5. Закон України «Про державну таємницю»

Цей Закон регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України, та складається з наступних розділів і статей.

Розділ I. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення термінів

Стаття 2. Законодавство України про державну таємницю

Стаття 3. Сфера дії Закону

Стаття 4. Державна політика щодо державної таємниці

Стаття 5. Компетенція державних органів, органів місцевого самоврядування та їх посадових осіб у сфері охорони державної таємниці

Стаття 6. Реалізація прав на секретну інформацію та її матеріальні носії

Стаття 7. Фінансування витрат на здійснення діяльності, пов'язаної з державною таємницею

Розділ II. ВІДНЕСЕННЯ ІНФОРМАЦІЇ ДО ДЕРЖАВНОЇ ТАЄМНИЦІ

Стаття 8. Інформація, що може бути віднесена до державної таємниці

Стаття 9. Державні експерти з питань таємниць

Стаття 10. Порядок віднесення інформації до державної таємниці

Стаття 11. Рішення державного експерта з питань таємниць

Стаття 12. Звід відомостей, що становлять державну таємницю

Стаття 13. Строк дії рішення про віднесення інформації до державної таємниці

Стаття 14. Зміна ступеня секретності інформації та скасування рішення про віднесення її до державної таємниці

Розділ III. ЗАСЕКРЕЧУВАННЯ ТА РОЗСЕКРЕЧУВАННЯ МАТЕРІАЛЬНИХ НОСІЇВ ІНФОРМАЦІЇ

Стаття 15. Засекречування та розсекречування матеріальних носіїв інформації

Стаття 16. Строк засекречування матеріальних носіїв інформації

Стаття 17. Оскарження рішення щодо засекречування матеріальних носіїв інформації

Розділ IV. ОХОРОНА ДЕРЖАВНОЇ ТАЄМНИЦІ

Стаття 18. Основні організаційно-правові заходи щодо охорони державної таємниці

Стаття 19. Єдині вимоги до матеріальних носіїв секретної інформації

Стаття 20. Дозвільний порядок провадження діяльності, пов'язаної з державною таємницею, та режим секретності

Стаття 21. Режимно-секретні органи

Стаття 22. Допуск громадян до державної таємниці

Стаття 23. Відмова у наданні допуску до державної таємниці

Стаття 24. Перевірка громадян у зв'язку з допуском їх до державної таємниці

Стаття 25. Оскарження громадянином відмови у наданні допуску до державної таємниці

Стаття 26. Переоформлення допуску до державної таємниці, підвищення або зниження його форми та скасування

Стаття 27. Доступ громадян до державної таємниці

Стаття 28. Обов'язки громадянина щодо збереження державної таємниці

Стаття 29. Обмеження прав у зв'язку з допуском та доступом до державної таємниці

Стаття 30. Компенсація громадянам у зв'язку з виконанням робіт, які передбачають доступ до державної таємниці

Стаття 30. Компенсація громадянам у зв'язку з виконанням робіт, які передбачають доступ до державної таємниці

Стаття 32. Обмеження щодо передачі державної таємниці іноземній державі чи міжнародній організації

Стаття 33. Обмеження, пов'язані з державною таємницею, щодо перебування і діяльності в Україні іноземців, осіб без громадянства та іноземних юридичних осіб, а також розташування та переміщення об'єктів і технічних засобів, що їм належать

Стаття 34. Особливості здійснення державними органами їх функцій щодо державних органів, органів місцевого самоврядування, підприємств, установ і організацій, що провадять діяльність, пов'язану з державною таємницею

Стаття 35. Технічний та криптографічний захисти секретної інформації

Стаття 36. Оперативно-розшукові заходи щодо охорони державної таємниці

Розділ V. КОНТРОЛЬ ЗА ЗАБЕЗПЕЧЕННЯМ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ТА НАГЛЯД ЗА ДОДЕРЖАННЯМ ЗАКОНОДАВСТВА ПРО ДЕРЖАВНУ ТАЄМНИЦЮ

Стаття 37. Контроль за забезпеченням охорони державної таємниці

Стаття 38. Нагляд за додержанням законодавства про державну таємницю

Розділ VI. ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА ПРО ДЕРЖАВНУ ТАЄМНИЦЮ

Стаття 39. Відповідальність за порушення законодавства про державну таємницю

Розділ І. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення термінів

У цьому Законі терміни вживаються у такому значенні:

– **державна таємниця (далі також – секретна інформація)** – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою;

– **віднесення інформації до державної таємниці** – процедура прийняття (державним експертом з питань таємниць) рішення про віднесення категорії відомостей або окремих відомостей до державної таємниці з установленням ступеня їх секретності шляхом обгрунтування та визначення можливої шкоди національній безпеці України у разі розголошення цих відомостей, включенням цієї інформації до Зводу відомостей, що становлять державну таємницю, та з опублікуванням цього Зводу, змін до нього;

– **гриф секретності** – реквізит матеріального носія секретної інформації, що засвідчує ступінь секретності даної інформації;

– **державний експерт з питань таємниць** – посадова особа, уповноважена здійснювати відповідно до вимог цього Закону віднесення інформації до державної таємниці у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, зміни ступеня секретності цієї інформації та її розсекречування;

– **допуск до державної таємниці** – оформлення права громадянина на доступ до секретної інформації;

– **доступ до державної таємниці** – надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, або ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, цією посадовою особою відповідно до її службових повноважень;

– **засекречування матеріальних носіїв інформації** – введення у встановленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом надання відповідного грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації;

– **Звід відомостей, що становлять державну таємницю**, – акт, в якому зведено переліки відомостей, що згідно з рішеннями державних експертів з питань таємниць становлять державну таємницю у визначених цим Законом сферах;

– **категорія режиму секретності** – категорія, яка характеризує важливість та обсяги відомостей, що становлять державну таємницю, які зосереджені в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях;

– **криптографічний захист секретної інформації** – вид захисту, що реалізується шляхом перетворення інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

– **матеріальні носії секретної інформації** – матеріальні об'єкти, в тому числі фізичні поля, в яких відомості, що становлять державну таємницю, відображені у вигляді текстів, знаків, символів, образів, сигналів, технічних рішень, процесів тощо;

– **охорона державної таємниці** – комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв;

– **режим секретності** – встановлений згідно з вимогами цього Закону та інших виданих відповідно до нього нормативно-правових актів єдиний порядок забезпечення охорони державної таємниці;

– **розсекречування матеріальних носіїв секретної інформації** – зняття в установленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом скасування раніше наданого грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації;

– **спеціальна експертиза щодо наявності умов для провадження діяльності, пов'язаної з державною таємницею**, – експертиза, що проводиться з метою визначення в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях наявності умов, передбачених цим Законом, для провадження діяльності, пов'язаної з державною таємницею;

– **ступінь секретності ("особливої важливості", "цілком таємно", "таємно")** – категорія, яка характеризує важливість секретної інформації, ступінь обмеження доступу до неї та рівень її охорони державою;

– **технічний захист секретної інформації** – вид захисту, спрямований на забезпечення інженерно-технічними заходами конфіденційності, цілісності та унеможливлення блокування інформації.

Стаття 5. Компетенція державних органів, органів місцевого самоврядування та їх посадових осіб у сфері охорони державної таємниці

Президент України, забезпечуючи національну безпеку, видає укази та розпорядження з питань охорони державної таємниці, віднесених цим Законом та іншими законами до його повноважень.

Рада національної безпеки і оборони України координує та контролює діяльність органів виконавчої влади у сфері охорони державної таємниці.

Кабінет Міністрів України спрямовує та координує роботу міністерств, інших органів виконавчої влади щодо забезпечення здійснення державної політики у сфері охорони державної таємниці.

Центральні та місцеві органи виконавчої влади, Рада міністрів Автономної Республіки Крим та органи місцевого самоврядування здійснюють державну політику у сфері охорони державної таємниці в межах своїх повноважень, передбачених законом.

Спеціально уповноваженим державним органом у сфері забезпечення охорони державної таємниці є Служба безпеки України.

Забезпечення охорони державної таємниці відповідно до вимог режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, діяльність яких пов'язана з державною таємницею, покладається на керівників зазначених органів, підприємств, установ і організацій.

Стаття 6. Реалізація прав на секретну інформацію та її матеріальні носії

Володілець секретної інформації або власник матеріальних носіїв такої інформації реалізує свої права з урахуванням обмежень, установлених в інтересах національної безпеки України відповідно до цього Закону.

Розділ ІІ. ВІДНЕСЕННЯ ІНФОРМАЦІЇ ДО ДЕРЖАВНОЇ ТАЄМНИЦІ

Стаття 8. Інформація, що може бути віднесена до державної таємниці

До державної таємниці у порядку, встановленому цим Законом, відноситься інформація:

1) **у сфері оборони**:

– про зміст стратегічних і оперативних планів та інших документів бойового управління, підготовку та проведення військових операцій, стратегічне та мобілізаційне розгортання військ, а також про інші найважливіші показники, які характеризують організацію, чисельність, дислокацію, бойову і мобілізаційну готовність, бойову та іншу військову підготовку, озброєння та матеріально-технічне забезпечення Збройних Сил України та інших військових формувань;

– про дислокацію, характеристики пунктів управління, зміст заходів загальнодержавного та регіонального, у разі необхідності міського і районного рівня, щодо приведення у готовність єдиної державної системи цивільного захисту населення і територій до виконання завдань в особливий період та про організацію системи зв'язку (оповіщення) в особливий період, можливості населених пунктів, регіонів і окремих об'єктів щодо евакуації, розосередження населення і забезпечення його життєдіяльності; забезпечення виробничої діяльності об'єктів національної економіки у воєнний час;

– про геодезичні, гравіметричні, картографічні та гідрометеорологічні дані і характеристики, які мають значення для оборони країни;

– про застосування систем озброєння, підготовку та проведення військових операцій;

– про винаходи, дослідження і розробку нових зразків озброєння в інтересах забезпечення національної безпеки і оборони та про результати таких досліджень і розробок;

– про заходи та показники розвитку Збройних Сил України та їх спроможностей;

– про склад, завдання та матеріально-технічне забезпечення розвідувального органу Міністерства оборони України та зібрану і створену ним інформацію в результаті його діяльності;

– про особовий склад Сил спеціальних операцій Збройних Сил України, а також осіб, які співпрацюють або раніше співпрацювали на конфіденційній

основі із Силами спеціальних операцій Збройних Сил України, фінансування та матеріально-технічне забезпечення руху опору, засоби, зміст, плани, організацію, завдання, форми, методи і результати ведення руху опору, оперативний резерв та мережу осередків руху опору;

2) **у сфері економіки, науки і техніки**:

– про зміст мобілізаційних планів державних органів та органів місцевого самоврядування, мобілізаційні потужності, заходи мобілізаційної підготовки і мобілізації та обсяги їх фінансування, запаси та обсяги постачання стратегічних видів сировини і матеріалів, а також зведені відомості про номенклатуру та рівні накопичення, загальні обсяги поставок, відпуску, закладення, освіження, розміщення і фактичні запаси державного матеріального резерву;

– про використання транспорту, зв'язку, потужностей інших галузей та об'єктів інфраструктури держави в інтересах забезпечення її безпеки;

– про плани, обсяги та інші найважливіші характеристики добування, виробництва та реалізації окремих стратегічних видів сировини і продукції;

– про державні запаси дорогоцінних металів монетарної групи, коштовного каміння, валюти та інших цінностей, операції, пов'язані з виготовленням грошових знаків і цінних паперів, їх зберіганням, охороною і захистом від підроблення, обігом, обміном або вилученням з обігу, а також про інші особливі заходи фінансової діяльності держави;

– про наукові, науково-дослідні, дослідно-конструкторські та проектні роботи, предметом яких є створення новітніх складних зразків озброєння, військової або спеціальної техніки та інші роботи, що мають важливе оборонне чи економічне значення або суттєво впливають на зовнішньоекономічну діяльність та національну безпеку України;

– про найменування, загальну кількість, вартість озброєння, військової техніки, боєприпасів, запасних частин та матеріалів до них, що закуповуються для потреб військових формувань (правоохоронних органів);

– про кількість, строки поставок військовим формуванням чи правоохоронним органам, спеціальним формуванням Міністерства внутрішніх справ України для забезпечення їх боєздатності основних видів пального (мастильних матеріалів), речового майна та продовольства;

– про факт та предмет закупівлі товарів, робіт і послуг оборонного призначення для забезпечення Збройних Сил України та інших військових формувань та правоохоронних органів (крім випадків, якщо окрема інформація про закупівлю таких товарів, робіт і послуг оборонного призначення, що закуповуються відповідно до Закону України "Про оборонні закупівлі", становить державну таємницю. У такому разі окрема інформація розміщується у додатку до тендерної документації).

– Інформація не може бути повторно віднесена до державної таємниці після розсекречення та оприлюднення;

3) **у сфері зовнішніх відносин**:

– про директиви, плани, вказівки делегаціям і посадовим особам з питань зовнішньополітичної і зовнішньоекономічної діяльності України, спрямовані на забезпечення її національних інтересів і безпеки;

– про військове, науково-технічне та інше співробітництво України з іноземними державами, якщо розголошення відомостей про це завдаватиме шкоди національній безпеці України;

– про експорт та імпорт озброєння, військової і спеціальної техніки, окремих стратегічних видів сировини і продукції;

– про зміст секретної інформації, що отримується від іноземної держави чи міжнародної організації;

4) **у сфері державної безпеки та охорони правопорядку**:

– про особовий склад органів, що здійснюють оперативно-розшукову діяльність або розвідувальну чи контррозвідувальну;

– про засоби, зміст, плани, організацію, фінансування та матеріально-технічне забезпечення, форми, методи і результати оперативно-розшукової, розвідувальної і контррозвідувальної діяльності; про осіб, які співпрацюють або раніше співпрацювали на конфіденційній основі з органами, що проводять таку діяльність; про склад і конкретних осіб, що є негласними штатними працівниками органів, які здійснюють оперативно-розшукову, розвідувальну і контррозвідувальну діяльність;

– про організацію та порядок здійснення охорони адміністративних будинків та інших державних об'єктів, посадових та інших осіб, охорона яких здійснюється відповідно до Закону України "Про державну охорону органів державної влади України та посадових осіб";

– про систему урядового та спеціального зв'язку;

– про організацію, зміст, стан і плани розвитку криптографічного захисту секретної інформації, зміст і результати наукових досліджень у сфері криптографії;

– про системи та засоби криптографічного захисту секретної інформації, їх розроблення, виробництво, технологію виготовлення та використання;

– про державні шифри, їх розроблення, виробництво, технологію виготовлення та використання;

– про організацію режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, державні програми, плани та інші заходи у сфері охорони державної таємниці;

– про організацію, зміст, стан і плани розвитку технічного захисту секретної інформації;

– про результати перевірок, здійснюваних згідно з законом прокурором у порядку відповідного нагляду за додержанням законів, та про зміст матеріалів оперативно-розшукової діяльності, досудового розслідування та судочинства з питань, зазначених у цій статті сфер;

– про інші засоби, форми і методи охорони державної таємниці.

Конкретні відомості можуть бути віднесені до державної таємниці за ступенями секретності "особливої важливості", "цілком таємно" та "таємно" лише за умови, що вони належать до категорій, зазначених у частині першій цієї статті, і їх розголошення завдаватиме шкоди інтересам національної безпеки України та з дотриманням вимог статті 6 Закону України "Про доступ до публічної інформації".

Забороняється віднесення до державної таємниці будь-яких відомостей, якщо цим будуть звужуватися зміст і обсяг конституційних прав та свобод людини і громадянина, завдаватиметься шкода здоров'ю та безпеці населення.

Не відноситься до державної таємниці інформація:

– про стан довкілля, про якість харчових продуктів і предметів побуту, про вплив товару (роботи, послуги) на життя та здоров’я людини;

– про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, які сталися або можуть статися і загрожують безпеці громадян;

– про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;

– про факти порушень прав і свобод людини і громадянина;

– про незаконні дії державних органів, органів місцевого самоврядування та їх посадових і службових осіб;

– інша інформація, доступ до якої відповідно до законів та міжнародних договорів, згода на обов’язковість яких надана Верховною Радою України, не може бути обмежено.

Стаття 9. Державні експерти з питань таємниць

Державний експерт з питань таємниць здійснює відповідно до вимог цього Закону віднесення інформації у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку до державної таємниці, зміни ступеня секретності цієї інформації та її розсекречування.

Стаття 10. Порядок віднесення інформації до державної таємниці

Віднесення інформації до державної таємниці здійснюється мотивованим рішенням державного експерта з питань таємниць за його власною ініціативою, за зверненням керівників відповідних державних органів, органів місцевого самоврядування, підприємств, установ, організацій чи громадян.

Державний експерт з питань таємниць відносить інформацію до державної таємниці з питань, прийняття рішень з яких належить до його компетенції згідно з посадою. У разі, якщо прийняття рішення про віднесення інформації до державної таємниці належить до компетенції кількох державних експертів з питань таємниць, воно за ініціативою державних експертів або за пропозицією Служби безпеки України приймається колегіально та ухвалюється простою більшістю голосів. При цьому кожен експерт має право викласти свою думку.

Інформація вважається державною таємницею з часу опублікування Зводу відомостей, що становлять державну таємницю, до якого включена ця інформація, чи зміни до нього у порядку, встановленому цим Законом.

Інформація відноситься до державної таємниці з урахуванням таких принципів:

– дотримання балансу інтересів національної безпеки, демократичних принципів відкритості та прозорості;

– вільного обігу інформації;

– презумпції публічності інформації до її віднесення в установленому законодавством порядку до державної таємниці.

У разі невідповідності інформації вимогам, встановленим цим Законом, забороняється віднесення її до державної таємниці. Засекречуванню підлягає інформація, а не документ. Якщо документ містить державну таємницю, для ознайомлення надається інформація, доступ до якої не обмежений.

Стаття 11. Рішення державного експерта з питань таємниць

У рішенні державного експерта з питань таємниць про віднесення інформації до державної таємниці зазначаються:

– інформація, яка має становити державну таємницю, та її відповідність категоріям і вимогам, передбаченим статтею 8 цього Закону та статтею 6 Закону України "Про доступ до публічної інформації";

– підстави для віднесення інформації до державної таємниці;

– критерії віднесення інформації до державної таємниці, зокрема:

– визначення рівня та опис загрози та шкоди національній безпеці (національним інтересам) у разі невіднесення інформації до державної таємниці;

– визначення дати або події розсекречування інформації;

– ступінь секретності зазначеної інформації;

– обсяг фінансування заходів, необхідних для охорони такої інформації;

– державний орган, орган місцевого самоврядування, підприємство, установа, організація чи громадянин, який вніс пропозицію про віднесення цієї інформації до державної таємниці, та державний орган (органи), якому надається право визначати коло суб'єктів, які матимуть доступ до цієї інформації;

– строк, протягом якого діє рішення про віднесення інформації до державної таємниці.

Стаття 12. Звід відомостей, що становлять державну таємницю

Звід відомостей, що становлять державну таємницю, формує Служба безпеки України на підставі рішень державних експертів з питань таємниць. Зазначений Звід та зміни до нього набирають чинності з моменту опублікування в офіційних виданнях України.

Зміни до Зводу відомостей, що становлять державну таємницю, вносяться не пізніше трьох місяців з дня одержання Службою безпеки України відповідного рішення державного експерта з питань таємниць.

Стаття 13. Строк дії рішення про віднесення інформації до державної таємниці

Строк, протягом якого діє рішення про віднесення інформації до державної таємниці, встановлюється державним експертом з питань таємниць з урахуванням ступеня секретності інформації, критерії визначення якого встановлюються Службою безпеки України, та інших обставин. **Він не може перевищувати для інформації із ступенем секретності "особливої важливості" – 30 років, для інформації "цілком таємно" – 10 років, для інформації "таємно" – 5 років.**

Після закінчення передбаченого частиною першою цієї статті строку дії рішення про віднесення інформації до державної таємниці державний експерт з питань таємниць приймає рішення про скасування рішення про віднесення її до державної таємниці або приймає рішення про продовження строку дії

зазначеного рішення в межах строків, встановлених частиною першою цієї статті.

Стаття 14. Зміна ступеня секретності інформації та скасування рішення про віднесення її до державної таємниці

Підвищення або зниження ступеня секретності інформації та скасування рішення про віднесення її до державної таємниці здійснюються на підставі рішення державного експерта з питань таємниць або на підставі рішення суду у випадках, передбачених статтею 12 цього Закону, та оформляються Службою безпеки України шляхом внесення відповідних змін до Зводу відомостей, що становлять державну таємницю.

Розділ III. ЗАСЕКРЕЧУВАННЯ ТА РОЗСЕКРЕЧУВАННЯ МАТЕРІАЛЬНИХ НОСІЇВ ІНФОРМАЦІЇ

Стаття 15. Засекречування та розсекречування матеріальних носіїв інформації

Засекречування матеріальних носіїв інформації здійснюється шляхом надання на підставі Зводу відомостей, що становлять державну таємницю (розгорнутих переліків відомостей, що становлять державну таємницю), відповідному документу, виробу або іншому матеріальному носію інформації грифа секретності посадовою особою, яка готує або створює документ, виріб або інший матеріальний носій інформації. Засекречування документів здійснюється лише в частині відомостей, що становлять державну таємницю. У разі подання запиту на документ, частина якого засекречена, доступ до такого документа забезпечується в частині, що не засекречена.

Гриф секретності кожного матеріального носія секретної інформації повинен відповідати ступеню секретності інформації, яка у ньому міститься, згідно із Зводом відомостей, що становлять державну таємницю, – **"особливої важливості", "цілком таємно" або "таємно"**. Реквізити кожного матеріального носія секретної інформації складаються із:

– грифа секретності;

– номера примірника;

– статті Зводу відомостей, що становлять державну таємницю, на підставі якої здійснюється засекречення;

– найменування посади та підпису особи, яка надала гриф секретності.

Якщо реквізити, зазначені у частині другій цієї статті, неможливо нанести безпосередньо на матеріальний носій секретної інформації, вони мають бути зазначені у супровідних документах.

Розділ IV. ОХОРОНА ДЕРЖАВНОЇ ТАЄМНИЦІ

Стаття 18. Основні організаційно-правові заходи щодо охорони державної таємниці

З метою охорони державної таємниці впроваджуються:

– єдині вимоги до виготовлення, користування, збереження, передачі, транспортування та обліку матеріальних носіїв секретної інформації;

– дозвільний порядок провадження державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями діяльності, пов'язаної з державною таємницею;

– обмеження оприлюднення, передачі іншій державі або поширення іншим шляхом секретної інформації;

– обмеження щодо перебування та діяльності в Україні іноземців, осіб без громадянства та іноземних юридичних осіб, їх доступу до державної таємниці, а також розташування і переміщення об'єктів і технічних засобів, що їм належать;

– особливості здійснення державними органами їх функцій щодо державних органів, органів місцевого самоврядування, підприємств, установ і організацій, діяльність яких пов'язана з державною таємницею;

– режим секретності державних органів, органів місцевого самоврядування, підприємств, установ і організацій, що провадять діяльність, пов'язану з державною таємницею;

– спеціальний порядок допуску та доступу громадян до державної таємниці;

– технічний та криптографічний захисти секретної інформації.

Стаття 21. Режимно-секретні органи

В державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, що провадять діяльність, пов'язану з державною таємницею, з метою розроблення та здійснення заходів щодо забезпечення режиму секретності, постійного контролю за їх додержанням створюються на правах окремих структурних підрозділів режимно-секретні органи (далі – РСО), які підпорядковуються безпосередньо керівнику державного органу, органу місцевого самоврядування, підприємства, установи, організації.

Стаття 22. Допуск громадян до державної таємниці

Залежно від ступеня секретності інформації встановлюються такі форми допуску до державної таємниці:

– форма 1 – для роботи з секретною інформацією, що має ступені секретності "особливої важливості", "цілком таємно" та "таємно";

– форма 2 – для роботи з секретною інформацією, що має ступені секретності "цілком таємно" та "таємно";

– форма 3 – для роботи з секретною інформацією, що має ступінь секретності "таємно",

а також такі терміни дії допусків:

– для форми 1 – 5 років;

– для форми 2 – 7 років;

– для форми 3 – 10 років.

Стаття 28. Обов'язки громадянина щодо збереження державної таємниці

Громадянин, якому надано допуск до державної таємниці, зобов'язаний:

– не допускати розголошення будь-яким способом державної таємниці, яка йому довірена або стала відомою у зв'язку з виконанням службових обов'язків;

– не брати участі в діяльності політичних партій та громадських організацій, діяльність яких заборонена в порядку, встановленому законом;

– не сприяти іноземним державам, іноземним організаціям чи їх представникам, а також окремим іноземцям та особам без громадянства у

провадженні діяльності, що завдає шкоди інтересам національної безпеки України;

– виконувати вимоги режиму секретності;

– повідомляти посадових осіб, які надали йому доступ до державної таємниці, та відповідні режимно-секретні органи про виникнення обставин, передбачених статтею 23 цього Закону, або інших обставин, що перешкоджають збереженню довіреної йому державної таємниці, а також повідомляти у письмовій формі про свій виїзд з України;

– додержуватися інших вимог законодавства про державну таємницю.

Стаття 29. Обмеження прав у зв'язку з допуском та доступом до державної таємниці

Громадянин, якому було надано допуск та доступ до державної таємниці у порядку, встановленому законодавством, і який реально був обізнаний з нею, може бути обмежений у праві виїзду на постійне місце проживання в іноземну державу до розсекречування відповідної інформації, але **не більш як на п'ять років з часу припинення діяльності, пов'язаної з державною таємницею**.

Не обмежується виїзд у держави, з якими Україна має міжнародні договори, що передбачають такий виїзд і згода на обов'язковість яких надана Верховною Радою України.

На громадянина також поширюються обмеження свободи інформаційної діяльності, що випливають з цього Закону.

Стаття 35. Технічний та криптографічний захисти секретної інформації

Технічний та криптографічний захисти секретної інформації здійснюються в порядку, встановленому Президентом України.

Стаття 36. Оперативно-розшукові заходи щодо охорони державної таємниці

Оперативно-розшукові заходи щодо охорони державної таємниці здійснюються відповідно до Закону України "Про оперативно-розшукову діяльність".

Розділ V. КОНТРОЛЬ ЗА ЗАБЕЗПЕЧЕННЯМ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ТА НАГЛЯД ЗА ДОДЕРЖАННЯМ ЗАКОНОДАВСТВА ПРО ДЕРЖАВНУ ТАЄМНИЦЮ

Стаття 37. Контроль за забезпеченням охорони державної таємниці

Керівники державних органів, органів місцевого самоврядування, підприємств, установ і організацій зобов'язані здійснювати постійний контроль за забезпеченням охорони державної таємниці.

Контроль за додержанням законодавства про державну таємницю в системі Служби безпеки України здійснюється відповідно до Закону України "Про Службу безпеки України".

Розділ VI. ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА ПРО ДЕРЖАВНУ ТАЄМНИЦЮ

Стаття 39. Відповідальність за порушення законодавства про державну таємницю

Посадові особи та громадяни, винні у:

– розголошенні державної таємниці;

– втраті документів та інших матеріальних носіїв секретної інформації;

– недодержанні встановленого законодавством порядку передачі державної таємниці іншій державі чи міжнародній організації;

– засекречуванні інформації, зазначеної у частинах третій і четвертій статті 8 цього Закону;

– навмисному невіднесенні до державної таємниці інформації, розголошення якої може завдати шкоди інтересам національної безпеки України, а також необгрунтованому заниженні ступеня секретності або необгрунтованому розсекречуванні секретної інформації;

– безпідставному засекречуванні інформації, у тому числі з порушенням вимог Закону України "Про доступ до публічної інформації";

– наданні грифа секретності матеріальним носіям інформації, яка не становить державної таємниці, або ненаданні грифа секретності матеріальним носіям інформації, що становить державну таємницю, а також безпідставному скасуванні чи зниженні грифа секретності матеріальних носіїв секретної інформації;

– порушенні встановленого законодавством порядку надання допуску та доступу до державної таємниці;

– порушенні встановленого законодавством режиму секретності та невиконанні обов'язків щодо збереження державної таємниці;

– невжитті заходів щодо забезпечення охорони державної таємниці та незабезпеченні контролю за охороною державної таємниці;

– провадженні діяльності, пов'язаної з державною таємницею, без одержання в установленому порядку спеціального дозволу на провадження такої діяльності, а також розміщенні державних замовлень на виконання робіт, доведенні мобілізаційних завдань, пов'язаних з державною таємницею, в державних органах, органах місцевого самоврядування, на підприємствах, в установах, організаціях, яким не надано спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею;

– недодержанні вимог законодавства щодо забезпечення охорони державної таємниці під час здійснення міжнародного співробітництва, прийому іноземних делегацій, груп, окремих іноземців та осіб без громадянства і проведення роботи з ними;

– невиконанні норм і вимог технічного захисту секретної інформації, внаслідок чого виникає реальна загроза порушення цілісності цієї інформації або просочення її технічними каналами,

несуть дисциплінарну, адміністративну та кримінальну відповідальність згідно із законом.

1.6. Закон України «Про захист персональних даних».

Стаття 1. Сфера дії Закону

Цей Закон регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних. Цей Закон поширюється на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів, а також на обробку персональних даних, що містяться у картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів.

Стаття 2. Визначення термінів

У цьому Законі нижченаведені терміни вживаються в такому значенні:

– **база персональних даних** – іменована сукупність упорядкованих персональних даних в електронній формі та/або у формі картотек персональних даних;

– **володілець персональних даних** – фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом;

– **згода суб'єкта персональних даних** – добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди. **У сфері електронної комерції** згода суб'єкта персональних даних може бути надана під час реєстрації в інформаційно-комунікаційній системі суб'єкта електронної комерції шляхом проставлення відмітки про надання дозволу на обробку своїх персональних даних відповідно до сформульованої мети їх обробки, за умови, що така система не створює можливостей для обробки персональних даних до моменту проставлення відмітки;

– **знеособлення персональних даних** – вилучення відомостей, які дають змогу прямо чи опосередковано ідентифікувати особу;

– **картотека** – будь-які структуровані персональні дані, доступні за визначеними критеріями, незалежно від того, чи такі дані централізовані, децентралізовані або розділені за функціональними чи географічними принципами;

– **обробка персональних даних** – будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем;

– **одержувач** – фізична чи юридична особа, якій надаються персональні дані, у тому числі третя особа;

– **персональні дані** – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована;

– **розпорядник персональних даних** – фізична чи юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця;

– **суб'єкт персональних даних** – фізична особа, персональні дані якої обробляються;

– **третя особа** – будь-яка особа, за винятком суб'єкта персональних даних, володільця чи розпорядника персональних даних та Уповноваженого Верховної Ради України з прав людини, якій володільцем чи розпорядником персональних даних здійснюється передача персональних даних.

Стаття 4. Суб'єкти відносин, пов'язаних із персональними даними

1. **Суб'єктами** відносин, пов'язаних із персональними даними, є:

– суб'єкт персональних даних;

– володілець персональних даних;

– розпорядник персональних даних;

– третя особа;

– Уповноважений Верховної Ради України з прав людини (далі – Уповноважений).

2. **Володільцем чи розпорядником персональних даних** можуть бути підприємства, установи і організації усіх форм власності, органи державної влади чи органи місцевого самоврядування, фізичні особи – підприємці, які обробляють персональні дані відповідно до закону.

3. **Розпорядником персональних даних, володільцем яких є орган державної влади чи орган місцевого самоврядування,** крім цих органів, може бути лише підприємство державної або комунальної форми власності.

4. **Володілець персональних даних може доручити** обробку персональних даних розпоряднику персональних даних відповідно до договору, укладеного в письмовій формі.

5. **Розпорядник персональних даних** може обробляти персональні дані лише з метою і в обсязі, визначених у договорі.

Стаття 5. Об'єкти захисту

1. **Об'єктами захисту є персональні дані**.

2. Персональні дані можуть бути віднесені до конфіденційної інформації про особу законом або відповідною особою**. Не є конфіденційною інформацією персональні дані,** що стосуються здійснення особою, уповноваженою на виконання функцій держави або місцевого самоврядування, посадових або службових повноважень.

3. **Персональні дані, зазначені у декларації особи**, уповноваженої на виконання функцій держави або місцевого самоврядування, оформленій за формою, визначеною відповідно до Закону України "Про запобігання корупції", **не належать до інформації з обмеженим доступом, крім відомостей, визначених Законом України "Про запобігання корупції".**

Не належить до інформації з обмеженим доступом інформація про отримання у будь-якій формі фізичною особою бюджетних коштів, державного чи комунального майна, структуру, принципи формування та розмір оплати праці, винагороди, додаткового блага керівника, заступника керівника

юридичної особи публічного права, керівника, заступника керівника, члена наглядової ради державного чи комунального підприємства або державної чи комунальної організації, що має на меті одержання прибутку, особи, яка постійно або тимчасово обіймає посаду члена виконавчого органу чи входить до складу наглядової ради господарського товариства, у статутному капіталі якого більше 50 відсотків акцій (часток, паїв) прямо чи опосередковано належать державі та/або територіальній громаді, крім випадків, передбачених статтею 6 Закону України "Про доступ до публічної інформації".

Не належить до інформації з обмеженим доступом інформація про фізичних осіб, які мають податковий борг, яка публікується на офіційному веб-порталі центрального органу виконавчої влади, що реалізує державну податкову політику, відповідно до вимог пункту 35.4 статті 35 Податкового кодексу України.

Законом може бути заборонено віднесення інших відомостей, що є персональними даними, до інформації з обмеженим доступом.

Стаття 6. Загальні вимоги до обробки персональних даних

1. Мета обробки персональних даних має бути сформульована в законах, інших нормативно-правових актах, положеннях, установчих чи інших документах, які регулюють діяльність володільця персональних даних, та відповідати законодавству про захист персональних даних.

Обробка персональних даних здійснюється відкрито і прозоро із застосуванням засобів та у спосіб, що відповідають визначеним цілям такої обробки.

У разі зміни визначеної мети обробки персональних даних на нову мету, яка є несумісною з попередньою, для подальшої обробки даних володілець персональних даних повинен отримати згоду суб’єкта персональних даних на обробку його даних відповідно до зміненої мети, якщо інше не передбачено законом.

2. Персональні дані мають бути точними, достовірними та оновлюватися в міру потреби, визначеної метою їх обробки.

3. Склад та зміст персональних даних мають бути відповідними, адекватними та ненадмірними стосовно визначеної мети їх обробки.

4. Первинними джерелами відомостей про фізичну особу є: видані на її ім'я документи; підписані нею документи; відомості, які особа надає про себе.

5. Обробка персональних даних здійснюється для конкретних і законних цілей, визначених за згодою суб’єкта персональних даних, або у випадках, передбачених законами України, у порядку, встановленому законодавством.

6. Не допускається обробка даних про фізичну особу, які є конфіденційною інформацією, без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

7. Якщо обробка персональних даних є необхідною для захисту життєво важливих інтересів суб'єкта персональних даних, обробляти персональні дані без його згоди можна до часу, коли отримання згоди стане можливим.

8. Персональні дані обробляються у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються, не довше, ніж це необхідно для законних цілей, у яких вони збиралися або надалі оброблялися.

Подальша обробка персональних даних в історичних, статистичних чи наукових цілях може здійснюватися за умови забезпечення їх належного захисту.

Стаття 7. Особливі вимоги до обробки персональних даних

1. Забороняється обробка персональних даних про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, засудження до кримінального покарання, а також даних, що стосуються здоров’я, статевого життя, біометричних або генетичних даних.

2. Положення частини першої цієї статті не застосовується, якщо обробка персональних даних:

1) здійснюється за умови надання суб'єктом персональних даних однозначної згоди на обробку таких даних;

2) необхідна для здійснення прав та виконання обов'язків володільця у сфері трудових правовідносин відповідно до закону із забезпеченням відповідного захисту;

3) необхідна для захисту життєво важливих інтересів суб'єкта персональних даних або іншої особи у разі недієздатності або обмеження цивільної дієздатності суб'єкта персональних даних;

4) здійснюється із забезпеченням відповідного захисту релігійною організацією, громадською організацією світоглядної спрямованості, політичною партією або професійною спілкою, що створені відповідно до закону, за умови, що обробка стосується виключно персональних даних членів цих об'єднань або осіб, які підтримують постійні контакти з ними у зв'язку з характером їх діяльності, та персональні дані не передаються третій особі без згоди суб'єктів персональних даних;

5) необхідна для обґрунтування, задоволення або захисту правової вимоги;

6) необхідна в цілях охорони здоров’я для:

– встановлення медичного діагнозу, для забезпечення піклування чи лікування або надання медичних послуг, моніторингу відповідності встановленим умовам надання таких послуг функціонування електронної системи охорони здоров’я за умови, що такі дані обробляються медичним працівником, фахівцем з реабілітації або іншою особою закладу охорони здоров’я, реабілітаційного закладу чи фізичною особою – підприємцем, яка одержала ліцензію на провадження господарської діяльності з медичної практики, та її працівниками, на яких покладено обов’язки щодо забезпечення захисту персональних даних та поширюється дія законодавства про лікарську таємницю, працівниками центрального органу виконавчої влади, що реалізує державну політику у сфері державних фінансових гарантій медичного обслуговування населення, працівниками закладу, що здійснює державний санітарно-епідеміологічний нагляд та діяльність у галузі громадського здоров’я, який одержав ліцензію на провадження господарської діяльності з медичної

практики, на яких покладено обов’язки щодо забезпечення захисту персональних даних;

– контролю якості надання медичних послуг за умови, що такі дані обробляються працівниками центрального органу виконавчої влади, що реалізує державну політику у сфері контролю якості надання медичних послуг;

– обміну інформацією про фінансування медичних послуг та послуг у сфері охорони здоров’я за умови, що такі дані обробляються працівниками Фонду соціального страхування України, Пенсійного фонду України, Фонду соціального захисту осіб з інвалідністю, центрального органу виконавчої влади, що забезпечує формування та реалізує державну фінансову та бюджетну політику, на яких покладено обов’язки щодо забезпечення захисту персональних даних.

6^{-1}) необхідна в цілях забезпечення ведення військового обліку призовників, військовозобов’язаних та резервістів (в обсягах даних, зазначених у статті 7 Закону України "Про Єдиний державний реєстр призовників, військовозобов’язаних та резервістів");

7) стосується вироків суду, виконання завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом та здійснюється державним органом в межах його повноважень, визначених законом;

8) стосується даних, які були явно оприлюднені суб'єктом персональних даних.

Стаття 8. Права суб'єкта персональних даних

1. Особисті немайнові права на персональні дані, які має кожна фізична особа, є невід'ємними і непорушними.

2. **Суб'єкт персональних даних має право:**

– знати про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки, місцезнаходження або місце проживання (перебування) володільця чи розпорядника персональних даних або дати відповідне доручення щодо отримання цієї інформації уповноваженим ним особам, крім випадків, встановлених законом;

– отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються його персональні дані;

– на доступ до своїх персональних даних;

– отримувати не пізніш як за тридцять календарних днів з дня надходження запиту, крім випадків, передбачених законом, відповідь про те, чи обробляються його персональні дані, а також отримувати зміст таких персональних даних;

– пред’являти вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних;

– пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними;

– на захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання

відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи;

– звертатися із скаргами на обробку своїх персональних даних до Уповноваженого або до суду;

– застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних;

– вносити застереження стосовно обмеження права на обробку своїх персональних даних під час надання згоди;

– відкликати згоду на обробку персональних даних;

– знати механізм автоматичної обробки персональних даних;

– на захист від автоматизованого рішення, яке має для нього правові наслідки.

Стаття 9. Повідомлення про обробку персональних даних

1. Володілець персональних даних повідомляє Уповноваженого про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, упродовж тридцяти робочих днів з дня початку такої обробки.

Види обробки персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, та категорії суб'єктів, на яких поширюється вимога щодо повідомлення, визначаються Уповноваженим.

2. Повідомлення про обробку персональних даних подається за формою та в порядку, визначеними Уповноваженим.

3. Володілець персональних даних зобов'язаний повідомляти Уповноваженого про кожну зміну відомостей, що підлягають повідомленню, упродовж десяти робочих днів з дня настання такої зміни.

4. Інформація, що повідомляється відповідно до цієї статті, підлягає оприлюдненню на офіційному веб-сайті Уповноваженого в порядку, визначеному Уповноваженим.

Стаття 10. Використання персональних даних

1. Використання персональних даних передбачає будь-які дії володільця щодо обробки цих даних, дії щодо їх захисту, а також дії щодо надання часткового або повного права обробки персональних даних іншим суб'єктам відносин, пов'язаних із персональними даними, що здійснюються за згодою суб'єкта персональних даних чи відповідно до закону.

2. Використання персональних даних володільцем здійснюється у разі створення ним умов для захисту цих даних. Володільцю забороняється розголошувати відомості стосовно суб'єктів персональних даних, доступ до персональних даних яких надається іншим суб'єктам відносин, пов'язаних з такими даними.

3. **Використання персональних даних працівниками суб'єктів відносин, пов'язаних з персональними даними, повинно здійснюватися лише відповідно до їхніх професійних чи службових або трудових обов'язків.** Ці працівники зобов'язані не допускати розголошення у будь-який спосіб персональних даних, які їм було довірено або які стали відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків, крім випадків,

передбачених законом. Таке зобов'язання чинне після припинення ними діяльності, пов'язаної з персональними даними, крім випадків, установлених законом.

4. **Відомості про особисте життя фізичної особи не можуть використовуватися як чинник, що підтверджує чи спростовує її ділові якості.**

5. **Стаття 11. Підстави для обробки персональних даних**

1. Підставами для обробки персональних даних є:

– згода суб'єкта персональних даних на обробку його персональних даних;

– дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень;

– укладення та виконання правочину, стороною якого є суб'єкт персональних даних або який укладено на користь суб'єкта персональних даних чи для здійснення заходів, що передують укладенню правочину на вимогу суб'єкта персональних даних;

– захист життєво важливих інтересів суб'єкта персональних даних;

– необхідність виконання обов'язку володільця персональних даних, який передбачений законом;

– необхідність захисту законних інтересів володільця персональних даних або третьої особи, якій передаються персональні дані, крім випадків, коли потреби захисту основоположних прав і свобод суб'єкта персональних даних у зв'язку з обробкою його даних переважають такі інтереси.

Стаття 12. Збирання персональних даних

1. Збирання персональних даних є складовою процесу їх обробки, що передбачає дії з підбору чи впорядкування відомостей про фізичну особу.

2. Суб'єкт персональних даних повідомляється про володільця персональних даних, склад та зміст зібраних персональних даних, свої права, визначені цим Законом, мету збору персональних даних та осіб, яким передаються його персональні дані:

– в момент збору персональних даних, якщо персональні дані збираються у суб'єкта персональних даних;

– в інших випадках протягом тридцяти робочих днів з дня збору персональних даних.

Стаття 13. Накопичення та зберігання персональних даних

1. Накопичення персональних даних передбачає дії щодо поєднання та систематизації відомостей про фізичну особу чи групу фізичних осіб або внесення цих даних до бази персональних даних.

2. Зберігання персональних даних передбачає дії щодо забезпечення їх цілісності та відповідного режиму доступу до них.

Стаття 14. Поширення персональних даних

1. Поширення персональних даних передбачає дії щодо передачі відомостей про фізичну особу за згодою суб'єкта персональних даних.

2. Поширення персональних даних без згоди суб'єкта персональних даних або уповноваженої ним особи дозволяється у випадках, визначених законом, і

лише (якщо це необхідно) в інтересах національної безпеки, економічного добробуту, прав людини та для проведення Всеукраїнського перепису населення.

3. Виконання вимог встановленого режиму захисту персональних даних забезпечує сторона, що поширює ці дані.

4. Сторона, якій передаються персональні дані, повинна попередньо вжити заходів щодо забезпечення вимог цього Закону.

Стаття 15. Видалення або знищення персональних даних

1. Персональні дані видаляються або знищуються в порядку, встановленому відповідно до вимог закону.

2. Персональні дані підлягають видаленню або знищенню у разі:

– закінчення строку зберігання даних, визначеного згодою суб'єкта персональних даних на обробку цих даних або законом;

– припинення правовідносин між суб'єктом персональних даних та володільцем чи розпорядником, якщо інше не передбачено законом;

– видання відповідного припису Уповноваженого або визначених ним посадових осіб секретаріату Уповноваженого;

– набрання законної сили рішенням суду щодо видалення або знищення персональних даних.

3. Персональні дані, зібрані з порушенням вимог цього Закону, підлягають видаленню або знищенню у встановленому законодавством порядку.

4. Персональні дані, зібрані під час виконання завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом, видаляються або знищуються відповідно до вимог закону.

Стаття 16. Порядок доступу до персональних даних

1. Порядок доступу до персональних даних третіх осіб визначається умовами згоди суб’єкта персональних даних на обробку цих даних, наданої володільцю персональних даних, або відповідно до вимог закону. Порядок доступу третіх осіб до персональних даних, які перебувають у володінні розпорядника публічної інформації, визначається Законом України "Про доступ до публічної інформації", крім даних, що отримує від інших органів центральний орган виконавчої влади, що забезпечує формування та реалізує державну фінансову та бюджетну політику, під час здійснення верифікації та моніторингу державних виплат.

2. Доступ до персональних даних третій особі не надається, якщо зазначена особа відмовляється взяти на себе зобов'язання щодо забезпечення виконання вимог цього Закону або неспроможна їх забезпечити.

3. Суб'єкт відносин, пов'язаних з персональними даними, подає запит щодо доступу (далі – запит) до персональних даних володільцю персональних даних.

4. **У запиті зазначаються**:

– прізвище, ім'я та по батькові, місце проживання (місце перебування) і реквізити документа, що посвідчує фізичну особу, яка подає запит (для фізичної особи – заявника);

– найменування, місцезнаходження юридичної особи, яка подає запит, посада, прізвище, ім'я та по батькові особи, яка засвідчує запит; підтвердження

того, що зміст запиту відповідає повноваженням юридичної особи (для юридичної особи – заявника);

– прізвище, ім'я та по батькові, а також інші відомості, що дають змогу ідентифікувати фізичну особу, стосовно якої робиться запит;

– відомості про базу персональних даних, стосовно якої подається запит, чи відомості про володільця чи розпорядника персональних даних;

– перелік персональних даних, що запитуються;

– мета та/або правові підстави для запиту.

5. **Строк вивчення запиту** на предмет його задоволення не може **перевищувати десяти робочих днів з дня його надходження**.

Протягом цього строку володілець персональних даних доводить до відома особи, яка подає запит, що запит буде задоволено або відповідні персональні дані не підлягають наданню, із зазначенням підстави, визначеної у відповідному нормативно-правовому акті.

Запит задовольняється протягом тридцяти календарних днів з дня його надходження, якщо інше не передбачено законом.

6. Суб'єкт персональних даних має право на одержання будь-яких відомостей про себе у будь-якого суб'єкта відносин, пов'язаних з персональними даними, за умови надання інформації, визначеної у пункті 1 частини четвертої цієї статті, крім випадків, установлених законом.

Стаття 17. Відстрочення або відмова у доступі до персональних даних

1. Відстрочення доступу суб'єкта персональних даних до своїх персональних даних не допускається.

2. Відстрочення доступу до персональних даних третіх осіб допускається у разі, якщо необхідні дані не можуть бути надані протягом тридцяти календарних днів з дня надходження запиту. При цьому загальний термін вирішення питань, порушених у запиті, не може перевищувати сорока п'яти календарних днів.

Повідомлення про відстрочення доводиться до відома третьої особи, яка подала запит, у письмовій формі з роз'ясненням порядку оскарження такого рішення.

У повідомленні про відстрочення зазначаються:

– прізвище, ім'я та по батькові посадової особи;

– дата відправлення повідомлення;

– причина відстрочення;

– строк, протягом якого буде задоволено запит.

3. Відмова у доступі до персональних даних допускається, якщо доступ до них заборонено згідно із законом.

У повідомленні про відмову зазначаються:

– прізвище, ім'я, по батькові посадової особи, яка відмовляє у доступі;

– дата відправлення повідомлення;

– причина відмови.

Стаття 18. Оскарження рішення про відстрочення або відмову в доступі до персональних даних

1. Рішення про відстрочення або відмову у доступі до персональних даних може бути оскаржено до Уповноваженого Верховної Ради України з прав людини або суду.

2. Якщо запит зроблено суб'єктом персональних даних щодо даних про себе, обов'язок доведення в суді законності відмови у доступі покладається на володільця персональних даних, до якого подано запит.

Стаття 19. Оплата доступу до персональних даних

1. Доступ суб'єкта персональних даних до даних про себе здійснюється безоплатно.

2. Доступ інших суб'єктів відносин, пов'язаних з персональними даними, до персональних даних певної фізичної особи чи групи фізичних осіб може бути платним у разі додержання умов, визначених цим Законом. Оплаті підлягає робота, пов'язана з обробкою персональних даних, а також робота з консультування та організації доступу до відповідних даних.

4. Органи державної влади та органи місцевого самоврядування мають право на безперешкодний і безоплатний доступ до персональних даних відповідно до їх повноважень.

Стаття 20. Зміни і доповнення до персональних даних

1. Володільці чи розпорядники персональних даних зобов'язані вносити зміни до персональних даних на підставі вмотивованої письмової вимоги суб'єкта персональних даних.

2. Володільці чи розпорядники персональних даних зобов’язані вносити зміни до персональних даних також за зверненням інших суб’єктів відносин, пов’язаних із персональними даними, якщо на це є згода суб’єкта персональних даних чи відповідна зміна здійснюється згідно з приписом Уповноваженого або визначених ним посадових осіб секретаріату Уповноваженого чи за рішенням суду, що набрало законної сили.

3. Зміна персональних даних, які не відповідають дійсності, проводиться невідкладно з моменту встановлення невідповідності.

Стаття 21. Повідомлення про дії з персональними даними

1. Про передачу персональних даних третій особі володілець персональних даних протягом десяти робочих днів повідомляє суб'єкта персональних даних, якщо цього вимагають умови його згоди або інше не передбачено законом.

2. Повідомлення, зазначені у частині першій цієї статті, не здійснюються у разі:

– передачі персональних даних за запитами при виконанні завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом;

– виконання органами державної влади та органами місцевого самоврядування своїх повноважень, передбачених законом;

– здійснення обробки персональних даних в історичних, статистичних чи наукових цілях;

– повідомлення суб’єкта персональних даних відповідно до вимог частини другої статті 12 цього Закону.

3. Про зміну, видалення чи знищення персональних даних або обмеження доступу до них володілець персональних даних протягом десяти робочих днів повідомляє суб'єкта персональних даних, а також суб'єктів відносин, пов'язаних із персональними даними, яким ці дані було передано.

Стаття 22. Контроль за додержанням законодавства про захист персональних даних

1. Контроль за додержанням законодавства про захист персональних даних у межах повноважень, передбачених законом, здійснюють такі органи:

– уповноважений;

– суди.

Стаття 24. Забезпечення захисту персональних даних

1. Володільці, розпорядники персональних даних та треті особи зобов’язані забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних.

2. В органах державної влади, органах місцевого самоврядування, а також у володільцях чи розпорядниках персональних даних, що здійснюють обробку персональних даних, яка підлягає повідомленню відповідно до цього Закону, створюється (визначається) структурний підрозділ або відповідальна особа, що організовує роботу, пов’язану із захистом персональних даних при їх обробці.

Інформація про зазначений структурний підрозділ або відповідальну особу повідомляється Уповноваженому Верховної Ради України з прав людини, який забезпечує її оприлюднення.

3. Структурний підрозділ або відповідальна особа, що організовує роботу, пов’язану із захистом персональних даних при їх обробці:

– інформує та консультує володільця або розпорядника персональних даних з питань додержання законодавства про захист персональних даних;

– взаємодіє з Уповноваженим Верховної Ради України з прав людини та визначеними ним посадовими особами його секретаріату з питань запобігання та усунення порушень законодавства про захист персональних даних.

4. Фізичні особи-підприємці, у тому числі лікарі, які мають відповідну ліцензію, адвокати, нотаріуси особисто забезпечують захист персональних даних, якими вони володіють, згідно з вимогами закону.

Стаття 28. Відповідальність за порушення законодавства про захист персональних даних

Порушення законодавства про захист персональних даних тягне за собою відповідальність, встановлену законом.

1.7. Постанова КМУ від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури

1. Ці Загальні вимоги визначають організаційно-методологічні, технічні та технологічні умови кіберзахисту об'єктів критичної інфраструктури, що є обов'язковими до виконання підприємствами, установами та організаціями, які відповідно до законодавства віднесені до об'єктів критичної інфраструктури.

2. У цих Загальних вимогах терміни вживаються у такому значенні:

– **критичні бізнес/операційні процеси об'єкта критичної інфраструктури** – процеси організації функціонування об'єктів критичної інфраструктури, реалізація загроз на які призводить до виведення з ладу або порушення функціонування самого об'єкта критичної інфраструктури та відповідно справляє негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіює майнову шкоду та/або становить загрозу для суспільства, життя і здоров'я людей; для організації функціонування цього процесу можуть використовуватися декілька інформаційно-телекомунікаційних систем;

– **система інформаційної безпеки –** сукупність організаційних та технічних заходів, а також засобів і методів захисту інформації, які впроваджуються на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури з метою запобігання кіберінцидентам, виявлення та захисту від кібератак, порушення конфіденційності, цілісності та доступності інформаційних ресурсів, що обробляються (передаються, зберігаються) на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури, запобігання порушенню режиму функціонування та/або недоступності служб (функцій) об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, порушенню функціонування компонентів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури; забезпечення спостережності за діями користувачів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури та функціонуванням засобів захисту об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

– **політика інформаційної безпеки** – політика, що визначає підхід підприємства, установи та організації, які відповідно до законодавства віднесені до об'єктів критичної інфраструктури, до інформаційної безпеки, вимоги, правила, обмеження, рекомендації, що регламентують порядок дотримання та забезпечення інформаційної безпеки.

3. Кіберзахист об'єкта критичної інфраструктури забезпечується шляхом впровадження на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури комплексної системи захисту інформації або системи інформаційної безпеки з підтвердженою відповідністю.

4. Кіберзахист об'єкта критичної інфраструктури є складовою частиною робіт із створення (модернізації) та експлуатації об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури. Заходи з

кіберзахисту передбачаються та впроваджуються на всіх стадіях життєвого циклу об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

5. Кіберзахист об'єкта критичної інфраструктури забезпечується власником та/або керівником об'єкта критичної інфраструктури відповідно до цих Загальних вимог та законодавства в сфері захисту інформації та кібербезпеки.

6. У випадку, якщо на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, положення цих Загальних вимог повинні бути враховані під час створення (модернізації) на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури комплексної системи захисту інформації, а їх відповідність перевіряється під час її державної експертизи в сфері технічного захисту інформації.

Створення комплексної системи захисту інформації об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури та її державна експертиза здійснюються відповідно до вимог законодавства в сфері захисту інформації та охорони державної таємниці.

7. У випадку, якщо на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури не обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, положення цих Загальних вимог враховуються під час створення (модернізації) системи інформаційної безпеки об'єкта критичної інфраструктури. Виконання Загальних вимог перевіряється під час незалежного аудиту інформаційної безпеки на об'єкті критичної інфраструктури.

Створення системи інформаційної безпеки об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури здійснюється відповідно до вимог технічного завдання на створення системи інформаційної безпеки.

Технічне завдання формується за результатами оцінки ризиків, які зазначаються в звіті за результатами оцінки ризиків на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури. Методичною основою для оцінки ризиків на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури є стандарт **ДСТУ ISO/IEC 27005.**

Власник та/або керівник об'єкта критичної інфраструктури організовує проведення незалежного аудиту інформаційної безпеки на об'єкті критичної інфраструктури згідно з вимогами законодавства в сфері захисту інформації та кібербезпеки.

8. Власник та/або керівник об'єкта критичної інфраструктури організовує невідкладне інформування урядової команди реагування на комп'ютерні надзвичайні події України **CERT-UA** (у разі наявності – галузевої команди реагування на комп'ютерні надзвичайні події), а також функціонального підрозділу контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Центрального управління СБУ (**Ситуаційний центр**

забезпечення кібербезпеки СБУ) або відповідного підрозділу регіонального органу СБУ про кіберінциденти та кібератаки, які стосуються його об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури.

1.8. ДСТУ 3396.0,1,2-97

ДСТУ 3396.0-96. Державний стандарт України. Захист інформації. Технічний захист інформації. Основні положення

Цей стандарт установлює об'єкт захисту, мету, основні організаційно-технічні положення технічного захисту інформації (ТЗІ), неправомірний доступ до якої може завдати шкоди громадянам, організаціям (юридичним особам) та державі, а також категорії нормативних документів з ТЗІ.

Вимоги стандарту обов'язкові для підприємств та установ усіх форм власності і підпорядкування, громадян – суб'єктів підприємницької діяльності, органів державної влади, органів місцевого самоврядування, військових частин усіх військових формувань, представництв України за кордоном, які володіють, користуються та розпоряджаються інформацією, що підлягає технічному захисту.

ДСТУ 3396.1-96. Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт

Цей стандарт установлює вимоги до порядку проведення робіт з технічного захисту інформації (ТЗІ).

Вимоги стандарту обов`язкові для підприємств та установ усіх форм власності й підпорядкування, громадян-суб`єктів підприємницької діяльності, органів державної влади, органів місцевого самоврядування, військових частин усіх військових формувань, представництв України за кордоном, які володіють, користуються та розпоряджаються інформацією, що підлягає технічному захисту.

ДСТУ 3396.2-97. Державний стандарт України. Захист інформації. Технічний захист інформації. Терміни та визначення

Цей стандарт установлює терміни та визначення понять у сфері технічного захисту інформації (ТЗІ). Терміни, регламентовані у цьому стандарті, обов'язкові для використання в усіх видах організаційної та нормативної документації, а також для робіт зі стандартизації, і рекомендовані для використання у довідковій та навчально-методичній літературі, що належить до сфери технічного захисту інформації. Терміни стандарту є обов'язковими для використання підприємствами та установами усіх форм власності і підпорядкування, громадянами – суб'єктами підприємницької діяльності, міністерствами (відомствами), центральними і місцевими органами державної виконавчої влади, військовими частинами усіх військових формувань, представництвами України за кордоном, які володіють, використовують та розпоряджаються інформацією, що становить державну чи іншу передбачену законом таємницю або є конфіденційною інформацією, яка належить державі.

1.9. ДСТУ ISO/IEC 15408-1:2017

ISO/IEC 15408-1:2022. Інформаційна безпека, кібербезпека та захист конфіденційності. Критерії оцінки IT-безпеки. Частина 1. Вступ і загальна модель

Цей документ встановлює загальні концепції та принципи оцінювання безпеки IT і визначає загальну модель оцінювання, що надається різними частинами стандарту, який у цілому призначений для використання в якості основи для оцінки властивостей безпеки IT-продуктів.

Цей документ містить огляд усіх частин серії ISO/IEC 15408. Він описує різні частини серії ISO/IEC 15408; визначає терміни та скорочення, які слід використовувати в усіх частинах стандарту; встановлює основну концепцію мети оцінювання (TOE); описує контекст оцінювання та описує аудиторію, якій адресовані критерії оцінювання. Дано вступ до основних концепцій безпеки, необхідних для оцінки IT-продуктів.

Цей документ представляє:

– ключові поняття профілів захисту (PP), модулів PP, конфігурацій PP, пакетів, цілей безпеки (ST) і типів відповідності;

– опис організації компонентів безпеки по всій моделі;

– різні операції, за допомогою яких функціональні компоненти та компоненти гарантії, наведені в ISO/IEC 15408-2 та ISO/IEC 15408-3, можуть бути налаштовані шляхом використання дозволених операцій;

– загальну інформацію про методи оцінювання, наведені в ISO/IEC 18045;

– настанова щодо застосування ISO/IEC 15408-4 для розробки методів оцінювання (EM) і діяльності з оцінювання (EA), виведених із ISO/IEC 18045;

– загальну інформацію про попередньо визначені рівні гарантії оцінювання (EAL), визначені в ISO/IEC 15408-5;

– інформація щодо обсягу схем оцінювання.

1.10. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу»

Цей документ установлює терміни і визначення понять у галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу.

Терміни, що установлюються цим документом, обов’язкові для застосування в усіх видах документації і літератури, що входять до системи технічного захисту інформації.

Для кожного поняття встановлено один термін. Застосування синонімів терміна не допускається.

Для довідки наведені іноземні еквіваленти термінів, що запроваджуються, а також алфавітні покажчики термінів.

1.11. НД ТЗІ 2.5-004-99. «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»

Цей нормативний документ (далі – Критерії) – установлює критерії оцінки захищеності інформації, оброблюваної в комп'ютерних системах, від несанкціонованого доступу.

Критерії є методологічною базою для визначення вимог з захисту інформації в комп'ютерних системах від несанкціонованого доступу; створення захищених комп'ютерних систем і засобів захисту від несанкціонованого доступу; оцінки захищеності інформації в комп'ютерних системах і їх придатності для обробки критичної інформації (інформації, що вимагає захисту).

Критерії надають:

1. Порівняльну шкалу для оцінки надійності механізмів захисту інформації від несанкціонованого доступу, реалізованих в комп'ютерних системах.

2. Базу (орієнтири) для розробки комп'ютерних систем, в яких мають бути реалізовані функції захисту інформації.

Критерії можуть застосовуватися до всього спектра комп'ютерних систем, включаючи однорідні системи, багатопроцесорні системи, бази даних, вбудовані системи, розподілені системи, мережі, об'єктно-орієнтовані системи та ін.

Цей документ призначено для постачальників (розробників), споживачів (замовників, користувачів) комп'ютерних систем, які використовуються для обробки (в тому числі збирання, зберігання, передачі і т. ін.) критичної інформації, а також для органів, що здійснюють функції оцінювання захищеності такої інформації та контролю за її обробкою.

Цей документ відображає сучасний стан проблеми і підходів до її розв'язання. З розвитком нових тенденцій в галузі і за умови достатньої обгрунтованості документ є відкритим для включення до його складу Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України нових послуг.

1.12. Закон України «Про доступ до публічної інформації»

Цей Закон визначає порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом, та інформації, що становить суспільний інтерес, та складається з наступних розділів і статей.

Розділ І. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Публічна інформація

Стаття 2. Мета і сфера дії Закону

Стаття 3. Гарантії забезпечення права на доступ до публічної інформації

Стаття 4. Принципи забезпечення доступу до публічної інформації

ІІ. ПОРЯДОК ДОСТУПУ ДО ІНФОРМАЦІЇ
Стаття 5. Забезпечення доступу до інформації
Стаття 6. Публічна інформація з обмеженим доступом
Стаття 7. Конфіденційна інформація
Стаття 8. Таємна інформація
Стаття 9. Службова інформація
Стаття 10. Доступ до інформації про особу
Стаття 10. Публічна інформація у формі відкритих даних
Стаття 11. Захист особи, яка оприлюднює інформацію
Розділ ІІІ. СУБ'ЄКТИ ВІДНОСИН У СФЕРІ ДОСТУПУ ДО ПУБЛІЧНОЇ ІНФОРМАЦІЇ
Стаття 12. Визначення та перелік суб'єктів
Стаття 13. Розпорядники інформації
Стаття 14. Обов'язки розпорядників інформації
Стаття 15. Оприлюднення інформації розпорядниками
Стаття 16. Відповідальні особи з питань доступу до публічної інформації
Стаття 17. Контроль за забезпеченням доступу до публічної інформації
Стаття 18. Реєстрація документів розпорядника інформації
Розділ IV. РЕАЛІЗАЦІЯ ПРАВА НА ДОСТУП ДО ІНФОРМАЦІЇ ЗА ІНФОРМАЦІЙНИМ ЗАПИТОМ
Стаття 19. Оформлення запитів на інформацію
Стаття 20. Строк розгляду запитів на інформацію
Стаття 21. Плата за надання інформації
Стаття 22. Відмова та відстрочка в задоволенні запиту на інформацію
Розділ V. ОСКАРЖЕННЯ РІШЕНЬ, ДІЙ ЧИ БЕЗДІЯЛЬНОСТІ РОЗПОРЯДНИКІВ ІНФОРМАЦІЇ
Стаття 23. Право на оскарження рішень, дій чи бездіяльності розпорядників інформації
Стаття 24. Відповідальність за порушення законодавства про доступ до публічної інформації

Розділ І. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Публічна інформація

1. **Публічна інформація** – це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом.

2. Публічна інформація є відкритою, крім випадків, встановлених законом.

Стаття 3. Гарантії забезпечення права на доступ до публічної інформації

1. **Право на доступ до публічної інформації** гарантується:

– обов'язком розпорядників інформації надавати та оприлюднювати інформацію, крім випадків, передбачених законом;

– визначенням розпорядником інформації спеціальних структурних підрозділів або посадових осіб, які організовують у встановленому порядку доступ до публічної інформації, якою він володіє;

– максимальним спрощенням процедури подання запиту та отримання інформації;

– доступом до засідань колегіальних суб'єктів владних повноважень, крім випадків, передбачених законодавством;

– здійсненням парламентського, громадського та державного контролю за дотриманням прав на доступ до публічної інформації;

– юридичною відповідальністю за порушення законодавства про доступ до публічної інформації.

Стаття 4. Принципи забезпечення доступу до публічної інформації

1. Доступ до публічної інформації відповідно до цього Закону здійснюється на принципах:

– прозорості та відкритості діяльності суб'єктів владних повноважень;

– вільного отримання, поширення та будь-якого іншого використання інформації, що була надана або оприлюднена відповідно до цього Закону, крім обмежень, встановлених законом;

– рівноправності, незалежно від ознак раси, політичних, релігійних та інших переконань, статі, етнічного та соціального походження, майнового стану, місця проживання, мовних або інших ознак.

Розділ ІІ. ПОРЯДОК ДОСТУПУ ДО ІНФОРМАЦІЇ

Стаття 5. Забезпечення доступу до інформації

1. Доступ до інформації забезпечується шляхом:

1) систематичного та оперативного оприлюднення інформації:

– в офіційних друкованих виданнях;

– на офіційних веб-сайтах в мережі Інтернет;

– на єдиному державному веб-порталі відкритих даних;

– на інформаційних стендах;

– будь-яким іншим способом;

2) надання інформації за запитами на інформацію.

Стаття 6. Публічна інформація з обмеженим доступом

1. Інформацією з обмеженим доступом є:

– конфіденційна інформація;

– таємна інформація;

– службова інформація.

2. Обмеження доступу до інформації здійснюється відповідно до закону при дотриманні сукупності таких вимог:

– виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи кримінальним

правопорушенням, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя;

– розголошення інформації може завдати істотної шкоди цим інтересам;

– шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

3. Інформація з обмеженим доступом має надаватися розпорядником інформації, якщо він правомірно оприлюднив її раніше.

4. Інформація з обмеженим доступом має надаватися розпорядником інформації, якщо немає законних підстав для обмеження у доступі до такої інформації, які існували раніше.

6. Не належать до інформації з обмеженим доступом відомості, зазначені у декларації особи, уповноваженої на виконання функцій держави або місцевого самоврядування, поданій відповідно до Закону України "Про запобігання корупції", крім випадків, визначених зазначеним Законом.

7. Не належить до інформації з обмеженим доступом інформація про структуру, принципи формування та розмір оплати праці, винагороди, додаткового блага керівника, заступника керівника юридичної особи публічного права, керівника, заступника керівника, члена наглядової ради державного чи комунального підприємства або державної чи комунальної організації, що має на меті одержання прибутку, особи, яка постійно або тимчасово обіймає посаду члена виконавчого органу чи входить до складу наглядової ради господарського товариства, у статутному капіталі якого більше 50 відсотків акцій (часток, паїв) прямо чи опосередковано належать державі та/або територіальній громаді.

8. Обмеженню доступу підлягає інформація, а не документ. Якщо документ містить інформацію з обмеженим доступом, для ознайомлення надається інформація, доступ до якої необмежений.

Стаття 7. Конфіденційна інформація

1. **Конфіденційна інформація** – інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов. Не може бути віднесена до конфіденційної інформація, зазначена в частині першій і другій статті 13 цього Закону.

Стаття 8. Таємна інформація

1. **Таємна інформація** – інформація, доступ до якої обмежується відповідно до частини другої статті 6 цього Закону, розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську, розвідувальну таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю.

Стаття 9. Службова інформація

1. Відповідно до вимог частини другої статті 6 цього Закону до службової може належати така інформація:

– що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або

здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

– зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

2. Документам, що містять інформацію, яка становить службову інформацію, присвоюється гриф **"для службового користування"**. Доступ до таких документів надається відповідно до частини другої статті 6 цього Закону.

Стаття 10. Доступ до інформації про особу

1. Кожна **особа має право**:

– знати у період збирання інформації, але до початку її використання, які відомості про неї та з якою метою збираються, як, ким і з якою метою вони використовуються, передаються чи поширюються, крім випадків, встановлених законом;

– доступу до інформації про неї, яка збирається та зберігається;

– вимагати виправлення неточної, неповної, застарілої інформації про себе, знищення інформації про себе, збирання, використання чи зберігання якої здійснюється з порушенням вимог закону;

– на ознайомлення за рішенням суду з інформацією про інших осіб, якщо це необхідно для реалізації та захисту прав та законних інтересів;

– на відшкодування шкоди у разі розкриття інформації про цю особу з порушенням вимог, визначених законом.

2. Обсяг інформації про особу, що збирається, зберігається і використовується розпорядниками інформації, має бути максимально обмеженим і використовуватися лише з метою та у спосіб, визначений законом.

3. Розпорядники інформації, які володіють інформацією про особу, зобов'язані:

– надавати її безперешкодно і безкоштовно на вимогу осіб, яких вона стосується, крім випадків, передбачених законом;

– використовувати її лише з метою та у спосіб, визначений законом;

– вживати заходів щодо унеможливлення несанкціонованого доступу до неї інших осіб;

4) виправляти неточну та застарілу інформацію про особу самостійно або на вимогу осіб, яких вона стосується.

4. Зберігання інформації про особу не повинно тривати довше, ніж це необхідно для досягнення мети, задля якої ця інформація збиралася.

5. Відмова особі в доступі до інформації про неї, приховування, незаконне збирання, використання, зберігання чи поширення інформації можуть бути оскаржені.

Стаття 10. Публічна інформація у формі відкритих даних

1. **Публічна інформація у формі відкритих даних** – це публічна інформація у форматі, що дозволяє її автоматизоване оброблення електронними засобами, вільний та безоплатний доступ до неї, а також її подальше використання.

Розділ ІІІ. СУБ'ЄКТИ ВІДНОСИН У СФЕРІ ДОСТУПУ ДО ПУБЛІЧНОЇ ІНФОРМАЦІЇ

Стаття 12. Визначення та перелік суб'єктів

1. **Суб'єктами** відносин у сфері доступу до публічної інформації є:

– **запитувачі інформації** – фізичні, юридичні особи, об'єднання громадян без статусу юридичної особи, крім суб'єктів владних повноважень;

– **розпорядники інформації** – суб'єкти, визначені у статті 13 цього Закону;

– **структурний підрозділ або відповідальна особа з питань доступу до публічної інформації розпорядників інформації**.

Стаття 13. Розпорядники інформації

1. **Розпорядниками інформації** для цілей цього Закону визнаються:

– **суб'єкти владних повноважень** – органи державної влади, інші державні органи, органи місцевого самоврядування, органи влади Автономної Республіки Крим, інші суб'єкти, що здійснюють владні управлінські функції відповідно до законодавства та рішення яких є обов'язковими для виконання;

– **юридичні особи, що фінансуються з державного, місцевих бюджетів, бюджету Автономної Республіки Крим**, – стосовно інформації щодо використання бюджетних коштів;

– **особи, якщо вони виконують делеговані повноваження суб'єктів владних повноважень згідно із законом чи договором, включаючи надання освітніх, оздоровчих, соціальних або інших державних послуг**, – стосовно інформації, пов'язаної з виконанням їхніх обов'язків;

– **суб'єкти господарювання, які займають домінуюче становище на ринку або наділені спеціальними чи виключними правами, або є природними монополіями**, – стосовно інформації щодо умов постачання товарів, послуг та цін на них;

– **юридичні особи публічного права, державні/комунальні підприємства або державні/комунальні організації, що мають на меті одержання прибутку, господарські товариства, у статутному капіталі яких більше 50 відсотків акцій (часток, паїв) прямо чи опосередковано належать державі та/або територіальній громаді**, – щодо інформації про структуру, принципи формування та розмір оплати праці, винагороди, додаткового блага їх керівника, заступника керівника, особи, яка постійно або тимчасово обіймає посаду члена виконавчого органу чи входить до складу наглядової ради.

Стаття 14. Обов'язки розпорядників інформації

1. Розпорядники інформації зобов'язані:

– оприлюднювати інформацію, передбачену цим та іншими законами;

– систематично вести облік документів, що знаходяться в їхньому володінні;

– вести облік запитів на інформацію;

– визначати спеціальні місця для роботи запитувачів з документами чи їх копіями, а також надавати право запитувачам робити виписки з них, фотографувати, копіювати, сканувати їх, записувати на будь-які носії інформації тощо;

– мати спеціальні структурні підрозділи або призначати відповідальних осіб для забезпечення доступу запитувачів до інформації та оприлюднення інформації;

– надавати та оприлюднювати достовірну, точну та повну інформацію, а також у разі потреби перевіряти правильність та об'єктивність наданої інформації і оновлювати оприлюднену інформацію.

Розділ IV. РЕАЛІЗАЦІЯ ПРАВА НА ДОСТУП ДО ІНФОРМАЦІЇ ЗА ІНФОРМАЦІЙНИМ ЗАПИТОМ

Стаття 19. Оформлення запитів на інформацію

1. **Запит на інформацію** – це прохання особи до розпорядника інформації надати публічну інформацію, що знаходиться у його володінні.

2. Запитувач має право звернутися до розпорядника інформації із запитом на інформацію незалежно від того, стосується ця інформація його особисто чи ні, без пояснення причини подання запиту.

3. Запит на інформацію може бути індивідуальним або колективним. Запити можуть подаватися в усній, письмовій чи іншій формі (поштою, факсом, телефоном, електронною поштою) на вибір запитувача.

4. Письмовий запит подається в довільній формі.

5. Запит на інформацію має містити:

– ім'я (найменування) запитувача, поштову адресу або адресу електронної пошти, а також номер засобу зв'язку, якщо такий є;

– загальний опис інформації або вид, назву, реквізити чи зміст документа, щодо якого зроблено запит, якщо запитувачу це відомо;

– підпис і дату за умови подання запиту в письмовій формі.

6. З метою спрощення процедури оформлення письмових запитів на інформацію особа може подавати запит шляхом заповнення відповідних форм запитів на інформацію, які можна отримати в розпорядника інформації та на офіційному веб-сайті відповідного розпорядника. Зазначені форми мають містити стислу інструкцію щодо процедури подання запиту на інформацію, її отримання тощо.

7. У разі якщо з поважних причин (інвалідність, обмежені фізичні можливості тощо) особа не може подати письмовий запит, його має оформити відповідальна особа з питань доступу до публічної інформації, обов'язково зазначивши в запиті своє ім'я, контактний телефон, та надати копію запиту особі, яка його подала.

Стаття 20. Строк розгляду запитів на інформацію

1. Розпорядник інформації має надати відповідь на запит на інформацію **не пізніше п'яти робочих днів** з дня отримання запиту.

2. У разі якщо запит на інформацію стосується інформації, необхідної для захисту життя чи свободи особи, щодо стану довкілля, якості харчових продуктів і предметів побуту, аварій, катастроф, небезпечних природних явищ та інших надзвичайних подій, що сталися або можуть статись і загрожують безпеці громадян, відповідь має бути надана **не пізніше 48 годин** з дня отримання запиту.

3. Клопотання про термінове опрацювання запиту має бути обґрунтованим.

4. У разі якщо запит стосується надання великого обсягу інформації або потребує пошуку інформації серед значної кількості даних, розпорядник інформації може **продовжити строк розгляду запиту до 20 робочих днів** з обґрунтуванням такого продовження. Про продовження строку розпорядник інформації повідомляє запитувача в письмовій формі не пізніше п'яти робочих днів з дня отримання запиту.

Стаття 21. Плата за надання інформації

1. Інформація на запит надається безкоштовно.

2. У разі якщо задоволення запиту на інформацію передбачає виготовлення копій документів обсягом **більш як 10 сторінок, запитувач зобов'язаний відшкодувати фактичні витрати на копіювання та друк**.

3. Розмір фактичних витрат визначається відповідним розпорядником на копіювання та друк в межах граничних норм, встановлених Кабінетом Міністрів України. У разі якщо розпорядник інформації не встановив розміру плати за копіювання або друк, інформація надається безкоштовно.

4. При наданні особі інформації про себе та інформації, що становить суспільний інтерес, плата за копіювання та друк не стягується.

Стаття 22. Відмова та відстрочка в задоволенні запиту на інформацію

1. Розпорядник інформації має право відмовити в задоволенні запиту в таких випадках:

1) розпорядник інформації не володіє і не зобов'язаний відповідно до його компетенції, передбаченої законодавством, володіти інформацією, щодо якої зроблено запит;

2) інформація, що запитується, належить до категорії інформації з обмеженим доступом відповідно до частини другої статті 6 цього Закону;

3) особа, яка подала запит на інформацію, не оплатила передбачені статтею 21 цього Закону фактичні витрати, пов'язані з копіюванням або друком;

4) не дотримано вимог до запиту на інформацію, передбачених частиною п'ятою статті 19 цього Закону.

2. Відповідь розпорядника інформації про те, що інформація може бути одержана запитувачем із загальнодоступних джерел, або відповідь не за суттю запиту вважається неправомірною відмовою в наданні інформації.

3. Розпорядник інформації, який не володіє запитуваною інформацією, але якому за статусом або характером діяльності відомо або має бути відомо, хто нею володіє, зобов'язаний направити цей запит належному розпоряднику з одночасним повідомленням про це запитувача. У такому разі відлік строку розгляду запиту на інформацію починається з дня отримання запиту належним розпорядником.

4. У відмові в задоволенні запиту на інформацію має бути зазначено:

– прізвище, ім'я, по батькові та посаду особи, відповідальної за розгляд запиту розпорядником інформації;

– дату відмови;

– мотивовану підставу відмови;

– порядок оскарження відмови;

– підпис.

5. Відмова в задоволенні запиту на інформацію надається в письмовій формі.

6. Відстрочка в задоволенні запиту на інформацію допускається в разі, якщо запитувана інформація не може бути надана для ознайомлення в передбачені цим Законом строки у разі настання обставин непереборної сили. Рішення про відстрочку доводиться до відома запитувача у письмовій формі з роз'ясненням порядку оскарження прийнятого рішення.

7. У рішенні про відстрочку в задоволенні запиту на інформацію має бути зазначено:

– прізвище, ім'я, по батькові та посаду особи, відповідальної за розгляд запиту розпорядником інформації;

– дату надсилання або вручення повідомлення про відстрочку;

– причини, у зв'язку з якими запит на інформацію не може бути задоволений у встановлений цим Законом строк;

– строк, у який буде задоволено запит;

– підпис.

1.13. Загрози, яким підлягає інформація

Як показує аналіз, сучасні комп’ютерні системи підлягають наступним найбільш розповсюдженим загрозам:

– ненавмисні помилки користувачів, операторів, системних адміністраторів і інших осіб (65%)

– крадіжки і фальсифікація В більшості випадків, що розслідувалися, винними виявлялися штатні співробітники організацій, відмінно знайомі із режимом роботи і мірами захисту;

– “ображені співробітники” – нинішні і колишні, наприклад, шляхом вживляння “логічної бомби”, введення невірних даних, вилучення або модифікації даних;

– загрози від навколишньої середи (відключення зв’язку, пожежа і т.і.);

– дії хакерів і злочинців, що можуть здійснювати обман шляхом створення неправдивих або модифікованих справжніх документів (інформації).

1.14. Стратегії реалізації загроз

В процесі реалізації загроз порушники і злочинці можуть реалізовувати наступні стратегії:

1. Видавання себе за іншого користувача, щоб зняти з себе відповідальність.

2. Видавання себе за іншого користувача, щоб використовувати його повноваження з метою:

– формування неправдивої інформації;

– зміни істинної інформації;

– застосування неправдивого посвідчення для отримання несанкціонованого доступу (НСД);

– санкціонування неправдивих обмінів інформацією або іхнє підтвердження.

3. Відмова джерела від факту формування і передачі інформації.

4. Твердження джерела про те, що одержувачу була відправлена інформація, в тому числі в певний час, що насправді не була відправлена або відправлена в інший час.

5. Відмова отримувача від факту отримання інформації, хоча насправді вона була отримана, або неправдиве затвердження про час її отримання.

6. Твердження про те, що інформація отримана від певного користувача, хоча насправді вона сформована самим же порушником.

7. Отримання НСД, тобто порушення конфіденційності інформації, що захищається.

8. Несанкціоноване розширення (зміна) своїх повноважень.

9. Несанкціонована зміна повноважень інших осіб (обмеження або розширення).

10. Введення в систему або активізація вірусів або інших “шкідливих” програм з метою перехоплення ключів і паролів, а також модифікації (непомітно) документів.

11. Спроба завадити передачі повідомлень між іншими користувачами, в частковості, внесення до повідомлення прихованих завад для того, щоб це повідомлення при автентифікації було спростоване.

12. Модифікація програмного забезпечення, наприклад, шляхом додання нових функцій.

13. Підрив довіри до протоколу шляхом виклику порушень або примушення інших порушити протокол шляхом введення неправдивої інформації і т.і.

1.15. Основні міри протидії загрозам безпеці, принципи побудови систем захисту, основні механізми захисту

Перекриття більшості названих загроз може бути здійснено за рахунок формування і проведення в життя **політики безпеки** – набору законів, правил і норм поведінки, які визначають те, як ІКС обробляє, захищає і розповсюджує інформацію. За суттю **політика безпеки** – це активний компонент захисту, що включає в себе аналіз можливих загроз і вибір мір протидії. В практичному додатку політика безпеки являє собою сукупність документованих управлінських рішень, направлених на захист інформації і асоційованих з нею ресурсів. В результаті реалізації такої політики повинна бути створена система

захисту інформації, що являє собою комплекс організаційних, технічних засобів і заходів, юридичних, законодавчих норм, фізичних обмежень й т.і., які реалізуються комплексно на всіх етапах життєвого циклу інформаційної системи: від проектування – і до застосування в різноманітних умовах.

В системах захисту інформації (СЗІ) повинні реалізовуватися функції безпеки і механізми безпеки; вони повинні перекривати всі виявлені загрози, перераховані вище.

1.16. Перелік основних задач, які повинні вирішуватися системою комп'ютерної безпеки:

– керування доступом користувачів до ресурсів ІКС, з метою її захисту від неправомірного випадкового або навмисного втручання у роботу системи і несанкціонованого (із перевищенням наданих повноваженнь) доступу до її інформаційних, програмних і апаратних ресурсів із боку сторонніх осіб, а також осіб із числа персоналу організації і користувачів;

– захист даних, що передаються по каналам зв'язку;

– реєстрація, збір, збереження, опрацювання і видача даних про усі події, що відбувалися у системі і мали відношення до її безпеки;

– контроль роботи користувачів системи з боку адміністрації і оперативне оповіщення адміністратора безпеки про спроби несанкціонованого доступу до ресурсів системи;

– контроль і підтримка цілісністності критичних ресурсів системи захисту і середовища виконання прикладних програм;

– забезпечення замкнутого середовища перевіреного програмного забезпечення, із метою захисту від безконтрольного впровадження у систему потенційно небезпечних програм (у яких можуть міститись вредоносні закладки або небезпечні помилки) і засобів подолання системи захисту, а також від впровадження і поширення комп'ютерних вірусів;

– керування засобами системи захисту.

Зазвичай розрізняють зовнішню і внутрішню безпеку комп'ютерних систем. **Зовнішня безпека** включає захист ІКС від стихійного лиха (пожежі, повені і т.п.) і від проникнення у систему зловмисника ззовні з цілями розкрадання, одержання доступу до інформації або виводу системи з ладу. **Внутрішня безпека** – створення надійних і зручних механізмів регламентації діяльністі усіх її законних користувачів і обслуговуючого персоналу для примусу їх до безумовного дотримання встановлених в організації дисципліни доступу до ресурсів системи.

Міри протидії погрозам безпеки. Класифікація мір забезпечення безпеки комп'ютерних систем

За способом здійснення усі міри забезпечення безпеки комп'ютерних систем підрозділяються на: правові (законодавчі), морально-етичні, організаційні (адміністративні), фізичні і технічні (апаратурні і програмні).

До **правових** мір захисту відносяться діючі у країні закони, укази і нормативні акти, що регламентують правила роботи з інформацією

До **морально-етичних** мір протидії відносяться норми поводження, що традиційно склались або складаються у міру поширення ЕОМ у країні або суспільстві.

Організаційні (адміністративні) міри захисту – це міри організаційного характеру, що регламентують процес функціонування системи опрацювання даних, використання її ресурсів, діяльність персоналу, а також порядок взаємодії користувачів з системою таким чином, щоб найбільшою мірою утруднити або виключити можливість реалізації погроз безпеки.

Фізичні міри захисту засновані на застосуванні різного роду механічних, електро- або електронно-механічних пристроїв і споруджень, спеціально призначених для створення фізичних перешкод на можливих шляхах проникнення і доступу потенційних порушників до компонент системи і захищаємої інформації, а також технічні засоби візуального спостереження, зв'язку і охоронної сигналізації.

Технічні (апаратно-програмні) міри захисту засновані на використанні різних електронних пристроїв і спеціальних програм, що входять до складу ІКС і виконують (самостійно або в комплексі з іншими засобами) функції захисту (ідентифікацію й автентифікацію користувачів, розмежування доступу до ресурсів, реєстрацію подій, криптографічне закриття інформації і т.д.)

1.17. Основні принципи побудови систем захисту інформаційно-комунікаційних систем (ІКС)

Захист інформації в ІКС повинний ґрунтуватися на наступних основних принципах:

- системності,
- комплексності;
- безперервності захисту;
- розумної достатності;
- гнучкості керування і застосування:
- відкритості алгоритмів і механізмів захисту;
- простоти застосування захисних мір і засобів.

Принцип системності

Системний підхід припускає необхідність обліку усіх взаємозалежних, взаємодіючих і елементів, умов і чинників, які змінюються в ІКС, значимих для розуміння і рішення проблеми забезпечення безпеки ІКС.

Принцип комплексності

У розпорядженні фахівців із комп'ютерної безпеки є широкий спектр мір, методів і засобів захисту комп'ютерних систем. Комплексне їхнє використання припускає погоджене застосування різнорідних засобів при побудові цілісної

системи захисту, що перекриває всі істотні канали реалізації погроз і не має слабких місць на стиках окремих її компонентів**.**

Принцип безперервності захисту

Захист інформації – це безупинний цілеспрямований процес, що припускає прийняття відповідних мір на всіх етапах життєвого циклу ІКС, починаючи із самих ранніх стадій проектування, а не тільки на етапі її експлуатації**.**

Розумна достатність

Створити абсолютно непереборну систему захисту принципово неможливо. При достатній кількості методів і засобів можна перебороти будь-який захист. Тому має сенс вести мову тільки про деякий прийнятний рівень безпеки.

Гнучкість системи захисту

Для забезпечення можливості варіювання рівнем захищеності, засоби захисту повинні мати визначену гнучкість. Особливо важливим ця властивість є в тих випадках, коли установку засобів захисту необхідно здійснювати на працюючу систему, не порушуючи процесу її нормального функціонування.

Відкритість алгоритмів і механізмів захисту

Суть принципу відкритості алгоритмів і механізмів захисту перебуває в тому, що захист не повинний забезпечуватися тільки за рахунок таємності структурної організації й алгоритмів функціонування її підсистем

Принцип простоти застосування засобів захисту

Механізми захисту повинні бути інтуїтивно зрозумілі і прості у використанні. Застосування засобів захисту не повинно бути зв'язане зі знанням спеціальних мов або з виконанням дій, що вимагають значних додаткових працезатрат при звичайній роботі законних користувачів, а також не повинно жадати від користувача виконання рутинних малозрозумілих йому операцій (введення кількох паролів і імен і т.д.).

Основні механізми захисту комп'ютерних систем від проникнення з метою дезорганізації їхньої роботи і НСД до інформації

Затвердимо ряд понять, необхідних надалі.

1. Об'єкт – пасивний компонент системи, одиниця ресурсу автоматизованої системи (пристрій, диск, каталог, файл і т.п.), доступ до якого регламентується правилами розмежування доступу.

2. Суб'єкт – активний компонент системи (користувач, процес, програма), дії якого регламентуються правилами розмежування доступу.

3. Доступ до інформації – ознайомлення з інформацією, (копіювання, тиражування), її модифікація (корректировка) або знищення (видалення).

4. Доступ до ресурсу – одержання суб'єктом можливості маніпулювати (використовувати, управляти, змінювати характеристики і т.п.) даним ресурсом.

5. Правила розмежування доступу – сукупність правил, що регламентують права доступу суб'єктів до об'єктів у деякій системі.

6. Розмежування доступу до ресурсів ІКС – це такий порядок використання ресурсів автоматизованої системи, при якому суб'єкти одержують доступ до об'єктів у суворій відповідності з установленими правилами.

7. Авторизований суб'єкт доступу – суб'єкт, якому надані відповідні права доступу до об'єктів системи (повноваження).

8. Несанкціонований доступ (НСД) – доступ суб'єкта до об'єкта в порушення встановлених у системі правил розмежування доступу.

9. Несанкціонована дія – дія суб'єкта в порушення встановлених у системі правил обробки інформації.

Для реалізації наведених вище мір захисту комп'ютерних систем використовуються **універсальні механізми захисту інформації**. До числа таких механізмів відносяться:

- ідентифікація (найменування і впізнання), автентифікація (підтвердження істинності) і авторизація (присвоєння повноважень) суб'єктів;
- контроль (розмежування) доступу до ресурсів системи;
- реєстрація й аналіз подій, що відбуваються в системі;
- контроль цілісності ресурсів системи.

Механізми ідентифікації, автентифікації й авторизації необхідні для підтвердження істинності суб'єкта, забезпечення його роботи в системі, і визначення законності прав суб'єкта на даний об'єкт або на визначені дії з ним.

Ідентифікація – це процес розпізнавання елемента системи, зазвичай за допомогою заздалегідь визначеного ідентифікатора або іншої унікальної інформації; кожний суб'єкт або об'єкт системи повинний бути однозначно ідентифікуємим.

Автентифікація – це перевірка істинності ідентифікації користувача, процесу, пристрою або іншого компоненту системи (звичайно здійснюється перед дозволом доступу); а також перевірка цілісності й авторства даних при їхньому збереженні або передачі для запобігання несанкціонованої модифікації.

Авторизація – це надання суб'єкту прав на доступ до об'єкта.

Приведемо приклад з доступом в онлайн-банкінг. Кожну дію користувача й системи розглянемо докладно.

Перебуваючи на сайті банку, користувач вирішує зайти в особистий кабінет, щоб зробити грошовий переказ. На сторінці особистого кабінету система спочатку просить ввести ідентифікатор. Це може бути логін, ім'я й прізвище, адреса електронної пошти або номер мобільного телефону.

Який конкретно вид даних необхідно ввести – залежить від ресурсу. Дані, які вказувалися при реєстрації, необхідно ввести для одержання доступу. Якщо при реєстрації вказувалося кілька типів даних – і логін, і адреса електронної пошти, і номер мобільного, то система сама підкаже що їй конкретно потрібно.

Введення цих даних необхідний для ідентифікації людини за монітором як користувача конкретно цього банку.

Якщо користувач як ідентифікатор увів «Олександр Ковальчук», і система знайшла у своїй базі запис про користувача з таким іменем, то ідентифікація завершилася.

Після ідентифікації випливає процес автентифікації, у якому користувачеві потрібно довести, що він є людиною, яка реєструвалася під іменем Олександр Ковальчук.

Для доказу необхідна наявність одного з типів автентифікаційних даних:

- Щось, властиве тільки користувачеві. Біометричні дані: сканери особи, відбитки пальців або сітківки ока.
- Щось, відоме тільки користувачеві. Сюди ставляться pin-коди, паролі, графічні ключі, секретні слова.
- Щось, наявне в користувача. У даній якості може виступати токен, тобто компактний пристрій, призначене для забезпечення інформаційної безпеки користувача, також використовується для ідентифікації власника. Найпростіші токени не вимагають фізичного підключення до комп'ютера – у них є дисплей, де відображається число, яке користувач уводить у систему для здійснення входу; більш складні підключаються до комп'ютерів за допомогою USB і Bluetooth-Інтерфейсів.

Найпоширеніший тип автентифікаційних даних – це пароль. Саме тому так важливо створювати й правильно зберігати свої паролі.

Після введення користувачем пароля система перевіряє: чи відповідає умовний пароль «Q45fp02@13» користувачеві з іменем Олександр Ковальчук. У такий спосіб відбувається автентифікація.

Якщо всі вірно, і пари логін-пароль вірні, то система надасть користувачеві доступ до його ресурсів і здійснення банківських операцій, тобто відбудеться авторизація.

Описані процеси завжди відбуваються тільки в такому порядку: ідентифікація, автентифікація, авторизація. Увесь ланцюжок втратить зміст, якщо, наприклад, сайт спочатку надасть доступ до коштів користувача, а потім буде уточнювати, чи він це насправді.

Процеси ідентифікації, автентифікації й авторизації характерні не тільки для онлайн-банкінгу, але й для електронної пошти, соціальних мереж і інших ресурсів.

Розділ 2. Міжнародні стандарти в галузі інформаційної та /або кібербезпеки

2.1. Регламенти ЄС в галузі кібербезпеки: Регламент Європейського Парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року «Про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій»

2.2. ДСТУ ISO 27001, ISO 27002, ISO 27003

2.3. ISO/IEC 15408- 2, ISO/IEC 15408-3

2.4. Стек протоколів ДСТУ ISO/IEC 27000

Кібернапади – це найбільші ризики, з якими може стикнутися будь-яка організація. За даними глобального огляду, проведеного об'єднанням ISACA тільки 38% респондентів вважають, що вони підготовлені до кібернападів, решта 83% відносять кібернапади до одною з найнебезпечніших загроз для організації. За наявності великого обсягу персональної та конфіденційної інформації, яку пересилають за допомогою електронних засобів, несанкціонований доступ до неї може спричинити серйозні наслідки.

Система кібербезпеки – набір засобів, стратегій, принципів забезпечення безпеки, гарантій безпеки, підходів до управління ризиками, дій, професійної підготовки, страхування і технологій, які використовуються для захисту кіберсереди, ресурсів організацій і користувачів.

Основними завданнями кібербезпеки вважаються забезпечення: конфіденційності доступності, а також цілісності, що включає автентичність. Кібербезпека є необхідною умовою розвитку інформаційного суспільства.

2.1 Регламенти ЄС в галузі кібербезпеки: Регламент Європейського Парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року «Про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій»

ENISA – Агентство Європейського Союзу з питань мережевої та інформаційної безпеки. Агентство Європейського Союзу з кібербезпеки, ENISA, є агентством Союзу, яке займається досягненням високого загального рівня кібербезпеки в Європі. Агентство Європейського Союзу з кібербезпеки, засноване в 2004 році та посилене Актом про кібербезпеку ЄС, сприяє кіберполітиці ЄС, підвищує надійність продуктів, послуг і процесів інформаційно-комунікаційних технологій (ІКТ) за допомогою схем сертифікації кібербезпеки, співпрацює з державами-членами та органами ЄС і допомагає Європі підготуватися для кібервикликів завтрашнього дня. Завдяки обміну знаннями, розбудові потенціалу та підвищенню обізнаності Агентство співпрацює зі своїми ключовими зацікавленими сторонами, щоб зміцнити довіру

до підключеної економіки, підвищити стійкість інфраструктури Союзу та, зрештою, зберегти європейське суспільство та громадян у цифровій безпеці.

РОЗДІЛ I. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Предмет та сфера застосування

1. З метою забезпечення належного функціонування внутрішнього ринку з одночасним прагненням досягнути високого рівня кібербезпеки, кіберстійкості та довіри в межах Союзу, цей Регламент встановлює:

(a) цілі, завдання та організаційні питання, що стосуються ENISA (Агентства Європейського Союзу з питань мережевої та інформаційної безпеки); та

(b) рамки для створення європейських схем сертифікації кібербезпеки з метою забезпечення належного рівня кібербезпеки для продуктів ІКТ, послуг ІКТ та процесів ІКТ в Союзі, а також з метою уникнення фрагментації внутрішнього ринку стосовно схем сертифікації кібербезпеки в Союзі.

Рамки, зазначені в пункті (b) першого підпараграфа, застосовують без обмежень до спеціальних положень в інших правових актах Союзу, що стосуються добровільної або обов'язкової сертифікації.

2. Цей Регламент не обмежує компетенцій держав-членів щодо діяльності, пов'язаної з громадською безпекою, обороною, національної безпекою, та діяльності держави у сферах кримінального права.

Стаття 2. Терміни та означення

Для цілей цього Регламенту застосовують такі терміни та означення:

(1) «**кібербезпека**» означає діяльність, необхідну для захисту мережевих та інформаційних систем, користувачів таких систем та інших осіб, які зазнають впливу кіберзагроз;

(2) «**мережева та інформаційна система**» означає:

(a) мережу електронного зв'язку у розумінні пункту (a) статті 2 Директиви 2002/21/ЄС;

(b) будь-який пристрій або групу взаємоз'єднаних чи пов'язаних пристроїв, один або декілька з яких, відповідно до програми, здійснює автоматичне опрацювання цифрових даних; або

(c) цифрові дані, які зберігають, опрацьовують, видобувають або передають за допомогою елементів, згаданих в пунктах (a) та (b), для цілей їхньої експлуатації, використання, захисту та технічного обслуговування;

(3) «**національна стратегія безпеки мережевих та інформаційних систем**» означає рамки, що забезпечують стратегічні цілі та пріоритети безпеки мережевих та інформаційних систем на національному рівні;

(4) «**оператор основних послуг**» означає оператора основних послуг, як означено в пункті (4) статті 4 Директиви (ЄС) 2016/1148;

(5) «**надавач цифрових послуг**» означає будь-яку юридичну особу, що надає цифрову послугу;

(6) «**інцидент**» означає будь-яку подію, що має фактичний негативний вплив на безпеку мережевих та інформаційних систем;

(7) «**врегулювання інцидентів**» означає всі процедури на підтримку виявлення, аналізу інциденту, обмеження його наслідків і реагування на нього;

(8) «**кіберзагроза**» означає будь-яку потенційну обставину, подію або дію, яка може пошкодити, порушити або інакше негативно вплинути на мережеві та інформаційні системи, користувачів таких систем та інших осіб;

(9) «**європейська схема сертифікації кібербезпеки**» означає комплексний набір правил, технічні вимоги, стандарти та процедури, які встановлені на рівні Союзу та які застосовують до сертифікації або оцінювання відповідності конкретних продуктів ІКТ, послуг ІКТ або процесів ІКТ;

(10) «**національна схема сертифікації кібербезпеки**» означає комплексний набір правил, технічні вимоги, стандарти та процедури, які розроблені та ухвалені національним органом публічної влади та які застосовують до сертифікації або оцінювання відповідності продуктів ІКТ, послуг ІКТ або процесів ІКТ в рамках конкретної схеми;

(11) «**європейський сертифікат з кібербезпеки**» означає документ, виданий відповідним органом, який підтверджує, що було проведено оцінювання певного продукту ІКТ, послуги ІКТ або процесу ІКТ на відповідність конкретним вимогам, встановленим у європейській схемі сертифікації кібербезпеки;

(12) «**продукт ІКТ**» означає елемент або групу елементів мережі або інформаційної системи;

(13) «**послуга ІКТ**» означає послугу, що головним або переважним чином полягає в передачі, зберіганні, отриманні або опрацюванні інформації за допомогою мережевих та інформаційних систем;

(14) «**процес ІКТ**» означає комплекс заходів, спрямованих на проєктування, розробку, надання або технічне обслуговування продукту ІКТ або послуги ІКТ;

(15) «**акредитація**» означає засвідчення національним органом з акредитації дотримання органом з оцінювання відповідності вимог, установлених у гармонізованих стандартах, та, у відповідних випадках, у будь-яких інших додаткових вимогах, у тому числі тих, що викладено у відповідних секторальних схемах, для провадження конкретної діяльності з оцінювання відповідності;

(16) «**національний орган з акредитації**» означає єдиний орган у державі-члені, який проводить акредитацію на підставі повноважень, наданих державою;

(17) «**оцінювання відповідності**» означає процес підтвердження того, що встановлені вимоги до продукту, процесу, послуги, системи, особи або органу було виконано;

(18) «**орган з оцінювання відповідності**» означає орган, який провадить діяльність з оцінювання відповідності, у тому числі такі її види як калібрування, випробування, сертифікацію та інспектування;

(19) «**стандарт**» означає стандарт, як означено в пункті (1) статті 2 Регламенту (ЄС) № 1025/2012;

(20) «**технічні специфікації**» означають документ, що встановлює технічні вимоги, яким повинні відповідати продукт ІКТ, послуга ІКТ або процес

ІКТ, або процедури оцінювання відповідності стосовно продукту ІКТ, послуги ІКТ або процесу ІКТ;

(21) «**рівень надійності**» означає основу впевненості в тому, що продукт ІКТ, послуга ІКТ або процес ІКТ відповідає вимогам безпеки конкретної європейської схеми сертифікації кібербезпеки, вказує, на якому рівні відбулося оцінювання продукту ІКТ, послуги ІКТ або процесу ІКТ, але як такий не визначає рівень безпеки відповідного продукту ІКТ, послуги ІКТ або процесу ІКТ;

(22) «**самооцінювання відповідності**» означає дію, виконувану виробником або надавачем продуктів ІКТ, послуг ІКТ або процесів ІКТ, яка надає оцінку стосовно того, чи такі продукти ІКТ, послуги ІКТ або процеси ІКТ відповідають вимогам конкретної європейської схеми сертифікації кібербезпеки.

У наступних розділах та статтях визначено наступне:

РОЗДІЛ ІІ. (АГЕНТСТВО ЄВРОПЕЙСЬКОГО СОЮЗУ З ПИТАНЬ МЕРЕЖЕВОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ)

ГЛАВА І. Мандат та цілі

Стаття 3. Мандат.

Стаття 4. Цілі

1. ENISA є центром експертних знань з кібербезпеки завдяки своїй незалежності, науковій та технічній якості наданих консультацій, допомоги та інформації, прозорості своїх оперативних процедур, методів роботи та сумлінного виконання своїх завдань.

2. ENISA надає допомогу установам, органам, офісам та агентствам Союзу, а також державам-членам у розробленні та імплементації політики Союзу з питань кібербезпеки, у тому числі галузевої політики з кібербезпеки.

3. ENISA підтримує розбудову потенціалу та готовність на території Союзу шляхом надання допомоги установам, органам, офісам та агентствам Союзу, а також державам-членам та публічним і приватним стейкхолдерам для посилення захисту їхніх мережевих та інформаційних систем, розробки та посилення кіберстійкості та можливості реагування, а також для розвитку вмінь і навичок у сфері кібербезпеки.

4. ENISA сприяє співпраці, у тому числі обміну інформацією та координації на рівні Союзу, серед держав-членів, установ, органів, офісів та агентств Союзу та відповідних приватних і публічних стейкхолдерів у питаннях кібербезпеки.

5. ENISA сприяє розширенню можливостей у сфері кібербезпеки на рівні Союзу, щоб підтримати заходи держав-членів для запобігання кіберзагрозам та реагування на них, зокрема у випадку транскордонних інцидентів.

6. ENISA сприяє використанню європейської схеми сертифікації кібербезпеки з метою уникнення фрагментації внутрішнього ринку. ENISA сприяє впровадженню та технічному обслуговуванню європейських рамок сертифікації кібербезпеки відповідно до розділу ІІІ цього Регламенту з метою посилення прозорості кібербезпеки продуктів ІКТ, послуг ІКТ, процесів ІКТ, внаслідок чого відбуватиметься посилення рівня впевненості в цифровому внутрішньому ринку та його конкурентоспроможності.

7. ENISA сприяє досягненню високого рівня обізнаності в питаннях кібербезпеки, у тому числі кібергігієни та кіберграмотності, серед громадян, організацій та підприємств.

РОЗДІЛ II. Завдання

Стаття 5. Розробка та імплементація політики та законодавства Союзу

Стаття 6. Розбудова потенціалу

Стаття 7. Оперативна співпраця на рівні Союзу

Стаття 8. Ринок, сертифікація кібербезпеки та стандартизація

Стаття 9. Знання та інформація

Стаття 10. Підвищення рівня обізнаності та освіта

Стаття 11. Дослідження та інновації

Стаття 12. Міжнародна співпраця

РОЗДІЛ III. Організація ENISA

Стаття 13. Структура ENISA

Секція 1. Правління

Стаття 14. Склад Правління

Стаття 15. Функції Правління

Стаття 16. Голова Правління

Стаття 17. Засідання Правління

Стаття 18. Правила голосування Правління

Секція 2. Виконавча рада

Стаття 19. Виконавча рада

Секція 3. Виконавчий директор

Стаття 20. Обов'язки виконавчого директора

Секція 4. Консультативна група ENISA, Група стейкхолдерів з питань сертифікації кібербезпеки та Мережа національних зв'язкових офіцерів

Стаття 21. Консультативна група ENISA

Стаття 22. Група стейкхолдерів з питань сертифікації кібербезпеки

Стаття 23. Мережа національних зв'язкових офіцерів

Секція 5. Діяльність

Стаття 24. Єдиний програмний документ

Стаття 25. Заяви про інтереси

Стаття 26. Прозорість

Стаття 27. Конфіденційність

Стаття 28. Доступ до документів

ГЛАВА IV. Формування і структура бюджету ENISA

Стаття 29. Формування бюджету ENISA

Стаття 30. Структура бюджету ENISA

Стаття 31. Виконання бюджету ENISA

Стаття 32. Фінансові правила

Стаття 33. Боротьба з шахрайством

ГЛАВА V. Персонал

Стаття 34. Загальні положення

Стаття 35. Привілеї та імунітет

Стаття 36. Виконавчий директор
Стаття 37. Прикомандировані національні експерти та інший персонал
ГЛАВА VI. Загальні положення, що стосуються ENISA
Стаття 38. Правовий статус ENISA
Стаття 39. Відповідальність ENISA
Стаття 40. Положення щодо мов
Стаття 41. Захист персональних даних
Стаття 42. Співпраця з третіми країнами та міжнародними організаціями
Стаття 43. Правила безпеки щодо захисту чутливої незасекреченої та секретної інформації
Стаття 44. Угода про штаб-квартиру та умови функціонування
Стаття 45. Адміністративний контроль
РОЗДІЛ III. РАМКИ СЕРТИФІКАЦІЇ КІБЕРБЕЗПЕКИ
Стаття 46. Європейські рамки сертифікації кібербезпеки
Стаття 47. Послідовна робоча програма Союзу для європейської сертифікації кібербезпеки
Стаття 48. Запит на європейську схему сертифікації кібербезпеки
Стаття 49. Підготовка, ухвалення та перегляд європейської схеми сертифікації кібербезпеки
Стаття 50. Вебсайт європейських схем сертифікації кібербезпеки
Стаття 51. Цілі безпеки європейських схем сертифікації кібербезпеки
Стаття 52. Рівні надійності європейських схем сертифікації кібербезпеки
Стаття 53. Самооцінювання відповідності
Стаття 54. Елементи європейських схем сертифікації кібербезпеки
Стаття 55. Додаткова інформація з питань забезпечення кібербезпеки стосовно сертифікованих продуктів ІКТ, послуг ІКТ та процесів ІКТ
Стаття 56. Сертифікація кібербезпеки
Стаття 57. Національні схеми сертифікації кібербезпеки та національні сертифікати з кібербезпеки
Стаття 58. Національні органи з сертифікації кібербезпеки
Стаття 59. Партнерська перевірка
Стаття 60. Органи з оцінювання відповідності
Стаття 61. Нотифікація
Стаття 62. Європейська група з сертифікації кібербезпеки
Стаття 63. Право подавати скаргу
Стаття 64. Право на дієвий судовий захист
Стаття 65. Санкції
РОЗДІЛ IV. ПРИКІНЦЕВІ ПОЛОЖЕННЯ
Стаття 66. Процедура комітету
Стаття 67. Оцінювання й перегляд
Стаття 68. Скасування та правонаступництво
Стаття 69. Набуття чинності

2.2. ДСТУ ISO 27001, ISO 27002, ISO 27003

Система кібербезпеки, яка базується на міжнародних стандартах надзвичайно важлива у сучасному цифровому світі. Розробкою зазначених стандартів займаються Міжнародна організація з стандартизації (ISO) спільно з Міжнародною електротехнічною комісією (IEC). На сьогодні фахівцями цих організацій розроблена серія стандартів ISO/IEC 27000, яка постійно доповнюється новими документами.В Україні на даний час діють стандарти серії ДСТУ ISO/IEC 27000, які відповідно гармонізовані з ISO/IEC 27000. До них відносяться наступні:

ДСТУ ISO/IEC 27000:2019

ДСТУ ISO/IEC 27000:2019 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Огляд і словник термінів (ISO/IEC 27000:2018, IDT) – ISO/IEC 27000:2018 дає змогу переглянути системи управління інформаційною безпекою (СУІБ). Це також забезпечує терміни і визначення, як правило, використовувані в СУІБ сімейства стандартів. Цей документ є застосованим до всіх типів і розмірів організації (наприклад, комерційні організації, державні агенції, не для сприяння охоплюють загальновживані терміни та визначення в сімействі стандартів СУІБ; не підтримують всі терміни і терміни, які застосовуються в сімействі стандартів СУІБ; не встановлює значення СУІБ у стандартах у визначенні нових термінів для використання.

ДСТУ ISO/IEC 27001:2015

ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT) – Цей стандарт визначає вимоги до проектування, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою з урахуванням обставин організації. Цей стандарт також містить вимоги для оцінювання та оброблення ризиків інформаційної безпеки, пов’язаних з потребами організації. Вимоги, наведені в цьому стандарті, є загальними та можуть бути запроваджені для всіх організацій незалежно від типу, розміру та природи. Вилучення будь-якої з вимог, наведених в розділах 4-10 неприпустимо в разі, якщо організація прагне відповідати цьому стандарту.

Входить в групу стандартів ISO 27000 – СУІБ та тісно пов'язаний із стандартом ISO/IEC 27002.

У стандарті ISO/IEC 27001 (ISO 27001) зібрані описи найкращих світових практик в області управління інформаційною безпекою. ISO 27001 встановлює вимоги до системи менеджменту інформаційної безпеки для демонстрації здатності організації захищати свої інформаційні ресурси. Цей стандарт підготовлений в якості моделі для розробки, впровадження, функціонування,

моніторингу, аналізу, підтримки та поліпшення **Системи Управління Інформаційної Безпеки (СУІБ)**.

Система управління інформаційною безпекою СУІБ (англ. *information security management system*, ISMS) – частина загальної системи управління, яка ґрунтується на підході, що враховує ризики інформаційної безпеки як бізнес-ризики, призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки.

Для **процесів СУІБ застосована модель ПВПД** (плануй-виконуй-перевіряй-дій; англ. ***Plan-Do-Check-Act, PDCA***):

– Plan (планування) – фаза створення СУІБ, створення переліку активів, оцінки ризиків та вибору заходів;

– Do (дія) – етап реалізації та впровадження відповідних заходів;

– Check (перевірка) – фаза оцінки ефективності та продуктивності СУІБ. Зазвичай виконується внутрішніми аудиторами;

– Act (поліпшення) – виконання превентивних і коригуючих дій

Складові політики інформаційної безпеки:

– визначення критичних бізнес-процесів/банківських продуктів;
– надання доступу до інформації;
– контроль доступу;
– парольний захист;
– антивірусний захист;
– захист мережі банку;
– віддалений доступ до ресурсів мережі;
– ідентифікація та автентифікація ресурсів СУІБ;
– криптографічний захист інформації;
– політика «чистого екрана» та «чистого стола»

Мета СУІБ – вибір відповідних заходів управління безпекою, призначених для захисту інформаційних активів і гарантують довіру зацікавлених сторін.

Інформаційна безпека – збереження конфіденційності, цілісності та доступності інформації; крім того, можуть бути включені і інші властивості, такі як справжність, неможливість відмови від авторства, достовірність.

Конфіденційність – забезпечення доступності інформації тільки для тих, хто має відповідні повноваження (авторизовані користувачі).

Доступність – забезпечення доступу до інформації авторизованим користувачам, коли це необхідно (на вимогу).

Цілісність – забезпечення точності і повноти інформації, а також методів її обробки.

Саме поняття «**Захист інформації**» трактується міжнародним стандартом як забезпечення конфіденційності, цілісності та доступності інформації. Основа стандарту ІСО 27001 – система управління ризиками, пов'язаними з інформацією. **Система управління ризиками** дозволяє отримувати відповіді на наступні питання:

– на якому напрямку інформаційної безпеки потрібно зосередити увагу;

– скільки часу і коштів можна витратити на дане технічне рішення для захисту інформації.

Стандарт ISO 27001 гармонізований зі стандартами систем менеджменту якості ISO 9001:2015 та ISO 14001:2015 та базується на їх основних принципах і процесному підході. Більш того, обов'язкові процедури стандарту ISO 9001 потрібні і стандартом ISO 27001. Структура документації за вимогами ISO 27001 аналогічна структурі за вимогами ISO 9001. Велика частина документації, необхідна по ISO 27001, вже могла бути розроблена, і могла використовуватися в рамках ISO 9001. Таким чином, якщо організація вже має систему менеджменту згідно, наприклад, з ISO 9001 або ISO 14001, то переважно забезпечувати виконання вимоги стандарту ISO 27001 в рамках вже існуючих систем.

Також **основними принципами стандарту ISO 27001** є:

– конфіденційність інформації
– доступність інформації
– цілісність інформації

Організація може бути **сертифікована акредитованими агентствами відповідно до цього стандарту. Процес сертифікації** складається з трьох стадій:

– стадія 1 – вивчення аудитором ключових документів системи менеджменту інформаційної безпеки – положення про можливість застосування (SoA), план обробки ризиків (RTP), і ін. Може виконуватися як на території організації так і шляхом висилки цих документів зовнішньому аудитору;

– стадія 2 – детальний, глибокий аудит включаючи тестування впроваджених заходів та оцінка їх ефективності. Включає повне вивчення документів, які вимагає стандарт;

– стадія 3 – виконання інспекційного аудиту для підтвердження, що сертифікована організація відповідає заявленим вимогам. Виконується на періодичній основі.

Процедура сертифікації системи менеджменту за допомогою одного з міжнародних стандартів або їх комбінації підрозділяється на 4 етапи:

– 1 етап. Підготовка до сертифікації;
– 2 етап. Аудит 1-го ступеня (перевірка готовності до сертифікації);
– 3 етап. Аудит 2-го ступеня (сертифікаційний аудит);
– 4-ий етап. Видача сертифіката і нагляд.

ДСТУ ISO/IEC 27002:2015

ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT) – Цей стандарт встановлює настанови стосовно організаційних стандартів щодо інформаційної безпеки та загальні практики управління інформаційною безпекою, охоплюючи вибір, впровадження та управління заходами безпеки з урахуванням розгляду середовища ризиків інформаційної безпеки організації. Цей стандарт розроблено для використання організаціями, які намагаються: визначити заходи безпеки в межах процесу впровадження **системи управління інформаційною безпекою (СУІБ)** або як її ще називають

системи менеджменту інформаційною безпекою (СМІБ) на основі ISO/IEC 27001; впровадити загальноприйняті заходи інформаційної безпеки; розробити власні настанови щодо управління інформаційною безпекою.

До 2007 року цей стандарт називався ISO/IEC 17799. Стандарт розроблений у 2005 році на основі версії **ISO 17799**, опублікованої в 2000, яка була повною копією Британського стандарту **BS 7799-1:1999**.

Стандарт надає найкращі практичні поради щодо менеджменту інформаційної безпеки для тих, хто відповідає за створення, реалізацію або обслуговування систем менеджменту інформаційної безпеки. ***Інформаційна безпека*** визначається стандартом як «збереження конфіденційності (впевненості в тому, що інформація доступна лише тим, хто уповноважений мати такий доступ), цілісності (гарантії точності та повноти інформації, а також методів її обробки) та доступності (гарантії того, що уповноважені користувачі мають доступ до інформації та пов'язаних з нею ресурсів)».

Поточна версія стандарту складається з таких основних розділів:

- Політика безпеки (*Security policy*).
- Організація інформаційної безпеки (*Organization of information security*).
- Управління ресурсами (*Asset management*).
- Безпека персоналу (*Human resources security*).
- Фізична безпека та безпека оточення (*Physical and environmental security*).
- Управління комунікаціями та операціями (*Communications and operations management*).
- Управління доступом (*Access control*).
- Придбання, розробка та підтримка систем (*Information systems acquisition, development and maintenance*).
- Управління інцидентами інформаційної безпеки (*Information security incident management*).
- Управління безперебійною роботою організації (*Business continuity management*).
- Відповідність нормативним вимогам (*Compliance*).

Цей документ описує 127 механізмів контролю, які необхідні для побудови системи управління інформаційною безпекою (СУІБ) організації, визначених на основі кращих прикладів світового досвіду (best practices) у цій галузі. Цей документ є практичним посібником зі створення СУІБ.

Британський стандарт BS 7799, на якому базується ISO/IEC 27002, рекомендує включати в документ, що характеризує політику безпеки організації, наступні розділи:

– вступний, підтверджуючий заклопотаність вищого керівництва проблемами інформаційної безпеки;

– організаційний, утримуючий опис підрозділів, комісій, груп і т.д., відповідальних за роботи в області інформаційної безпеки;

– класифікаційний, що описує наявні в організації матеріальні й інформаційні ресурси й необхідний рівень їхнього захисту;

– штатний, що характеризує міри безпеки, застосовувані до персоналу (опис посад з погляду інформаційної безпеки, організація навчання й перепідготовки персоналу, порядок реагування на порушення режиму безпеки й т.п.);

– розділ, що висвітлює питання *фізичного захисту*;

– керуючий розділ, що описує підхід до управління комп'ютерами й комп'ютерними мережами;

– розділ, що описує *правила розмежування* доступу до виробничої інформації;

– розділ, що характеризує *порядок розробки* й супроводу систем;

– розділ, що описує міри, спрямовані на забезпечення *безперервної роботи* організації;

– юридичний розділ, що підтверджує відповідність політики безпеки чинному законодавству.

Існує 3 рівня:

– Верхній.

– Середній.

– Нижній.

Верхній рівень

Програму верхнього рівня очолює особа, відповідальна за інформаційну безпеку організації. У цієї програми наступні головні цілі:

– управління ризиками (*оцінка ризиків*, вибір ефективних засобів захисту);

– *координація* діяльності в області інформаційної безпеки, поповнення й розподіл ресурсів;

– *стратегічне планування*;

– *контроль* діяльності в області інформаційної безпеки.

У рамках програми верхнього рівня приймаються стратегічні рішення по забезпеченню безпеки, оцінюються технологічні новинки. Інформаційні технології розвиваються дуже швидко, і необхідно мати чітку політику відстеження й впровадження нових засобів.

Контроль діяльності в області безпеки має двосторонню спрямованість. По-перше, необхідно гарантувати, що дії організації не суперечать законам. При цьому варто підтримувати контакти із зовнішніми контролюючими організаціями. По-друге, потрібно постійно відслідковувати стан безпеки усередині організації, реагувати на випадки порушень і допрацьовувати захисні міри з урахуванням зміни обстановки.

Варто підкреслити, що програма верхнього рівня повинна займати строго певне місце в діяльності організації, вона повинна офіційно прийматися й підтримуватися керівництвом, а також мати певний штат і бюджет.

Середній рівень

До середнього рівня можна віднести питання, що стосуються окремих аспектів інформаційної безпеки, але важливі для різних експлуатованих організацією систем. Приклади таких питань – відношення до передових (але, можливо, недостатньо перевірених) технологій, доступ в Internet (як сполучити

незалежність доступу до інформації із захистом від зовнішніх погроз?), використання домашніх комп'ютерів, застосування користувачами неофіційного програмного забезпечення й т.д.

Політика середнього рівня повинна для кожного аспекту висвітлювати наступні теми:

– Опис аспекту. Наприклад, якщо розглянути застосування користувачами неофіційного програмного забезпечення, останнє можна визначити як ПЗ, що не було схвалено й/або закуплене на рівні організації.

– Область застосування. Варто визначити, де, коли, як, стосовно кого й чому застосовується дана *політика безпеки*.

– Позиція організації по даному аспекту. Продовжуючи приклад з неофіційним програмним забезпеченням, можна уявити собі позиції повної заборони, розробки процедури приймання подібного ПЗ й т.п. Позиція може бути сформульована й у набагато більше загальному виді, як набір цілей, які переслідує організація в даному аспекті. Взагалі стиль документів, що визначають політику безпеки (як і їхній перелік), у різних організаціях може сильно відрізнятися.

– Ролі й обов'язки. В «політичний» документ необхідно включити інформацію про посадові особи, відповідальні за реалізацію політики безпеки. Наприклад, якщо для використання неофіційного програмного забезпечення співробітникам потрібен дозвіл керівництва, повинне бути відомо, у кого і як його можна одержати. Якщо неофіційне програмне забезпечення використовувати не можна, варто знати, хто стежить за виконанням даного правила.

– Законослухняність. Політика повинна містити загальний опис заборонених дій і покарань за них.

– Точки контакту. Повинно бути відомо, куди варто звертатися за роз'ясненнями, допомогою й додатковою інформацією. Звичайно «точкою контакту» служать певні посадові особи, а не конкретна людина, що займає в цей момент даний пост.

Нижній рівень

Політика безпеки **нижнього рівня відноситься до конкретних інформаційних сервісів.** Вона містить у собі два аспекти – цілі й правила їхнього досягнення, тому її часом важко відокремити від питань реалізації. На відміну від двох верхніх рівнів, розглянута *політика* повинна бути визначена більш докладно. Є багато речей, специфічних для окремих видів послуг, які не можна єдиним образом регламентувати в рамках всієї організації. У той же час, ці речі настільки важливі для забезпечення режиму безпеки, що стосовні до них рішення повинні прийматися на управлінському, а не технічному рівні. Приведемо кілька прикладів питань, на які варто дати відповідь у політику безпеки нижнього рівня:

– хто має право доступу до об'єктів, підтримуваним сервісом?
– при яких умовах можна читати й модифікувати дані?
– як організований віддалений доступ до сервісу?

При формулюванні цілей політики нижнього рівня можна виходити з міркувань цілісності, доступності й конфіденційності, але не можна на цьому зупинятися. Її цілі повинні бути більше конкретними. Наприклад, якщо мова йде про систему розрахунку заробітної плати, можна поставити ціль, щоб тільки співробітникам відділу кадрів і бухгалтерії дозволялося вводити й модифікувати інформацію. У більш загальному випадку цілі повинні зв'язувати між собою об'єкти сервісу й дії з ними.

Із цілей виводяться правила безпеки, що описують, хто, що й при яких умовах може робити. Чим докладніше правила, тим більш формально вони викладені, тим простіше підтримати їхнє виконання програмно-технічними засобами. З іншого боку, занадто тверді правила можуть заважати роботі користувачів, імовірно, їх прийдеться часто переглядати. Керівництву має бути знайти розумний компроміс, коли за прийнятну ціну буде забезпечений прийнятний рівень безпеки, а співробітники не виявляться надмірно зв'язані. Звичайно найбільше формально задаються права доступу до об'єктів через особливу важливість даного питання.

Ціль програми нижнього рівня – забезпечити надійний і економічний захист конкретного сервісу або групи однорідних сервісів. На цьому рівні вирішується, які варто використовувати механізми захисту; закупаються й установлюються технічні засоби; виконується повсякденне адміністрування; відслідковується стан слабких місць і т.п. Звичайно за програму нижнього рівня відповідають адміністратори сервісів.

Програма безпеки

Після того, як сформульована *політика безпеки*, можна приступати до складання програми її реалізації й властиво до реалізації.

Щоб зрозуміти й реалізувати яку-небудь програму, її потрібно структурувати по рівнях, звичайно у відповідності зі структурою організації. У найпростішому й найпоширенішому випадку досить двох рівнів – верхнього, або центрального, котрий охоплює всю організацію, і нижнього, або службового, котрий відноситься до окремих послуг або груп однорідних сервісів.

Синхронізація програми безпеки з життєвим циклом систем

Якщо синхронізувати програму безпеки нижнього рівня з *життєвим циклом* сервісу, що захищається, можна домогтися більшого ефекту з меншими витратами. Програмісти знають, що додати нову можливість до вже готової системи на порядок складніше, ніж споконвічно спроектувати й реалізувати її. Те ж справедливо й для інформаційної **безпеки.**

У *життєвому циклі* інформаційного сервісу можна виділити наступні етапи:

Ініціація. На даному етапі виявляється необхідність у придбанні нового сервісу, документується його передбачуване призначення. З погляду безпеки найважливішою дією тут є оцінка критичності як самого сервісу, так і інформації, що з його допомогою буде оброблятися.

Закупівля. На даному етапі складаються специфікації, пророблюються варіанти придбання, виконується властиво *закупівля*. Зрозуміло, особлива увага повинне приділятися питанням сумісності нового сервісу з існуючою конфігурацією. Підкреслимо також, що нерідко засобу безпеки є необов'язковими компонентами комерційних продуктів, і потрібно простежити, щоб відповідні пункти не випали зі специфікації.

Установка. Сервіс установлюється, конфігурується, тестується й вводиться в *експлуатацію*. Як правило, комерційні продукти поставляються з відключеними засобами безпеки; їх необхідно включити й належним чином налаштувати. Для великої організації, де багато користувачів і даних, початкове настроювання може стати досить трудомісткою й відповідальною справою. По-друге, новий сервіс має потребу в процедурних регуляторах. Варто подбати про чистоту й охорону приміщення, про документи, що регламентують використання сервісу, про підготовку планів на випадок екстрених ситуацій, про організацію навчання користувачів і т.п.

Експлуатація. На даному етапі сервіс не тільки працює й адмініструється, але й піддається модифікаціям. Якщо безпека не підтримувати, вона слабшає. Користувачі не настільки ревно виконують посадові інструкції, адміністратори менш ретельно аналізують реєстраційну інформацію. То той, то інший користувач одержує додаткові привілеї. Здається, що в сутності нічого не змінилося; насправді ж від колишньої безпеки не залишилося й сліду. Для боротьби з ефектом повільних змін доводиться прибігати до періодичних перевірок безпеки сервісу.

Виведення з експлуатації. Відбувається перехід на новий сервіс. Тільки в специфічних випадках необхідно піклуватися про фізичне руйнування апаратних компонентів, що зберігають конфіденційну інформацію. При *виведенні даних з експлуатації* їх звичайно переносять на іншу систему, архівують, викидають або знищують.

ДСТУ ISO/IEC 27003:2018

– ДСТУ ISO/IEC 27003:2018 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Настанова (ISO/IEC 27003:2017, IDT) – забезпечує висвітлення та управління на ISO/IEC 27001:2013.

ISO/IEC 27003 містить керівні вказівки щодо вимог до системи управління інформаційною безпекою (СУІБ), як зазначено у стандарті ISO/IEC 27001, і надає рекомендації, можливості та дозволи щодо них. Цей документ не передбачає надання загальних рекомендацій з усіх аспектів інформаційної безпеки. Статті 4-10 цього документа відображають структуру ISO/IEC 27001:2013. Стандарт ISO/IEC 27003 не додає нових вимог до СУІБ та пов'язаних з ними термінів та визначень. Організації, що впроваджують СУІБ, не зобов'язані дотримуватися вказівок у цьому документі. СУІБ підкреслює важливість наступних етапів:

– розуміння потреб організації та необхідності встановлення політики інформаційної безпеки та цілей інформаційної безпеки;

– оцінка ризиків організації, пов'язаних з інформаційною безпекою;

– впровадження та керування процесами інформаційної безпеки, контролю та іншими заходами щодо ліквідації ризиків;

– моніторинг та перевірка продуктивності та ефективності СУІБ;

– впровадження постійного вдосконалення СУІБ.

СУІБ, подібний до будь-якого іншого типу системи управління, включає такі **ключові компоненти**:

а) політика;

б) особи з визначеними обов'язками;

в) процеси управління, пов'язані з:

– встановлення політики;

– забезпечення обізнаності та компетентності;

– планування;

– реалізація;

– експлуатація;

– оцінка продуктивності;

– огляд управління;

– вдосконалення;

г) документально підтверджена інформація.

СУІБ має додаткові ключові компоненти, такі як:

д) оцінка ризику інформаційної безпеки;

є) обробка ризиків інформаційної безпеки, включаючи детермінацію та здійснення контролю.

Цей документ є загальним і призначений для застосування до всіх організацій, незалежно від типу (державні чи комерційні) та розміру. Організація повинна визначити, яка частина цього стандарту поширюється на неї відповідно до її специфічного організаційного контексту (Стаття 4 ISO/IEC 27001:2013). Деякі інструкції можуть бути придатними для великих організацій, але для дуже маленьких організацій (наприклад, з менш ніж 10 співробітниками) можуть бути непотрібними або неприйнятними.

2.3. ISO/IEC 15408- 2, ISO/IEC 15408-3

Стек стандартів **ISO/IEC 15408 включає в себе наступні стандарти:**

ISO/IEC 15408-1/2/3:2017 Інформаційні технології. Методи захисту. Критерії оцінки:

Частина 1. Вступ та загальна модель (ISO/IEC 15408-1: 2022, IDT).

Частина 2. Функціональні вимоги (ISO/IEC 15408-2: 2022, IDT).

Частина 3. Вимоги до гарантії безпеки (ISO/IEC 15408-3: 2022, IDT).

Стандарт містить загальний набір вимог до функцій безпеки IT-продуктів і систем, а також до заходів гарантії, застосованих до них під час оцінки безпеки.

Якщо взяти європейські стандарти, відносно яких відбувається гармонізація, то їх вже 5:

ISO/IEC 15408-1:2022. Інформаційна безпека, кібербезпека та захист конфіденційності. Критерії оцінки IT-безпеки. Частина 1. Вступ і загальна модель

Цей документ встановлює загальні концепції та принципи оцінювання безпеки IT і визначає загальну модель оцінювання, що надається різними частинами стандарту, який у цілому призначений для використання в якості основи для оцінки властивостей безпеки IT-продуктів.

Цей документ містить огляд усіх частин серії ISO/IEC 15408. Він описує різні частини серії ISO/IEC 15408; визначає терміни та скорочення, які слід використовувати в усіх частинах стандарту; встановлює основну концепцію мети оцінювання (TOE); описує контекст оцінювання та описує аудиторію, якій адресовані критерії оцінювання. Дано вступ до основних концепцій безпеки, необхідних для оцінки IT-продуктів.

Цей документ представляє:

– ключові поняття профілів захисту (PP), модулів PP, конфігурацій PP, пакетів, цілей безпеки (ST) і типів відповідності;

– опис організації компонентів безпеки по всій моделі;

– різні операції, за допомогою яких функціональні компоненти та компоненти гарантії, наведені в ISO/IEC 15408-2 та ISO/IEC 15408-3, можуть бути налаштовані шляхом використання дозволених операцій;

– загальну інформацію про методи оцінювання, наведені в ISO/IEC 18045;

– настанова щодо застосування ISO/IEC 15408-4 для розробки методів оцінювання (EM) і діяльності з оцінювання (EA), виведених із ISO/IEC 18045;

– загальну інформацію про попередньо визначені рівні гарантії оцінювання (EAL), визначені в ISO/IEC 15408-5;

– інформація щодо обсягу схем оцінювання.

ISO/IEC 15408-2:2022. Інформаційна безпека, кібербезпека та захист конфіденційності. Критерії оцінки IT-безпеки. Частина 2. Функціональні компоненти безпеки.

Цей документ визначає необхідну структуру та зміст функціональних компонентів безпеки з метою оцінки безпеки. Він містить каталог функціональних компонентів, який відповідає загальним вимогам безпеки багатьох IT-продуктів.

ISO/IEC 15408-3:2022. Інформаційна безпека, кібербезпека та захист конфіденційності. Критерії оцінювання IT-безпеки. Частина 3. Компоненти забезпечення безпеки.

Цей документ визначає вимоги серії стандартів ISO/IEC 15408. Він включає окремі компоненти гарантії, з яких складаються рівні гарантії оцінки та інші пакети, що містяться в ISO/IEC 15408-5, а також критерії для оцінки профілів захисту (PP), конфігурацій PP, модулів PP та цілей безпеки (STs).

ISO/IEC 15408-4:2022. Інформаційна безпека, кібербезпека та захист конфіденційності. Критерії оцінки IT-безпеки. Частина 4. Структура для специфікації методів оцінювання та діяльності

Цей документ забезпечує стандартизовану структуру для визначення об’єктивних, повторюваних і відтворюваних методів оцінювання та діяльності з

оцінювання. Цей документ не визначає, як оцінювати, приймати або підтримувати методи оцінювання та діяльність з оцінювання. Ці аспекти є справою для тих, хто розробляє методи оцінювання та діяльність з оцінювання в їхній конкретній сфері інтересів.

ISO/IEC 15408-5:2022. Інформаційна безпека, кібербезпека та захист конфіденційності. Критерії оцінювання ІТ-безпеки. Частина 5. Попередньо визначені пакети вимог до безпеки.

Цей документ надає пакети забезпечення безпеки та функціональні вимоги безпеки, які були визначені як корисні для підтримки загального використання зацікавленими сторонами.

Приклади наданих пакетів включають рівні гарантії оцінювання (EAL) і складені пакети гарантій (CAP).

Цей документ представляє:

– сімейство пакетів *рівня гарантії оцінки (EAL),* які визначають попередньо визначені набори компонентів гарантії безпеки, на які можна посилатися в PP та ST, і які визначають відповідні гарантії безпеки, які необхідно надати під час оцінювання цілі оцінки (TOE);

– сімейство пакетів *гарантії композиції (CAP),* які вказують набори компонентів гарантії безпеки, що використовуються для визначення відповідних гарантій безпеки, які мають бути надані під час оцінювання складених ТО;

– пакет *складеного продукту (COMP),* який визначає набір компонентів гарантії безпеки, що використовуються для визначення відповідних гарантій безпеки, які мають бути надані під час оцінювання TOE складеного продукту;

– сімейство пакетів *гарантії профілю захисту (PPA),* які вказують набори компонентів гарантії безпеки, що використовуються для визначення відповідних гарантій безпеки, які мають надаватися під час оцінювання профілю захисту;

– сімейство пакетів *гарантії цільової безпеки (STA),* які вказують набори компонентів гарантії безпеки, що використовуються для визначення відповідних гарантій безпеки, які мають бути надані під час оцінки цільової безпеки.

Серед користувачів цього документа можуть бути споживачі, розробники та оцінювачі безпечних ІТ-продуктів.

Опис стандарту 15408

У стандарті, що отримав назву «Загальні критерії оцінки безпеки інформаційних технологій » (The Common Criteria for Information Technology Security Evaluation), докладно розглянуто загальні підходи, методи та функції забезпечення захисту інформації в організаціях.

Функції системи інформаційної безпеки забезпечують виконання вимог конфіденційності, цілісності, достовірності та доступності інформації. **Всі функції представлені у вигляді чотирирівневої ієрархічної структури**: клас – сімейство – компонент – елемент.

За аналогією представлені вимоги якості. Подібна градація дозволяє описати будь-яку систему інформаційної безпеки і зіставити створену модель з поточним станом справ.

У стандарті виділені 11 класів функцій:

– аудит;
– ідентифікація та аутентифікація;
– криптографічний захист;
– конфіденційність;
– передача даних;
– захист даних користувача;
– управління безпекою;
– захист функцій безпеки системи;
– використання ресурсів;
– доступ до системи;
– надійність засобів.

Оцінка інформаційної безпеки базується на моделях системи безпеки, що складаються з перерахованих у стандарті функцій. У ISO 15408 міститься **ряд зумовлених моделей** (так званих **профілів),** що описують стандартні модулі системи безпеки. З їх допомогою можна не створювати моделі поширених засобів захисту самостійно, винаходячи велосипед, а користуватися вже готовими наборами описів, цілей, функцій і вимог до цих засобів. Простим прикладом профілів може служити модель міжмережевого екрану.

Сертифікований профіль являє собою повний опис певної частини (або функції) системи безпеки. У ньому міститься аналіз внутрішнього і зовнішнього середовища об'єкта, вимоги до його функціональності і надійності, логічне обгрунтування його використання, можливості та обмеження розвитку об'єкта.

Стандарт ISO 15408 вигідно відрізняє **відкритість.** Описує ту чи іншу область системи безпеки профіль можна створити самостійно за допомогою розробленої в ISO 15408 структури документа. У стандарті визначена також послідовність дій для самостійного створення профілів.

Загальні критерії узагальнили зміст і досвід використання Помаранчевої книги, розвинули рівні впевненості Європейських критеріїв, втілили в реальні структури концепцію профілів захисту Федеральних критеріїв США.

Стандарт ISO/IEC 15408 «Загальні критерії оцінки безпеки інформаційних технологій» (англ. Common Criteria for Information Technology Security Evaluation) описує інфраструктуру (Framework) в якій користувачі комп'ютерної системи можуть описати вимоги, розробники можуть заявити про властивості безпеки продуктів, а експерти з безпеки визначити, чи задовольняє продукт заявам. Таким чином цій стпндарт дозволяє бути впевненим, що процес опису, розробки та перевірки продукту був проведений в строгому порядку.

У "Загальних критеріях" (ЗК) проведена класифікація широкого набору функціональних вимог і вимог довіри до безпеки, визначені структури їх групування і принципи цільового використання

Загальні критерії дозволяють підвищити довіру до засобів захисту і самої інформації, що захищається за рахунок трьох основних якостей:

1. Можливості гнучкого завдання вимог до засобів захисту інформації з урахуванням їх призначення і умов застосування.

2. Більш повного і обгрунтованого набору вимог безпеки.

3. Наявності методології оцінки, що забезпечує об'єктивність і порівнянність результатів.

Загальні критерії являють собою набір з п'яти окремих взаємопов'язаних частин. До них відносяться:

– Введення і загальна модель.

– Функціональні вимоги безпеки.

– Вимоги до надійності захисних механізмів.

– Попереднє визначення профілі захисту.

– Процедури реєстрації профілів захисту.

Основними відмітними рисами ЗК є наступні:

1. Перш за все, ЗК – це певна методологія та система формування вимог і оцінки безпеки ІТ. Системність простежується, починаючи від термінології та рівнів абстракції представлення вимог аж до їх застосування при оцінці безпеки на всіх етапах життєвого циклу продуктів і систем ІТ.

2. Загальні критерії характеризуються найбільш повною на сьогоднішній день сукупністю вимог безпеки ІТ.

3. У ЗК проведено чіткий поділ вимог безпеки на функціональні вимоги і вимоги довіри до безпеки. **Функціональні вимоги** (11 класів, 66 родин, 135 компонентів) відносяться до **функцій безпеки** (ідентифікації, аутентифікації, управління доступом, аудиту і т. д.), а **вимоги довіри** (8 класів, 44 сімейства, 93 компонента) – до досягнення **впевненості в коректності реалізації та ефективності функцій безпеки** шляхом оцінки технології розробки, тестування, аналізу вразливостей експлуатаційної документації, постачання і супроводу продуктів та систем ІТ.

4. Загальні критерії включають шкалу довіри до безпеки (оціночні рівні довіри – ОРД), яка може використовуватися для отримання різного ступеня впевненості у безпеці продуктів і систем ІТ

5. Систематизація і класифікація вимог щодо ієрархії «клас» – «сімейство» – «компонент» – «елемент» з унікальними ідентифікаторами вимог забезпечує зручність їх використання.

6. Компоненти вимог в родинах і класах ранжовані за ступенем повноти і строгості, а вимоги довіри згруповані в пакети вимог

7. Гнучкість у підході до формування вимог безпеки для різних типів продуктів і систем ІТ та умов їх застосування забезпечується можливістю цілеспрямованого формування необхідних наборів вимог у вигляді певних в ЗК стандартизованих структур (пакетів вимог, профілів захисту і завдань з безпеки).

8. Загальні критерії володіють відкритістю і розширюваністю, тобто дозволяють уточнювати існуючі і вводити додаткові вимоги.

Як показують оцінки фахівців у галузі інформаційної безпеки за рівнем систематизації, повноті і можливостям деталізації вимог, універсальності і гнучкості в застосуванні ЗК представляють найбільш досконалий з існуючих в даний час стандартів. Причому, що дуже важливо, в силу особливостей побудови він має практично необмежені можливості для розвитку і являє собою базовий стандарт, що містить методологію завдання вимог і оцінки безпеки ІТ, а також систематизований каталог вимог безпеки. Як функціональних стандартів, в яких

формулюються вимоги до безпеки певних типів продуктів і систем ІТ, передбачається використання профілів захисту (ПЗ), що створюються за методологією і на основі каталогу вимог ЗК. У ПЗ можуть бути включені і будь-які інші вимоги, які є необхідними для забезпечення безпеки конкретного типу продуктів або систем ІТ.

2.4. Стек протоколів ДСТУ ISO/IEC 27000

Крім вищеперерахованих протоколів ДСТУ ISO/IEC 27000, 27001, 27002, 27003, до даного стеку протоколів відносяться наступні:

– **ДСТУ ISO/IEC 27004:2018 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Моніторинг, вимірювання, аналізування та оцінювання (ISO/IEC 27004:2016, IDT) –** ISO/IEC 27004:2016 містить настанови, спрямовані на допомогу організаціям в оцінюванні ефективності інформаційної безпеки та ефективності системи управління інформаційною безпекою з метою виконання вимог ISO/IEC 27001:2013, 9.1. Він встановлює: моніторинг та вимірювання ефективності інформаційної безпеки; моніторинг та вимірювання ефективності системи управління інформаційною безпекою (СУІБ), включаючи її процеси та засоби контролю; аналіз та оцінка результатів моніторингу та вимірювання. ISO/IEC 27004:2016 застосовний до організацій усіх типів і розмірів.

– **ДСТУ ISO/IEC 27005:2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT) –** Цей документ містить вказівки щодо управління ризиками інформаційної безпеки. Цей документ підтримує загальні концепції, визначені в ISO/IEC 27001, і призначений для сприяння задовільній реалізації інформаційної безпеки на основі підходу до управління ризиками. Знання концепцій, моделей, процесів і термінології, описаних у ISO/IEC 27001 та ISO/IEC 27002, є важливим для повного розуміння цього документа. Цей документ застосовується до всіх типів організацій (наприклад, комерційних підприємств, державних установ, некомерційних організацій), які мають намір керувати ризиками, які можуть поставити під загрозу інформаційну безпеку організації.

– **ДСТУ ISO/IEC 27006:2015 Інформаційні технології. Методи захисту. Вимоги до органів, які надають послуги з аудиту і сертифікації систем управління інформаційною безпекою (ISO/IEC 27006:2015, IDT) –** Цей стандарт визначає вимоги та надає настанови для організацій, які надають послуги з аудиту та сертифікації систем управління інформаційною безпекою (СУІБ) додатково до вимог, що містяться в ISO/IEC 17021-1 та ISO/IEC 27001. Це, в першу чергу, спрямовано на підтримку акредитації організацій, які надають послуги із сертифікації СУІБ. Вимоги, які містить цей стандарт, необхідно продемонструвати в термінах компетентності та надійності всім організаціям, які

здійснюють сертифікацію СУІБ, а настанови, долучені до цього стандарту, надають додаткову інтерпретацію цих вимог для будь-якої організації, яка виконує сертифікацію СУІБ. Цей стандарт може бути застосований як документ критеріїв для акредитації, експертного оцінювання або інших процесів аудиту.

– **ДСТУ ISO/IEC 27007:2018 Інформаційні технології. Методи захисту. Настанова щодо аудиту систем управління інформаційною безпекою (ISO/IEC 27007:2017, IDT) –** Цей документ містить вказівки щодо управління програмою аудиту системи управління інформаційною безпекою (СУІБ), щодо проведення аудитів та компетентності аудиторів СУІБ, на додаток до вказівок, що містяться в ISO 19011. Цей документ стосується тих, хто потребує розуміння чи проведення внутрішніх чи зовнішніх аудитів СУІБ або управління програмою аудиту СУІБ.

– **ДСТУ ISO/IEC TS 27008:2019 Інформаційні технології. Методи захисту. Настанова щодо оцінювання захисту інформаційної безпеки (ISO/IEC TS 27008:2019, IDT) –** У цьому документі містяться вказівки щодо перегляду та оцінки впровадження та функціонування засобів контролю інформаційної безпеки, включаючи технічну оцінку засобів контролю інформаційної системи, відповідно до встановлених організацією вимог до інформаційної безпеки, включаючи технічну відповідність критеріям оцінки на основі вимог інформаційної безпеки, встановлених організації. У цьому документі пропонуються вказівки щодо того, як переглядати та оцінювати засоби контролю інформаційної безпеки, якими керують через систему управління інформаційною безпекою, визначену ISO/IEC 27001. Він застосовний до організацій усіх типів і розмірів, включаючи державні та приватні компанії, державні установи та некомерційні організації, які проводять огляди інформаційної безпеки та перевірки технічної відповідності.

– **ДСТУ ISO/IEC 27009:2018 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Визначення для сфери застосування ISO/IEC 27001. Вимоги (ISO/IEC 27009:2016, IDT) –** Цей документ визначає вимоги до створення галузевих стандартів, які розширюють ISO/IEC 27001 і доповнюють або змінюють ISO/IEC 27002 для підтримки конкретного сектора (домену, області застосування або ринку). Цей документ пояснює, як: включати вимоги на додаток до вимог ISO/IEC 27001: уточнювати або інтерпретувати будь-які вимоги ISO/IEC 27001; включати засоби контролю на додаток до засобів ISO/IEC 27001:2013, Додаток А та ISO/IEC 27002; модифікувати будь-які засоби управління ISO/IEC 27001:2013, додаток А та ISO/IEC 27002; додати настанови до або змінити настанови ISO/IEC 27002. У цьому документі зазначено, що додаткові чи вдосконалені вимоги не роблять вимоги ISO/IEC 27001 недійсними. Цей документ застосовується до тих, хто бере участь у розробці галузевих стандартів.

– **ДСТУ ISO/IEC 27010:2018 Інформаційні технології. Методи захисту. Управління інформаційною безпекою для міжгалузевих та міжорганізаційних комунікацій (ISO/IEC 27010:2015, IDT) –** ISO/IEC 27010:2015 надає рекомендації на додаток до вказівок, наданих у сімействі стандартів ISO/IEC 27000, для впровадження управління інформаційною безпекою в спільнотах обміну інформацією. Цей міжнародний стандарт надає засоби контролю та вказівки, що стосуються, зокрема, ініціювання, впровадження, підтримки та покращення інформаційної безпеки в міжорганізаційних та міжгалузевих комунікаціях. Він містить вказівки та загальні принципи щодо того, як зазначені вимоги можуть бути виконані за допомогою встановлених повідомлень та інших технічних методів. Цей міжнародний стандарт застосовний до всіх форм обміну та спільного використання конфіденційної інформації, як загальнодоступної, так і приватної, на національному та міжнародному рівнях, у межах однієї галузі чи сектора ринку чи між секторами. Зокрема, це може бути застосовано до обміну інформацією та спільного використання, що стосується забезпечення, підтримки та захисту критичної інфраструктури організації або національної держави. Він призначений для підтримки створення довіри під час обміну конфіденційною інформацією та заохочення тим самим міжнародного зростання спільнот обміну інформацією.

– **ДСТУ ISO/IEC 27011:2018 Інформаційні технології. Методи захисту. Настанова для телекомунікаційних організацій щодо управління інформаційною безпекою на основі ISO/IEC 27002 (ISO/IEC 27011:2016, IDT) –** Сфера застосування цієї Рекомендації | ISO/IEC 27011:2016 має визначити настанови, що підтримують впровадження засобів контролю інформаційної безпеки в телекомунікаційних організаціях. Прийняття цієї Рекомендації | ISO/IEC 27011:2016 дозволить телекомунікаційним організаціям відповідати базовим вимогам управління безпекою інформації щодо конфіденційності, цілісності, доступності та будь-яких інших відповідних властивостей безпеки.

– **ДСТУ ISO/IEC 27013:2017 Інформаційні технології. Методи захисту. Настанови для інтегрованого впровадження ISO/IEC 27001 та ISO/IEC 20000-1 (ISO/IEC 27013:2015, IDT) –** ISO/IEC 27013:2021. Інформаційна безпека, кібербезпека та захист конфіденційності – Настанови щодо інтегрованого впровадження ISO/IEC 27001 та ISO/IEC 20000-1 – Цей документ містить вказівки щодо інтегрованого впровадження ISO/IEC 27001 та ISO/IEC 20000-1 для організацій, які мають намір: запровадити ISO/IEC27001, коли вже запроваджено ISO/IEC 20000-1, або навпаки; впроваджувати як ISO/IEC27001, так і ISO/IEC 20000-1 разом; інтегрувати існуючі системи менеджменту на основі ISO/IEC27001 та ISO/IEC 20000-1. Цей документ зосереджується виключно на інтегрованій реалізації системи управління інформаційною безпекою (ISMS), як зазначено в ISO/IEC 27001, і системи управління послугами (SMS), як зазначено в ISO/IEC 20000-1.

– **ISO/IEC 27014:2020. Інформаційна безпека, кібербезпека та захист конфіденційності – Управління інформаційною безпекою** – У цьому документі містяться вказівки щодо концепцій, цілей і процесів управління інформаційною безпекою, за допомогою яких організації можуть оцінювати, спрямовувати, контролювати та передавати пов'язані з інформаційною безпекою процеси всередині організації. Цільова аудиторія цього документа: орган управління та вище керівництво; тих, хто відповідає за оцінку, управління та моніторинг системи управління інформаційною безпекою (СУІБ) на основі ISO/IEC 27001; особи, відповідальні за управління інформаційною безпекою, яке відбувається поза сферою СУІБ на основі ISO/IEC 27001, але в межах сфери управління. Цей документ застосовується до організацій усіх типів і розмірів. Усі посилання на СУІБ у цьому документі стосуються СУІБ на основі ISO/IEC 27001. Цей документ зосереджується на трьох типах організацій СУІБ, наведених у Додатку B. Однак цей документ також може використовуватися іншими типами організацій.

– **ISO/IEC TR 27015:2012. Інформаційні технології – Методи безпеки – Настанови щодо управління інформаційною безпекою для фінансових послуг** – ISO/IEC TR 27015:2012 містить інструкції з інформаційної безпеки, які доповнюють засоби контролю інформаційної безпеки, визначені в ISO/IEC 27002:2005, для ініціювання, впровадження, підтримки та покращення інформаційної безпеки в організаціях, що надають фінансові послуги.

– **ISO/IEC TR 27016:2014. Інформаційні технології – Техніка безпеки – Управління інформаційною безпекою – Економіка організації** – ISO/IEC TR 27016:2014 надає вказівки щодо того, як організація може приймати рішення щодо захисту інформації та розуміння економічних наслідків цих рішень у контексті конкуруючих вимог до ресурсів. ISO/IEC TR 27016:2014 застосовний до організацій усіх типів і розмірів і надає інформацію для прийняття економічних рішень щодо управління інформаційною безпекою вищим керівництвом, яке несе відповідальність за рішення щодо інформаційної безпеки.

– **ДСТУ ISO/IEC 27017:2017 Інформаційні технології. Методи захисту. Звід практик стосовно заходів інформаційної безпеки, що ґрунтуються на ISO/IEC 27002, для хмарних послуг (ISO/IEC 27017:2015, IDT) –** Цей стандарт надає рекомендації щодо заходів інформаційної безпеки, які застосовують для надання та застосування хмарних послуг, за допомогою формування: додаткових рекомендацій щодо впровадження для відповідних заходів безпеки, визначених в ISO/IEC 27002; додаткових заходів безпеки з рекомендаціями щодо впровадження, що конкретно стосуються хмарних послуг. У цьому стандарті наведено заходи безпеки та рекомендації щодо впровадження як для провайдерів, так і для споживачів хмарних послуг.

– **ДСТУ ISO/IEC 27018:2019 Інформаційні технології. Методи захисту. Кодекс усталеної практики для захисту персональної ідентифікаційної інформації (PII) у загальнодоступних хмарах, що діють як процесори PII (ISO/IEC 27018:2019, IDT) –** У цьому документі встановлюються загальноприйняті цілі контролю, засоби контролю та вказівки щодо впровадження заходів із захисту особистої ідентифікаційної інформації (PII) відповідно до принципів конфіденційності в ISO/IEC 29100 для загальнодоступного середовища хмарних обчислень. Зокрема, цей документ містить інструкції на основі ISO/IEC 27002, беручи до уваги нормативні вимоги щодо захисту ідентифікаційної інформації, які можуть бути застосовані в контексті середовища(ів) ризику інформаційної безпеки постачальника публічних хмарних послуг. Цей документ стосується організацій усіх типів і розмірів, у тому числі державних і приватних компаній, державних установ і некомерційних організацій, які надають послуги з обробки інформації як процесори ідентифікаційної інформації через хмарні обчислення за контрактом з іншими організаціями. Рекомендації в цьому документі також можуть стосуватися організацій, які виконують функції контролерів ідентифікаційної інформації. Однак на контролери ідентифікаційної інформації можуть поширюватися додаткові законодавчі акти, положення та зобов'язання щодо захисту ідентифікаційної інформації, які не стосуються обробників ідентифікаційної інформації. Цей документ не призначений для покриття таких додаткових зобов'язань.

– **ДСТУ ISO/IEC 27019:2019 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою для енергопостачальних організацій (ISO/IEC 27019:2017, IDT) –** ISO/IEC 27019:2017 надає вказівки на основі ISO/IEC 27002:2013, застосовані до систем управління процесами, що використовуються в енергетиці для контролю та моніторингу виробництва або виробництва, передачі, зберігання та розподілу електроенергії, газу, нафти та тепла, а також для контролю відповідних допоміжних процесів. Це включає, зокрема, таке: технологія централізованого та розподіленого управління процесами, моніторингу та автоматизації, а також інформаційні системи, що використовуються для їх роботи, такі як пристрої програмування та параметризації; цифрові контролери та компоненти автоматизації, такі як контрольні та польові пристрої або програмовані логічні контролери (PLC), включаючи цифрові датчики та виконавчі елементи; усі додаткові допоміжні інформаційні системи, що використовуються в області управління процесом, наприклад, для додаткових задач візуалізації даних і для контролю, моніторингу, архівування даних, реєстрації історії, звітності та документації; комунікаційна технологія, яка використовується в області управління процесом, наприклад, мережі, телеметрія, програми телеконтролю та технології дистанційного управління; Компоненти розширеної інфраструктури вимірювання (AMI), наприклад розумні лічильники; вимірювальні пристрої, наприклад, для значень викидів; цифрові системи захисту та безпеки, наприклад реле захисту, ПЛК безпеки, механізми аварійного регулювання; системи енергоменеджменту,

наприклад розподілених енергетичних ресурсів (DER), інфраструктури електричних зарядок у приватних домогосподарствах, житлових будинках або промислових установках споживачів; розподілені компоненти середовища інтелектуальної мережі, наприклад, в енергетичних мережах, у приватних домогосподарствах, житлових будинках або промислових установках споживачів; усе програмне забезпечення, мікропрограми та програми, встановлені у вищезазначених системах, наприклад програми DMS (система управління розподілом) або OMS (система управління збоями); будь-які приміщення, в яких розміщено вищезазначене обладнання та системи; системи дистанційного обслуговування вищевказаних систем. ISO/IEC 27019:2017 не застосовується до області управління процесом ядерних установок. Цей домен охоплює стандарт IEC 62645. ISO/IEC 27019:2017 також містить вимогу щодо адаптації процесів оцінки та обробки ризиків, описаних у ISO/IEC 27001:2013, до вказівок, які наведені в цьому документі в секторі енергетики.

– **ДСТУ ISO/IEC 27021:2018 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги до компетенції професіоналів з управління інформацією (ISO/IEC 27021:2017, IDT**) – ISO/IEC 27021:2017 визначає вимоги до компетентності для фахівців із СУІБ, які керують або беруть участь у створенні, впровадженні, підтримці та постійному вдосконаленні одного або кількох процесів системи управління інформаційною безпекою, які відповідають ISO/IEC 27001.

– **ДСТУ ISO/IEC 27031:2015 Інформаційні технології. Методи захисту. Настанови щодо готовності інформаційно-комунікаційних технологій для неперервності роботи бізнесу (ISO/IEC 27031:2011, IDT) –** ISO/IEC 27031:2011 описує концепції та принципи готовності інформаційно-комунікаційних технологій (ІКТ) до безперервності бізнесу та надає структуру методів і процесів для ідентифікації та визначення всіх аспектів (таких як критерії ефективності, проектування та впровадження) для підвищення готовності організації до ІКТ для забезпечення безперервності бізнесу. Це стосується будь-якої організації (приватної, урядової та неурядової, незалежно від розміру), яка розробляє свою програму готовності до ІКТ для забезпечення безперервності бізнесу (IRBC), і вимагає, щоб її послуги/інфраструктури ІКТ були готові підтримувати бізнес-операції у разі виникнення події та інциденти, а також пов’язані з ними збої, які можуть вплинути на безперервність (включаючи безпеку) критичних бізнес-функцій. Сфера застосування ISO/IEC 27031:2011 охоплює всі події та інциденти (включаючи пов’язані з безпекою), які можуть вплинути на інфраструктуру та системи ІКТ. Він включає в себе та розширює практики обробки інцидентів інформаційної безпеки та управління ними, а також планування готовності до ІКТ та послуги.

– **ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT) –** Цей стандарт містить рекомендації щодо підвищення рівня кібербезпеки, розглядаючи різні

аспекти цього питання та їхній зв’язок з іншими видами безпеки, зокрема: інформаційною безпекою; мережевою безпекою; Інтернет-безпекою; захистом інформаційної інфраструктури. У стандарті розглянуто основні методи захисту зацікавлених сторін у кіберпросторі. Стандарт містить: огляд кібербезпеки; пояснення зв’язків між кібербезпекою та іншими видами безпеки; визначення зацікавлених сторін та їхньої ролі в кіберпросторі; настанова з вирішення основних питань кібербезпеки; способи взаємодії зацікавлених сторін для вирішення основних питань кібербезпеки. Цей стандарт стосується постачальників послуг у кіберпросторі. Але цільова аудиторія охоплює також споживачів, які користуються цими послугами. Якщо організації надають послуги в кіберпросторі іншим організаціям або людям для домашнього використання, то таким організаціям може знадобитися підготувати настанови на основі цього стандарту, які міститимуть додаткові пояснення або приклади, необхідні для повного розуміння читачами того, як треба діяти.

– **ДСТУ ISO/IEC 27033:2017. Інформаційні технології. Методи захисту. Безпека мережі. – складається з 6 частин:**

– ДСТУ ISO/IEC 27033-1:2017 Інформаційні технології. Методи захисту. Захист мережі. Частина 1. Огляд і поняття (ISO/IEC 27033-1:2015, IDT) – ISO/IEC 27033-1:2015 містить огляд мережевої безпеки та відповідних визначень. Він визначає й описує концепції, пов’язані з мережевою безпекою, і надає вказівки щодо управління нею. (Мережева безпека стосується безпеки пристроїв, безпеки управлінських дій, пов’язаних із пристроями, програмами/службами та кінцевими користувачами, на додаток до безпеки інформації, що передається через канали зв’язку.) Це актуально для всіх, хто бере участь у володінні, експлуатації або використанні мережі. Це включає керівників вищої ланки та інших нетехнічних менеджерів або користувачів, на додаток до керівників і адміністраторів, які мають конкретні обов’язки за інформаційну безпеку та/або безпеку мережі, роботу мережі або які відповідають за загальну програму безпеки організації та розробку політики безпеки. Це також актуально для всіх, хто бере участь у плануванні, проектуванні та реалізації архітектурних аспектів безпеки мережі. ISO/IEC 27033-1:2015 також включає наступне: надає вказівки щодо того, як ідентифікувати та аналізувати ризики безпеки мережі та визначення вимог безпеки мережі на основі цього аналізу; надає огляд елементів управління, які підтримують архітектури технічної безпеки мережі та відповідні технічні засоби контролю, а також тих нетехнічних засобів контролю та технічних засобів контролю, які застосовуються не лише до мереж; знайомить із тим, як досягти високоякісної архітектури технічної безпеки мережі, а також аспекти ризику, дизайну та контролю, пов’язані з типовими мережевими сценаріями та областями мережевих «технологій» (які детально розглядаються в наступних частинах ISO/IEC 27033), і коротко розглядає питання, пов'язані з впровадженням і експлуатацією засобів контролю безпеки мережі, а також постійний моніторинг і перегляд їх впровадження. Загалом він містить огляд цього міжнародного стандарту та «дорожню карту» для всіх інших частин.

– ДСТУ ISO/IEC 27033-2:2016 Інформаційні технології. Методи захисту. Безпека мережі. Частина 2. Настанови щодо проектування та реалізації безпеки мережі (ISO/IEC 27033-2:2012, IDT) – ISO/IEC 27033-2:2012 містить вказівки для організацій щодо планування, проектування, впровадження та документування безпеки мережі.

– ДСТУ ISO/IEC 27033-3:2016 Інформаційні технології. Методи захисту. Безпека мережі. Частина 3. Еталонні мережеві сценарії. Загрози, методи проектування та проблеми управління (ISO/IEC 27033-3:2010, IDT) – ISO/IEC 27033-3:2010 описує загрози, методи проектування та проблеми управління, пов'язані зі сценаріями еталонної мережі. Для кожного сценарію в ньому надаються детальні вказівки щодо загроз безпеці, а також методи розробки безпеки та засоби контролю, необхідні для пом'якшення пов'язаних ризиків. У відповідних випадках він містить посилання на ISO/IEC 27033-4 – ISO/IEC 27033-6, щоб уникнути дублювання змісту цих документів. Інформація в ISO/IEC 27033-3:2010 призначена для використання під час перегляду архітектури/проекту технічної безпеки та під час вибору та документування бажаної архітектури/проекту технічної безпеки та пов'язаних засобів контролю безпеки відповідно до ISO/IEC 27033-2. Вибрана конкретна інформація (разом з інформацією, вибраною з ISO/IEC 27033-4 до ISO/IEC 27033-6) залежатиме від характеристик мережевого середовища, що перевіряється, тобто конкретного мережевого сценарію(ів) і теми «технології». Загалом, ISO/IEC 27033-3:2010 суттєво допоможе в комплексному визначенні та реалізації безпеки для мережевого середовища будь-якої організації.

– ДСТУ ISO/IEC 27033-4:2016 Інформаційні технології. Методи захисту. Безпека мережі. Частина 4. Убезпечення комунікацій між мережами з використанням шлюзів безпеки (ISO/IEC 27033-4:2014, IDT) – ISO/IEC 27033-4:2014 містить настанови щодо захисту зв'язку між мережами за допомогою шлюзів безпеки (брандмауер, брандмауер програм, система захисту від вторгнень тощо) відповідно до задокументованої політики інформаційної безпеки шлюзів безпеки, включаючи: виявлення та аналіз загроз мережевій безпеці, пов'язаних зі шлюзами безпеки; визначення вимог безпеки мережі для шлюзів безпеки на основі аналізу загроз; використання методів для проектування та впровадження для вирішення загроз та аспектів контролю, пов'язаних із типовими мережевими сценаріями; вирішення проблем, пов'язаних із впровадженням, експлуатацією, моніторингом та переглядом елементів управління шлюзом безпеки мережі.

– ДСТУ ISO/IEC 27033-5:2016 Інформаційні технології. Методи захисту. Безпечність мережі. Частина 5. Убезпечення комунікацій уздовж мереж із використанням віртуальних приватних мереж (VPNs) (ISO/IEC 27033-5:2013, IDT) – ISO/IEC 27033-5:2013 містить вказівки щодо вибору, впровадження та моніторингу технічних засобів контролю, необхідних для забезпечення безпеки мережі за допомогою з'єднань віртуальної приватної мережі (VPN) для з'єднання мереж і підключення віддалених користувачів до мереж.

– ДСТУ ISO/IEC 27033-6:2018 Інформаційні технології. Методи захисту. Безпека мережі. Частина 6. Забезпечення безпроводового доступу до IP-мережі (ISO/IEC 27033-6:2016, IDT) – ISO/IEC 27033-6:2016 описує загрози, вимоги безпеки, контроль безпеки та методи проектування, пов'язані з безпроводовими мережами. Він містить вказівки щодо вибору, впровадження та моніторингу технічних засобів контролю, необхідних для забезпечення безпечного зв'язку за допомогою безпроводових мереж. Інформація в цій частині ISO/IEC 27033 призначена для використання під час перегляду або вибору архітектури/проекту технічної безпеки, які передбачають використання безпроводової мережі відповідно до ISO/IEC 27033-2. Загалом, ISO/IEC 27033-6 значно допоможе у всебічному визначенні та реалізації безпеки для безпроводового мережевого середовища будь-якої організації. Він призначений для користувачів і розробників, які відповідають за впровадження та підтримку технічного контролю, необхідного для забезпечення безпечних безпроводових мереж.

ISO/IEC CD 27033-7. Інформаційна технологія. Безпека мережі. Частина 7. Настанови щодо безпеки віртуалізації мережі – В стадії розробки

ДСТУ ISO/IEC 27034:2017 Інформаційні технології. Методи захисту. Безпека програм. – складається з 7 частин:

– ДСТУ ISO/IEC 27034-1:2017 Інформаційні технології. Методи захисту. Безпека прикладних програм. Частина 1. Огляд і загальні поняття (ISO/IEC 27034-1:2011; Cor 1:2014, IDT) – ISO/IEC 27034 надає організаціям інструкції, які допомагають інтегрувати безпеку в процеси, які організації використовують для управління своїми додатками. У цьому стандарті наведено загальний огляд безпеки додатків. Вона представляє визначення, принципи та процеси, які стосуються безпеки додатків. ISO/IEC 27034 можна застосовувати для додатків, розроблених в організації чи придбаних у третьої сторони, а також у разі аутсорсингу розроблення чи експлуатації додатків.

– ДСТУ ISO/IEC 27034-2:2016 Інформаційні технології. Методи захисту. Безпека прикладних програм. Частина 2. Основні нормативні положення організації (ISO/IEC 27034-2:2015, IDT) – ISO/IEC 27034-2:2015 містить детальний опис нормативної бази організації та надає керівництво для організацій щодо її впровадження.

– ДСТУ ISO/IEC 27034-3:2018 Інформаційні технології. Методи захисту. Безпека прикладних програм. Частина 3. Процес управління безпекою прикладних програм (ISO/IEC 27034-3:2018, IDT) – У цьому документі міститься детальний опис і інструкції щодо впровадження процесу управління безпекою додатків.

– ДСТУ ISO/IEC TS 27034-5-1:2019 Інформаційні технології. Захист застосунків. Частина 5-1. Структура даних управління протоколами та захистом застосунків. Схеми XML (ISO/IEC TS 27034-5-1:2018, IDT) – ISO/IEC 27034-5 описує та пояснює мінімальний набір основних атрибутів контролю безпеки додатків (ASC), а також докладно описує дії та ролі еталонної моделі життєвого циклу безпеки додатків (ASLCRM).

– ДСТУ ISO/IEC 27034-6:2018 Інформаційні технології. Методи захисту. Безпека прикладних програм. Частина 6. Вивчення випадків (ISO/IEC 27034-6:2016, IDT) – ISO/IEC 27034-6:2016 надає приклади використання ASC для конкретних застосувань. Зазначені тут ASC надаються лише з метою пояснення, і аудиторії рекомендується створити власні ASC для забезпечення безпеки програми.

– ISO/IEC 27034-7:2018. Інформаційні технології. Безпека додатків. Частина 7. Структура прогнозування впевненості – Цей документ описує мінімальні вимоги, коли необхідні дії, визначені контролем безпеки додатків (ASC), замінюються обґрунтуванням безпеки додатків прогнозування (PASR). ASC, зіставлений із PASR, визначає очікуваний рівень довіри для наступної програми. У контексті очікуваного рівня довіри завжди існує оригінальна заявка, у якій команда проекту виконувала дії зазначеного ASC для досягнення фактичного рівня довіри. Використання обґрунтувань безпеки додатків прогнозування (PASR), визначених у цьому документі, застосовується до проектних груп, які мають визначену нормативну структуру додатків (ANF) і оригінальну програму з фактичним рівнем довіри. Прогнози щодо агрегування кількох компонентів або історії розробника щодо інших програм виходять за рамки цього документа.

– ДСТУ ISO/IEC 27035:2018 Інформаційні технології. Методи захисту. Управління інцидентами інформаційної безпеки. – складається з 4 частин:

– ДСТУ ISO/IEC 27035-1:2018 Інформаційні технології. Методи захисту. Управління інцидентами інформаційної безпеки. Частина 1. Принципи управління інцидентами (ISO/IEC 27035-1:2016, IDT) – ISO/IEC 27035-1:2016 є основою цього багатокомпонентного міжнародного стандарту. Він представляє основні концепції та етапи управління інцидентами інформаційної безпеки та поєднує ці концепції з принципами в структурованому підході до виявлення, звітування, оцінювання та реагування на інциденти, а також застосування отриманих уроків. Принципи, наведені в ISO/IEC 27035-1:2016, є загальними та призначені для застосування в усіх організаціях, незалежно від типу, розміру чи природи. Організації можуть коригувати вказівки, наведені в ISO/IEC 27035-1:2016, відповідно до свого типу, розміру та характеру бізнесу щодо ситуації ризику інформаційної безпеки. Це також стосується зовнішніх організацій, які надають послуги з управління інцидентами інформаційної безпеки.

– ДСТУ ISO/IEC 27035-2:2018 Інформаційні технології. Методи захисту. Управління інцидентами інформаційної безпеки. Частина 2. Настанова щодо планування та підготовки до реагування на інциденти (ISO/IEC 27035-2:2016, IDT) – ISO/IEC 27035-2:2016 надає рекомендації щодо планування та підготовки до реагування на інциденти. Рекомендації базуються на етапі «Планування та підготовка» та етапі «Здобуті уроки» моделі «Фази управління інцидентами інформаційної безпеки», представленої в ISO/IEC 27035-1. Основні моменти на етапі «Планування та підготовка» включають наступне: політика управління інцидентами інформаційної безпеки та зобов'язання вищого керівництва політики інформаційної безпеки, включаючи ті, що стосуються управління

ризиками, оновлені як на корпоративному рівні, так і на рівні системи, сервісу та мережі план управління інцидентами інформаційної безпеки створення групи реагування на інциденти (IRT) встановлювати стосунки та зв'язки з внутрішніми та зовнішніми організаціями технічне та інше забезпечення (включаючи організаційне та операційне) інструктажі та тренінги з управління інцидентами інформаційної безпеки тестування плану управління інцидентами інформаційної безпеки. Принципи, наведені в цій частині ISO/IEC 27035, є загальними та призначені для застосування в усіх організаціях, незалежно від типу, розміру чи природи. Організації можуть коригувати вказівки, надані в цій частині ISO/IEC 27035, відповідно до їх типу, розміру та характеру бізнесу щодо ситуації ризику інформаційної безпеки. Ця частина ISO/IEC 27035 також застосовується до зовнішніх організацій, що надають послуги з управління інцидентами інформаційної безпеки.

– ISO/IEC 27035-3:2020. Інформаційна технологія. Управління інцидентами інформаційної безпеки. Частина 3. Настанови щодо операцій реагування на інциденти ІКТ – У цьому документі містяться вказівки щодо реагування на інциденти інформаційної безпеки в операціях безпеки ІКТ. Цей документ робить це, по-перше, охоплюючи операційні аспекти операцій безпеки ІКТ з точки зору людей, процесів і технологій. Далі він зосереджується на реагуванні на інциденти інформаційної безпеки в операціях безпеки ІКТ, включаючи виявлення інцидентів інформаційної безпеки, звітування, сортування, аналіз, реагування, стримування, викорінення, відновлення та завершення. Цей документ не стосується операцій реагування на інциденти, не пов’язані з ІКТ, як-от втрата паперових документів. Цей документ базується на фазі «Виявлення та звітування», фазі «Оцінка та прийняття рішення» та фазі «Відповіді» моделі «Фази управління інцидентами інформаційної безпеки», представленої в ISO/IEC 27035-1:2016. Принципи, наведені в цьому документі, є загальними та призначені для застосування в усіх організаціях, незалежно від типу, розміру чи природи. Організації можуть коригувати положення, наведені в цьому документі, відповідно до свого типу, розміру та характеру бізнесу щодо ситуації ризику інформаційної безпеки. Цей документ також стосується зовнішніх організацій, які надають послуги з управління інцидентами інформаційної безпеки.

– ISO/IEC CD 27035-4. Інформаційні технології. Управління інцидентами інформаційної безпеки. Частина 4. Координація – В стадії розробки

– ДСТУ ISO/IEC 27036:2017 Інформаційні технології. Методи захисту. Інформаційна безпека у відносинах із постачальниками. – складається з 4 частин:

– ДСТУ ISO/IEC 27036-1:2017 Інформаційні технології. Методи захисту. Інформаційна безпека у відносинах із постачальниками. Частина 1. Огляд та поняття (ISO/IEC 27036-1:2014, IDT) – Цей документ є вступною частиною ISO/IEC 27036. Він містить огляд настанов, спрямованих на допомогу організаціям у захисті їх інформації та інформаційних систем у контексті відносин з постачальниками. Він також представляє концепції, які детально

описані в інших частинах ISO/IEC 27036. Цей документ розглядає точки зору як покупців, так і постачальників.

– ДСТУ ISO/IEC 27036-2:2017 Інформаційні технології. Методи захисту. Інформаційна безпека у відносинах з постачальниками. Частина 2. Вимоги (ISO/IEC 27036-2:2014, IDT) – Цей документ визначає фундаментальні вимоги інформаційної безпеки для визначення, впровадження, експлуатації, моніторингу, перегляду, підтримки та покращення відносин постачальника та покупця. Ці вимоги охоплюють будь-яку закупівлю та постачання продуктів і послуг, таких як виробництво або складання, закупівля бізнес-процесів, програмних і апаратних компонентів, закупівля процесу знань, створення-експлуатація-передача та послуги хмарних обчислень. Цей документ застосовується до всіх організацій, незалежно від типу, розміру та характеру. Щоб відповідати вимогам, очікується, що організація запровадила всередині ряд базових процесів або активно планує це зробити. Ці процеси включають, але не обмежуються: управління бізнесом, управління ризиками, управління операційними й людськими ресурсами та інформаційна безпека.

– ДСТУ ISO/IEC 27036-3:2017 Інформаційні технології. Методи захисту. Інформаційна безпека у відносинах з постачальниками. Частина 3. Настанови щодо безпеки ланцюга постачання інформаційних та комунікаційних технологій (ISO/IEC 27036-3:2013, IDT) – ISO/IEC 27036-3:2013 надає покупцям продуктів і послуг і постачальникам у ланцюзі постачання інформаційно-комунікаційних технологій (ІКТ) настанови щодо: отримання видимості та управління ризиками інформаційної безпеки, спричиненими фізично розосередженими та багаторівневими ланцюгами постачання ІКТ; реагування на ризики, пов’язані з глобальним ланцюгом постачання ІКТ-продуктів і послуг, які можуть мати вплив на інформаційну безпеку організацій, які використовують ці продукти та послуги. Ці ризики можуть бути пов’язані як з організаційними, так і з технічними аспектами (наприклад, введення шкідливого коду або наявність підроблених продуктів інформаційних технологій (IT); інтеграція процесів і практик інформаційної безпеки в процеси життєвого циклу системи та програмного забезпечення, описані в ISO/IEC 15288 та ISO/IEC 12207, одночасно підтримуючи засоби контролю інформаційної безпеки, описані в ISO/IEC 27002. ISO/IEC 27036-3:2013 не включає питання управління безперервністю бізнесу/відмовостійкості, пов’язані з ланцюгом постачання ІКТ. ISO/IEC 27031 стосується безперервності бізнесу.

– ДСТУ ISO/IEC 27036-4:2018 Інформаційні технології. Методи захисту. Інформаційна безпека у відносинах з постачальниками. Частина 4. Настанова щодо безпеки хмарних послуг (ISO/IEC 27036-4:2016, IDT) – ISO/IEC 27036-4:2016 надає клієнтам хмарних послуг і постачальникам хмарних послуг рекомендації щодо отримання інформації про ризики інформаційної безпеки, пов’язані з використанням хмарних служб, і ефективне управління цими ризиками, а також реагування на ризики, характерні для придбання або надання хмарних послуг, які можуть мати вплив на інформаційну безпеку організацій, які використовують ці служби. ISO/IEC 27036-4:2016 не включає питання управління безперервністю бізнесу/відмовостійкості, пов’язані з хмарною

службою. ISO/IEC 27031 стосується безперервності бізнесу. ISO/IEC 27036-4:2016 не надає вказівок щодо того, як постачальник хмарних послуг повинен запроваджувати, керувати та керувати інформаційною безпекою. Інструкції щодо них можна знайти в ISO/IEC 27002 та ISO/IEC 27017. Сфера застосування ISO/IEC 27036-4:2016 полягає у визначенні настанов, що підтримують впровадження управління безпекою інформації для використання хмарних служб.

– **ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (ISO/IEC 27037:2012, IDT) –** Цей стандарт надає настанови для специфічної діяльності з оброблення потенційних цифрових доказів, такими процесами є: ідентифікація, збирання, здобуття та збереження потенційних цифрових доказів. Ці процеси потрібні під час слідства для підтримання цілісності цифрових доказів – прийнятна методологія отримання цифрових доказів, яка буде забезпечувати їхню допустимість у законодавчих та дисциплінарних судових процесах, а також інших потрібних інстанціях. Цей стандарт також надає загальні настанови стосовно збирання нецифрових доказів, які можуть буті корисними на стадії аналізування потенційних цифрових доказів. Цей стандарт також спрямовано на інформування осіб, які приймають рішення, та тих, кому потрібно визначати надійність потенційних цифрових доказів, що були їм надані. Він прийнятний для організацій, яким необхідно захищати, аналізувати та презентувати потенційні цифрові докази. Він важливий для поліцейських підрозділів, які формують та запроваджують процедури щодо цифрових доказів, часто як частину доказів більшого об'єму. Потенційні цифрові докази, розглянуті в цьому стандарті, можуть мати походження з різних типів цифрових пристроїв, мереж, баз даних тощо. Вони стосуються даних, які вже є в цифровому форматі. Цей стандарт не намагається охопити перетворення аналогових даних у цифровий формат. Завдяки недовговічності цифрових доказів потрібно мати прийнятну методологію для гарантування цілісності та автентичності потенційних цифрових доказів. Цей стандарт не вимагає обов'язкового використання винятковых інструментів або методів. Ключовим компонентом, який забезпечує довіру в розслідуваннях, є методологія, яку застосовують протягом цього процесу, та особи, що мають кваліфікацію для виконання завдань, визначених цією методологією. Цей стандарт не стосується методології для законодавчих та дисциплінарних судових процесів, а також інших пов'язаних діяльностей під час оброблення потенційних цифрових доказів, які знаходяться поза межами сфери ідентифікації, збирання, здобуття та збереження. Запровадження цього стандарту потребує відповідності національним законам, правилам та нормативним документам. Він не повинен заміняти специфічні законодавчі вимоги будь-якої юрисдикції. Фактично, він може слугувати практичною настановою для DEFR або DES у дослідженнях, які охоплюють потенційні цифрові докази. Він не впливає на аналізування цифрових доказів та не замінює специфічних юридичних вимог, що стосуються таких питань, як визнання доказів, доказова вага, значущість та інші юридично

контрольовані обмеження використання потенційних цифрових доказів у судах. Цей стандарт може допомогти у сприянні обміну потенційними цифровими доказами між юрисдикціями. Для підтримання цілісності цифрових доказів користувачам цього стандарту потрібно адаптувати та скоригувати процедури, описані в цьому стандарті, відповідно до специфічних законодавчих вимог юрисдикції для доказів. Хоча цей стандарт не охоплює судової готовності, відповідна судова готовність може бути значною мірою підтримана процесами ідентифікації, збирання, здобуття та збереження цифрових доказів. Судова готовність – це досягнення відповідного рівня здатності організації для спроможності ідентифікації, збирання, здобуття, збереження, захисту та аналізування цифрових доказів. Незважаючи на те, що процеси та діяльності, описані в цьому стандарті, є в основному реактивними заходами, використовуваними в розслідуваннях інциденту після того, як він вже трапився, судова готовність є проективним процесом спроби планування процесу дослідження інциденту. Цей стандарт відповідає ISO/IEC 27001 та ISO/IEC 27002, зокрема вимогам заходів щодо безпеки стосовно потенційних цифрових доказів за допомогою надання додаткової настанови щодо запровадження. Крім того, цей стандарт має застосування в контексті, незалежному від ISO/IEC 27001 та ISO/IEC 27002. Цей стандарт потрібно розглядати разом з іншими стандартами, пов’язаними з цифровими доказами та розслідуваннями інцидентів інформаційної безпеки. Цей стандарт надає настанови для специфічної діяльності з оброблення цифрових доказів, а саме: ідентифікації, збирання, здобуття та збереження цифрових доказів, що можуть мати доказове значення. Цей стандарт надає настанови для фахівців стосовно звичайних випадків, які трапляються в процесі оброблення цифрових доказів, та допомагає організаціям в їхніх дисциплінарних процедурах та забезпеченні обміну потенційними цифровими доказами між юрисдикціями. Цей стандарт надає настанови для таких пристроїв та/або функцій, використовуваних за різних обставин: Носій для зберігання цифрових даних, використовуваний у стандартних комп’ютерах, подібний жорстким дискам, гнучким дискам, оптичним і магнітооптичним дискам, цифровим пристроям з подібними функцпми; Мобільні телефони, Персональні цифрові помічники (PDAs), Персональні електронні прилади (PEDs), карти пам’яті; Мобільні навігаційні системи; Цифрові фото- та відеокамери (зокрема CCTV); Стандартний комп’ютер з мережевими з'єднаннями; Мережі, які ґрунтовані на TCP/IP та інших цифрових протоколах; Прилади з функціями, подібними наведеним вище.

– **ДСТУ ISO/IEC 27038:2018 Інформаційні технології. Методи захисту. Специфікація цифрового редагування (ISO/IEC 27038:2014, IDT) –** ISO/IEC 27038:2014 визначає характеристики методів виконання цифрового редагування цифрових документів. Він також визначає вимоги до засобів редагування програмного забезпечення та методів перевірки надійності цифрового редагування. ISO/IEC 27038:2014 не включає редагування інформації з баз даних.

– **ДСТУ ISO/IEC 27039:2017 Інформаційні технології. Методи захисту. Вибирання, розгортання та експлуатування систем виявлення та запобігання вторгненням (IDPS) (ISO/IEC 27039:2015, IDT) –** ISO/IEC 27039:2015 надає рекомендації для допомоги організаціям у підготовці до розгортання систем виявлення та запобігання вторгненням (IDPS). Зокрема, йдеться про вибір, розгортання та роботу IDPS. Він також містить довідкову інформацію, на основі якої походять ці рекомендації.

– **ДСТУ ISO/IEC 27040:2016 Інформаційні технології. Методи захисту. Безпека зберігання (ISO/IEC 27040:2015, IDT) –** ISO/IEC 27040:2015 надає детальні технічні вказівки щодо того, як організації можуть визначити відповідний рівень зниження ризику за допомогою перевіреного та послідовного підходу до планування, проектування, документування та реалізації безпеки зберігання даних. Безпека зберігання стосується захисту (безпеки) інформації, де вона зберігається, і безпеки інформації, що передається через канали зв'язку, пов'язані зі зберіганням. Безпека зберігання включає безпеку пристроїв і носіїв, безпеку дій з управління, пов'язаних із пристроями та носіями, безпеку програм і служб, а також безпеку, актуальну для кінцевих користувачів протягом усього терміну служби пристроїв і носіїв і після завершення використання. Безпека зберігання актуальна для всіх, хто бере участь у володінні, експлуатації або використанні пристроїв зберігання даних, засобів масової інформації та мереж. Це включає керівників вищої ланки, покупців продуктів і послуг зберігання та інших нетехнічних менеджерів або користувачів, на додаток до менеджерів і адміністраторів, які мають конкретні обов'язки за інформаційну безпеку чи безпеку зберігання, роботу сховища або які відповідають за загальну безпеку організації розробка програми та політики безпеки. Це також актуально для всіх, хто бере участь у плануванні, проектуванні та реалізації архітектурних аспектів безпеки мережі зберігання. ISO/IEC 27040:2015 містить огляд концепцій безпеки зберігання та відповідних визначень. Він містить вказівки щодо загроз, дизайну та аспектів контролю, пов'язаних із типовими сценаріями зберігання та областями технологій зберігання. Крім того, він надає посилання на інші міжнародні стандарти та технічні звіти, які стосуються існуючих практик і методів, які можуть бути застосовані для безпеки зберігання.

– ДСТУ ISO/IEC 27041:2016 Інформаційні технології. Методи захисту. Посібник із забезпечення прийнятності та адекватності методів розслідування (ISO/IEC 27041:2015, IDT) – ISO/IEC 27041:2015 надає вказівки щодо механізмів забезпечення того, що методи та процеси, які використовуються під час розслідування інцидентів інформаційної безпеки, «відповідають меті». Він інкапсулює найкращі практики щодо визначення вимог, опису методів і надання доказів того, що реалізації методів можна показати, що задовольняють вимоги. Він включає в себе розгляд того, як тестування постачальників і третіх сторін можна використовувати для сприяння цьому процесу гарантії. Цей документ має на меті: надавати вказівки щодо збору й аналізу функціональних і нефункціональних вимог, пов'язаних із розслідуванням інцидентів

інформаційної безпеки (IS); давати вказівки щодо використання валідації як засобу забезпечення придатності процесів, залучених до розслідування; надати вказівки щодо оцінювання необхідних рівнів валідації та доказів, необхідних для перевірки; надати вказівки щодо того, як зовнішнє тестування та документацію можна включити в процес валідації.

– **ДСТУ ISO/IEC 27042:2016 Інформаційні технології. Методи захисту. Настанови щодо аналізу та інтерпретації цифрового доказу (ISO/IEC 27042:2015, IDT) –** ISO/IEC 27042:2015 містить настанови щодо аналізу та інтерпретації цифрових доказів у спосіб, який розглядає питання безперервності, валідності, відтворюваності та повторюваності. Він інкапсулює найкращі практики для вибору, проектування та реалізації аналітичних процесів і запису достатньої інформації, щоб такі процеси могли бути піддані незалежному контролю, коли це необхідно. У ньому містяться вказівки щодо належних механізмів демонстрації кваліфікації та компетентності слідчої групи. Аналіз та інтерпретація цифрових доказів може бути складним процесом. За деяких обставин може бути застосовано кілька методів, і члени слідчої групи повинні будуть обґрунтувати свій вибір певного процесу та показати, наскільки він еквівалентний іншому процесу, який використовують інші дослідники. За інших обставин дослідникам, можливо, доведеться розробити нові методи дослідження цифрових доказів, які раніше не розглядалися, і вони повинні мати можливість показати, що отриманий метод «відповідає меті». Застосування певного методу може вплинути на інтерпретацію цифрових доказів, оброблених цим методом. Наявні цифрові докази можуть впливати на вибір методів для подальшого аналізу цифрових доказів, які вже були отримані. ISO/IEC 27042:2015 забезпечує загальну структуру для аналітичних та інтерпретаційних елементів обробки інцидентів безпеки інформаційних систем, які можуть бути використані для допомоги у впровадженні нових методів і забезпечують мінімальний загальний стандарт для цифрових доказів, отриманих у результаті такої діяльності.

– **ДСТУ ISO/IEC 27043:2016 Інформаційні технології. Методи захисту. Принципи та процеси розслідування інцидентів (ISO/IEC 27043:2015, IDT) –** ISO/IEC 27043:2015 надає вказівки на основі ідеалізованих моделей для загальних процесів розслідування інцидентів у різних сценаріях розслідування інцидентів із використанням цифрових доказів. Це включає процеси від підготовки до інциденту до закриття розслідування, а також будь-які загальні поради та застереження щодо таких процесів. Інструкції описують процеси та принципи, застосовні до різних типів розслідувань, включаючи, але не обмежуючись, несанкціонований доступ, пошкодження даних, збої системи або корпоративні порушення інформаційної безпеки, а також будь-які інші цифрові розслідування. Підсумовуючи, цей міжнародний стандарт надає загальний огляд усіх принципів і процесів розслідування інцидентів, не вказуючи конкретних деталей у рамках кожного з принципів і процесів розслідування, охоплених цим міжнародним стандартом. Багато інших відповідних міжнародних стандартів, де

є посилання в цьому міжнародному стандарті, надають більш детальний зміст конкретних принципів і процесів розслідування.

–ДСТУ ISO/IEC 27050-1:2018 Інформаційні технології. Методи захисту. Електронне виявлення. – складається з 4 частин:

– ДСТУ ISO/IEC 27050-1:2018 Інформаційні технології. Методи захисту. Електронне виявлення. Частина 1. Огляд та поняття (ISO/IEC 27050-1:2016, IDT) – Електронне відкриття – це процес виявлення відповідної інформації, що зберігається в електронному вигляді (ESI) або даних, однією чи декількома сторонами, залученими до розслідування, судового розгляду чи подібного процесу. Цей документ містить огляд електронного відкриття. Крім того, у ньому даються визначення пов'язаних термінів і описуються концепції, включаючи, але не обмежуючись цим, ідентифікацію, збереження, збір, обробку, перегляд, аналіз і виробництво ESI. Цей документ також визначає інші відповідні стандарти (наприклад, ISO/IEC 27037) і те, як вони стосуються та взаємодіють із діяльністю з електронних відкриттів. Цей документ стосується як нетехнічного, так і технічного персоналу, який бере участь у деяких або всіх видах електронної техніки.

– ISO/IEC 27050-2:2018. Інформаційна технологія. Електронне відкриття. Частина 2. Керівництво з управління електронним відкриттям – У цьому документі містяться вказівки для технічного та нетехнічного персоналу на вищому рівні керівництва в організації, включно з тими, хто відповідає за дотримання законодавчих і нормативних вимог, а також галузевих стандартів. Він описує, як такий персонал може ідентифікувати ризики, пов'язані з електронним відкриттям, і взяти на себе відповідальність за них, встановити політику та досягти відповідності відповідним зовнішнім і внутрішнім вимогам. Він також пропонує, як виробити такі політики у формі, яка може інформувати процес управління. Крім того, він містить вказівки щодо того, як запроваджувати та контролювати електронні відкриття відповідно до політики.

– ДСТУ ISO/IEC 27050-3:2018 Інформаційні технології. Методи захисту. Електронне виявлення. Частина 3. Звід правил для електронного виявлення (ISO/IEC 27050-3:2017, IDT) – У цьому документі містяться вимоги та рекомендації щодо діяльності з електронного відкриття, включаючи, але не обмежуючись, ідентифікацію, збереження, збір, обробку, перегляд, аналіз і створення електронно збереженої інформації (ESI). Крім того, цей документ визначає відповідні заходи, які охоплюють життєвий цикл ESI від його початкового створення до остаточної ліквідації. Цей документ стосується як нетехнічного, так і технічного персоналу, який бере участь у деяких або всіх видах електронної техніки. Важливо зазначити, що користувач повинен знати про будь-які застосовні вимоги юрисдикції.

– ISO/IEC 27050-4:2021. Інформаційні технології – Електронне відкриття – Частина 4: Технічна готовність – У цьому документі містяться вказівки щодо того, як організація може планувати, готуватися до та впроваджувати електронне відкриття з точки зору як технологій, так і процесів. Цей документ містить вказівки щодо профілактичних заходів, які можуть

допомогти забезпечити ефективне та відповідне електронне відкриття та процеси. Цей документ стосується як нетехнічного, так і технічного персоналу, який бере участь у деяких або всіх видах електронної техніки.

– ISO/IEC 27099:2022. Інформаційні технології – Інфраструктура відкритих ключів – Практика та рамки політики – У цьому документі встановлюється система вимог до управління інформаційною безпекою для постачальників довірчих послуг інфраструктури відкритих ключів (PKI) через політику сертифікації, положення про практику сертифікації та, де це можливо, їх внутрішню підтримку системою управління інформаційною безпекою (СУІБ) (ISMS). Структура вимог включає оцінку та обробку ризиків інформаційної безпеки, адаптованих для задоволення узгоджених вимог користувачів до послуг, як зазначено в політиці сертифікатів. Цей документ також призначений для того, щоб допомогти постачальникам послуг довіри підтримувати кілька політик сертифікатів. У цьому документі розглядається життєвий цикл сертифікатів відкритих ключів, які використовуються для цифрових підписів, автентифікації або встановлення ключа для шифрування даних. У ньому не йдеться про методи автентифікації, вимоги щодо неспростування або протоколи управління ключами, засновані на використанні сертифікатів відкритих ключів. Для цілей цього документа термін «сертифікат» стосується сертифікатів відкритих ключів. Цей документ не застосовується до сертифікатів атрибутів. У цьому документі використовуються концепції та вимоги СУІБ, як визначено в сімействі стандартів ISO/IEC 27000. Він використовує кодекс практики для контролю інформаційної безпеки, як визначено в ISO/IEC 27002. Конкретні вимоги до PKI (наприклад, вміст сертифіката, перевірка ідентичності, обробка відкликання сертифіката) не розглядаються безпосередньо СУІБ, як визначено в ISO/IEC 27001. Використання ISMS або еквівалента адаптовано до застосування вимог до служби PKI, зазначених у політиці сертифікатів, як описано в цьому документі. Постачальник довірчих послуг PKI – це спеціальний клас довірчих послуг для використання сертифікатів відкритих ключів. Цей документ розрізняє системи PKI, які використовуються в закритому, відкритому та договірному середовищах. Цей документ призначений для полегшення впровадження операційного, базового контролю та практики в договірному середовищі. Хоча цей документ зосереджений на договірному середовищі, застосування цього документа до відкритих чи закритих середовищ не виключається.

Розділ 3. Інструментальні та прикладні застосунки в інформаційній та/або кібербезпеці

3.1. Мережева модель OSI.
3.2. Основні протоколи стеку TCP/IP.
3.3. Віртуалізація (принципи, гіпервізори).
3.4. Архітектура комп'ютерів.

3.1. Мережева модель OSI

Комп'ютерна мережа – це об'єднання двох або більше комп'ютерів та/або комп'ютерного обладнання (сервери, маршрутизатори та ін.) з метою спільної обробки, зберігання або передачі даних.

За призначенням комп'ютерні мережі розподіляються на:
1. Обчислювальні.
2. Інформаційні.
3. Змішані.

Обчислювальні мережі призначені головним чином для рішення завдань користувачів з обміном даними між їхніми абонентами. **Інформаційні мережі** орієнтовані в основному на надання інформаційних послуг користувачам.

Змішані мережі сполучають функції перших двох.

Мережева модель – теоретичний опис принципів роботи набору взаємодіючих один з одним мережевих протоколів.

Модель звичайно ділиться на рівні, так щоб протоколи більш високого рівня використовували протоколи більш низького рівня, точніше, дані протоколу вищерозташованого рівня передавалися за допомогою протоколів нижчерозташованих рівнів – цей процес називають **інкапсуляцією**, в свою чергу, процес добування даних вищерозташованого рівня з даних нижчерозташованого називають **деінкапсуляцією**).

Моделі бувають як практичні (що використовуються в мережах, вони іноді заплутані і неповні, але вирішують поставлені задачі), так і теоретичні (що показують принципи реалізації мережевих моделей, вони більш наглядні і повні, але заради наглядності жертвують продуктивністю та деякими можливостями практичних моделей).

Багаторівнева мережева модель описує взаємодію між різними протоколами усередині кожного рівня, а також взаємодію з верхніми й нижніми рівнями.

Використання багаторівневої мережевої моделі дає ряд переваг:

– спрощує розробку протоколів, тому що протоколи, що працюють на певному рівні, визначають формат оброблюваних даних і надають інтерфейс до верхніх і нижніх рівнів;

– змушує постачальників конкуруючих продуктів створювати уніфіковані рішення;

– виключає можливості зміни технологій або функцій одного рівня без врахування наслідків для верхніх і нижніх рівнів;

– надає загальну мову для опису функцій мережевої взаємодії.

Найбільш відомі мережеві моделі:

– Модель OSI (вона ж ЕМ ВВС – еталонна модель взаємозв'язку відкритих систем) – еталонна теоретична модель, описана в міжнародних стандартах і ДСТ.

– Модель TCP/IP (Модель DOD) – модель, що використовується на практиці, прийнята для роботи в Інтернеті.

– Модель SPX/IPX – модель стека SPX/IPX (сімейство протоколів для ЛОМ)

– Модель AppleTalk – модель для мереж AppleTalk (протоколи для роботи мереж з устаткуванням Apple)

– Модель Fibre Channel – модель для високошвидкісних мереж Fibre Channel.

Мережева модель TCP/IP

Перша багаторівнева еталонна модель мережевої взаємодії була створена на початку 70-х років і називається моделлю мережі Інтернет. У ній визначені чотири обов'язкових категорії функцій, необхідних для успішної взаємодії. Архітектура протоколів TCP/IP побудована на основі цієї моделі. Тому модель мережі Інтернет звичайно називають моделлю TCP/IP.

Протоколи працюють один з одним у стеку – це означає, що протокол, що розташовується на рівні вище, працює «поверх» нижнього, використовуючи механізми інкапсуляції.

Мережева модель TCP/IP представлена на рисунку 3.1.

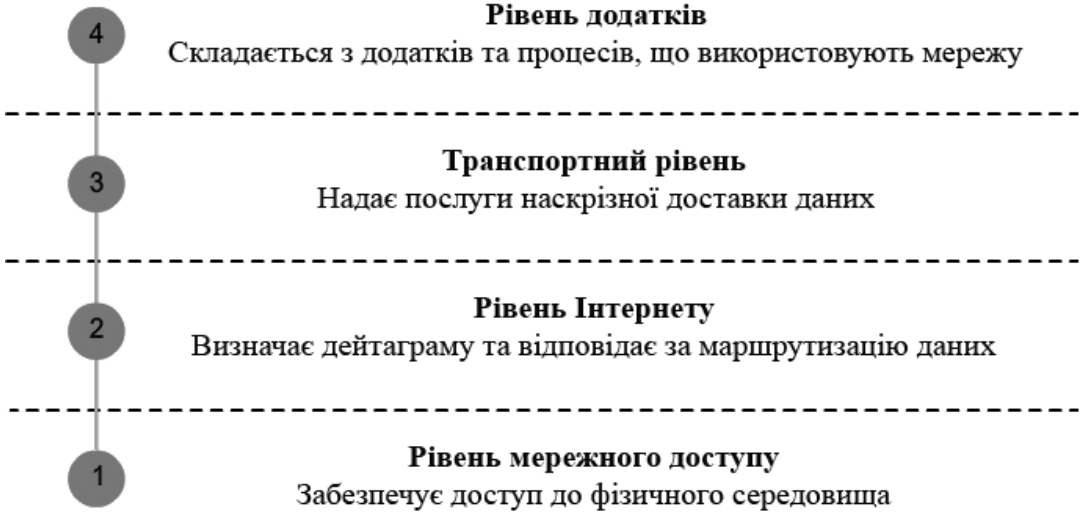


Рисунок 3.1 – Модель TCP/IP

Модель TCP/IP складається із чотирьох рівнів (знизу нагору):

- Рівень мережевого доступу (*Network Access*).
- Рівень Інтернету (*Internet*).
- Транспортний рівень (*Transport*).
- Рівень додатків (*Process/Application*).

Кожний із чотирьох рівнів моделі TCP/IP виконує свої функції.

Прикладний рівень (рівень додатків). Верхній рівень моделі, що включає протоколи, які обробляють дані користувачів і здійснюють керування обміном даними між додатками. На цьому рівні стандартизується представлення даних. Приклади протоколів: HTTP, SMTP, POP, IMAP, FTP, DNS, DHCP, Telnet.

Транспортний рівень. Містить протоколи для забезпечення цілісності даних при наскрізній передачі. Забезпечує керування ініціалізацією й закриттям з'єднань. Приклади протоколів: TCP та UDP.

Рівень Інтернету. Містить протоколи для маршрутизації повідомлень у мережі та служить для розміщення даних у дейтаграмі. Приклади протоколів: IP, NAT, ICMP, OSPF, RIP, BGP.

Рівень мережевого доступу. Нижній рівень моделі. Містить протоколи для фізичної доставки даних до мережевих пристроїв. Цей рівень розміщує дані в кадрі. Приклади протоколів: PPP, ARP, Ethernet, ATM.

Мережева модель OSI

Мережева модель OSI (англ. Open Systems Interconnection Basic Reference Model – базова еталонна модель взаємодії відкрітіх систем) – абстрактна мережева модель для комунікацій и розробки мережевих протоколів. Пропонує погляд на комп'ютерну мережу з точки зору вимірів. Кожний вимір обслуговує свою частину процесу взаємодії. Завдякі такій структурі спільна робота мережевого обладнання и програмного забезпечення стає набагато простішою й прозорішою.

Модель взаємодії відкритих систем була розроблена Міжнародною Організацією по Стандартизації (ISO) в 1984 році. На відміну від моделі TCP/IP, вона не описує взаємодій між окремими протоколами. Вона була створена як базова архітектура, яку розробники використовували для створення протоколів мережевої взаємодії. Хоча в далеко не всіх стеках протоколів у точності реалізовані всі сім рівнів моделі взаємодії відкритих систем, на сьогоднішній день вона вважається еталонною моделлю міжкомп’ютерних взаємодій.

У моделі OSI представлені всі функції або завдання, асоційовані з мережевими взаємодіями, а не тільки з певними протоколами TCP/IP. На відміну від моделі TCP/IP, у якій представлено тільки чотири рівні, модель OSI складається з семи більш специфічних рівнів (див. рисунок 3.2).

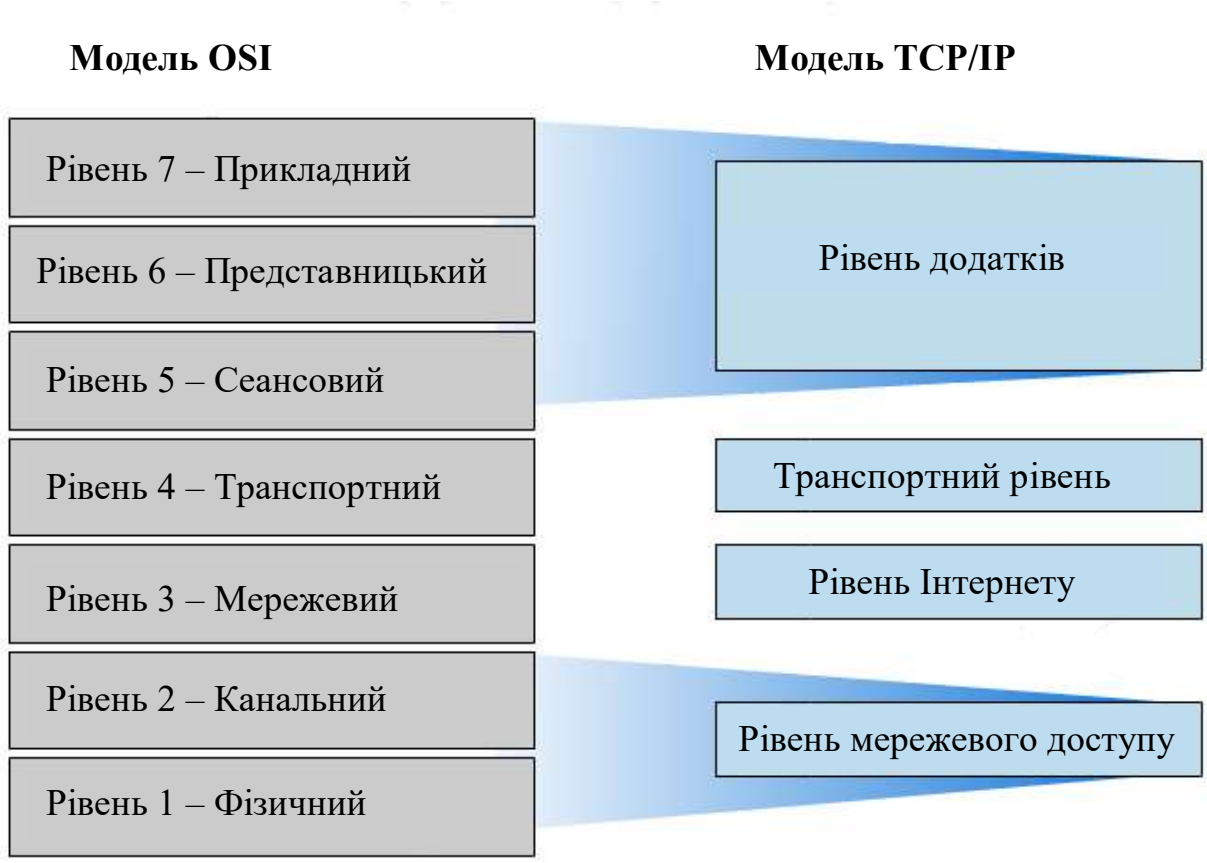


Рисунок 3.2 – Порівняння мережевих моделей OSI та TCP/IP

Кожному рівню присвоюється своя задача або група задач. Поділ функцій забезпечує незалежне функціонування кожного рівня в стеці. Наприклад, доступ до веб-сайту можливий як з портативного комп'ютера, підключеного до домашнього модему, так і з портативного комп'ютера за допомогою бездротового або мобільного телефону з підтримкою функцій бездротового доступу. Нижні рівні не впливають на ефективність роботи рівня додатка.

Точно так само нижні рівні не залежать від інших рівнів. Наприклад, на швидкість з'єднання з Інтернетом не впливає одночасний запуск декількох додатків, наприклад, електронна пошта, перегляд веб-сторінок, обмін миттєвими повідомленнями й завантаження музичних файлів.

3.2. Основні протоколи стеку TCP/IP

На рисунку 3.3 представлені рівні мережевої моделі OSI та їх призначення.

Група	Номер рівня	Назва рівня	Протоколи та технології	Розподілені мережеві компоненти даного рівня
Верхні рівні	7	Прикладний	DNS, NFS, DHCP, SNMP, FTP, TFTP, SMTP, POP3, IMAP, HTTP, Telnet	Додатки для контролю стану мережі, електронна пошта, веб-браузери, передача файлів тощо
	6	Представницький	SSL, оболонки і редиректори, MIME	
	5	Сеансовий	NetBIOS, інтерфейси програм, віддалені виклики процедури	
Нижні рівні	4	Транспортний	TCP та UDP	Механізни потокового відео та голосового зв’язку, списки фільтрів міжмережевих екранів
	3	Мережевий	IPv4, IPv6, IP NAT	IP-адресація, маршрутизація
	2	Канальний	Сімейство протоколів Ethernet, WLAN, Wi-Fi, ATM, PPP	Мережеві інтерфейсні плати та накопичувачі, мережева комутація, підключення до глобальної мережі
	1	Фізичний	Передача електричних сигналів, форми світлових хвиль, форми радіохвиль	Фізичне середовище передачі даних (мідна вита пара, оптоволоконний кабель, бездротові передавачі), концентратори і повторювачі

Рисунок 3.3 – Мережева модель OSI

Сім рівнів моделі OSI можна розділити на дві групи: верхні й нижні.

Верхніми рівнями часто називають усе, що перебуває вище транспортного рівня моделі OSI. Верхні рівні відносяться до роботи додатків і звичайно реалізуються тільки на програмному рівні. У рамках моделі OSI найвищий рівень – це прикладний рівень і він найближче розташований до кінцевого користувача.

Нижні рівні моделі OSI відносяться до передачі даних. Фізичний та канальний рівні реалізовані на апаратному й програмному рівнях. Фізичний рівень ближче всього до фізичного середовища передачі, до мережевих дротів. Він фактично поміщає інформацію в середовище.

Кінцеві станції, наприклад, клієнти й сервери, звичайно працюють на всіх семи рівнях. Мережеві пристрої працюють тільки на нижніх рівнях. Концентратори – це рівень 1, комутатори – рівні 1 і 2, маршрутизатори – рівні від 1 до 3, мережеві екрани – рівні 1, 2, 3 і 4.

Будь-який протокол моделі OSI повинен взаємодіяти або із протоколами свого рівня, або із протоколами на одиницю вище й/або нижче свого рівня. Взаємодії із протоколами свого рівня називаються горизонтальними, а з рівнями на одиницю вище або нижче – вертикальними. Будь-який протокол моделі OSI може виконувати тільки функції свого рівня й не може виконувати функцій іншого рівня, що не виконується в протоколах альтернативних моделей.

На кожному з рівнів одиниці інформації називаються по-різному. На фізичному рівні найменша одиниця інформації – біт. На канальному рівні інформація об'єднана у фрейми (або пакети). На мережевому рівні говорять про дейтаграми. На транспортному рівні одиницею вимірювання є сегмент. Прикладні рівні обмінюються повідомленнями. Пряма паралель із файловою системою на диску: локальні зміни намагніченості – біти об'єднані в сектори, що мають заголовки, сектори поєднуються в блоки, а ті, у свою чергу, у файли, що теж мають заголовки, що містять службову інформацію.

Таблиця 3.1 – Функції та одиниці вимірювання інформації різних рівнів моделі OSI

Рівень	**Функції**	**Тип даних**
Прикладний	Доступ до мережевих служб	Дані
Представницький	Подання й кодування даних	
Сеансовий	Керування сеансом зв'язку	
Транспортний	Прямий зв'язок між кінцевими пунктами й надійність	Сегменти
Мережевий	Визначення маршруту й логічна адресація	Пакети
Канальний	Фізична адресація	Кадри
Фізичний	Робота із середовищем передачі, сигналами й двійковими даними	Біти

Розглянемо кожний рівень моделі OSI більш докладно.

Фізичний рівень

Фізичний рівень має справу з передачею бітів по фізичних каналах зв'язку, таких, наприклад, як коаксіальний кабель, кручена пара, оптоволоконний кабель або цифровий територіальний канал. До цього рівня мають відношення характеристики фізичних середовищ передачі даних, такі як смуга пропускання, перешкодозахищеність, хвильовий опір і ін. На цьому ж рівні визначаються характеристики електричних сигналів, що передають дискретну інформацію, наприклад крутизна фронтів імпульсів, рівні напруги або струму переданого сигналу, тип кодування, швидкість передачі сигналів. Крім цього, тут стандартизуються типи роз’ємів і призначення кожного контакту.

Функції фізичного рівня реалізуються у всіх пристроях, підключених до мережі. З боку комп'ютера функції фізичного рівня виконуються мережевим адаптером або послідовним портом.

Прикладом протоколу фізичного рівня може служити специфікація 10Base-T технології Ethernet, що визначає як використовуваний кабель неекрановану кручену пару категорії 3 із хвильовим опором 100 Ом, роз’ємом RJ-45, максимальну довжину фізичного сегмента 100 м, манчестерский код для представлення даних у кабелі, а також деякі інші характеристики середовища й електричних сигналів.

Канальний рівень

На фізичному рівні просто пересилаються біти. При цьому не враховується, що в деяких мережах, у яких лінії зв'язку використовуються (розділяються) поперемінно декількома парами взаємодіючих комп'ютерів, фізичне середовище передачі може бути зайняте. Тому однією із задач канального рівня є перевірка доступності середовища передачі. Іншим завданням канального рівня є реалізація механізмів виявлення й корекції помилок. Для цього на канальному рівні біти групуються в набори, так звані *кадри (frames).* Канальний рівень забезпечує коректність передачі кожного кадру, поміщаючи спеціальну послідовність бітів у початок і кінець кожного кадру для його виділення, а також обчислює контрольну суму, обробляючи всі байти кадру певним способом і додаючи контрольну суму до кадру. Коли кадр приходить по мережі, одержувач знову обчислює контрольну суму отриманих даних і порівнює результат з контрольною сумою з кадру. Якщо вони збігаються, кадр вважається правильним і приймається. Якщо ж контрольні суми не збігаються, то фіксується помилка. Канальний рівень може не тільки виявляти помилки, але й виправляти їх за рахунок повторної передачі ушкоджених кадрів. Необхідно відзначити, що функція виправлення помилок не є обов'язковою для канального рівня, тому в деяких протоколах цього рівня вона відсутній, наприклад в Ethernet і Frame Relay.

У протоколах канального рівня, використовуваних у локальних мережах, закладена певна структура зв'язків між комп'ютерами й способи їхньої адресації.

Хоча канальний рівень і забезпечує доставку кадру між будь-якими двома вузлами локальної мережі, він це робить тільки в мережі із зовсім певною топологією зв'язків, саме тією топологією, для якої він був розроблений. До

таких типових топологій, підтримуваних протоколами канального рівня локальних мереж, відносяться загальна шина, кільце й зірка, а також структури, отримані з них за допомогою мостів і комутаторів. Прикладами протоколів канального рівня є протоколи Ethernet, Token Ring, FDDI.

У локальних мережах протоколи канального рівня використовуються комп'ютерами, мостами, комутаторами й маршрутизаторами. У комп'ютерах функції канального рівня реалізуються спільними зусиллями мережевих адаптерів і їхніх драйверів.

У глобальних мережах, які рідко мають регулярну топологію, канальний рівень часто забезпечує обмін повідомленнями тільки між двома сусідніми комп'ютерами, з'єднаними індивідуальною лінією зв'язку. Прикладами протоколів «точка-точка» (як часто називають такі протоколи) можуть служити широко розповсюджені протоколи PPP і LAP-B. У таких випадках для доставки повідомлень між кінцевими вузлами через всю мережу використовуються засоби мережевого рівня. Саме так організовані мережі X.25. Іноді в глобальних мережах функції канального рівня в чистому вигляді виділити важко, тому що в тому самому протоколі вони поєднуються з функціями мережевого рівня. Прикладами такого підходу можуть служити протоколи технологій ATM і Frame Relay.

У цілому канальний рівень являє собою досить потужний і закінчений набір функцій по пересиланню повідомлень між вузлами мережі. У деяких випадках протоколи канального рівня виявляються самодостатніми транспортними засобами й можуть допускати роботу поверх себе безпосередньо протоколів прикладного рівня або додатків, без залучення засобів мережевого й транспортного рівнів. Наприклад, існує реалізація протоколу керування мережею SNMP безпосередньо поверх Ethernet, хоча стандартно цей протокол працює поверх мережевого протоколу IP і транспортного протоколу UDP. Природно, що застосування такої реалізації буде обмеженим – вона не підходить для складених мереж різних технологій, наприклад Ethernet і X.25, і навіть для такої мережі, у якій у всіх сегментах застосовується Ethernet, але між сегментами існують петлевидні зв'язки. А от у двосегментній мережі Ethernet, об'єднаній мостом, реалізація SNMP над канальним рівнем буде цілком працездатною.

Проте для забезпечення якісного транспортування повідомлень у мережах будь-яких топологій і технологій функцій канального рівня виявляється недостатньо, тому в моделі OSI рішення цього завдання покладає на два наступні рівні – мережевий і транспортний.

Канальний рівень забезпечує передачу пакетів даних, що надходять від протоколів верхніх рівнів, вузлу призначення, адреса якого також указує протокол верхнього рівня. Протоколи канального рівня оформляють передані їм пакети в кадри власного формату, поміщаючи зазначену адресу призначення в одне з полів такого кадру, а також супроводжуючи кадр контрольною сумою. Протокол канального рівня має локальний сенс, він призначений для доставки кадрів даних, як правило, у межах мереж із простою топологією зв'язків і однотипною або близькою технологією, наприклад в односегментних мережах Ethernet або ж у багатосегментних мережах Ethernet і Token Ring ієрархічної

топології, розділених тільки мостами й комутаторами. У всіх цих конфігураціях адреса призначення має локальний сенс для даної мережі й не змінюється при проходженні кадру від вузла-джерела до вузла призначення. Можливість передавати дані між локальними мережами різних технологій пов'язана з тим, що в цих технологіях використовуються адреси однакового формату, до того ж виробники мережевих адаптерів забезпечують унікальність адрес незалежно від технології.

Іншою областю дії протоколів канального рівня є зв'язки типу «точка-точка» глобальних мереж, коли протокол канального рівня відповідальний за доставку кадру безпосередньому сусідові. Адреса в цьому випадку не має принципового значення, а на перший план виходить здатність протоколу відновлювати викривлені й загублені кадри, тому що погана якість територіальних каналів, особливо телефонних, часто вимагає виконання подібних дій.

Якщо ж перераховані вище умови не дотримуються, наприклад зв'язки між сегментами Ethernet мають петлевидну структуру, або поєднувані мережі використовують різні способи адресації, як це має місце в мережах Ethernet і X.25, то протокол канального рівня не може самостійно впоратися із задачею передачі кадру між вузлами й вимагає допомоги протоколу мережевого рівня.

Мережевий рівень

Мережевий рівень служить для утворення єдиної транспортної системи, що поєднує декілька мереж, причому ці мережі можуть використовувати зовсім різні принципи передачі повідомлень між кінцевими вузлами й мати довільну структуру зв'язків. Функції мережевого рівня досить різноманітні. Почнемо їхній розгляд на прикладі об'єднання локальних мереж.

Протоколи канального рівня локальних мереж забезпечують доставку даних між будь-якими вузлами тільки в мережі з відповідною типовою топологією, наприклад топологією ієрархічної зірки. Це дуже жорстке обмеження, що не дозволяє будувати мережі з розвинутою структурою, наприклад мережі, що поєднують кілька мереж підприємства в єдину мережу, або високонадійні мережі, у яких існують надлишкові зв'язки між вузлами. Можна було б ускладнювати протоколи канального рівня для підтримки петлевидних надлишкових зв'язків, але принцип розподілу обов'язків між рівнями приводить до іншого рішення. Щоб, з одного боку, зберегти простоту процедур передачі даних для типових топологий, а з іншого боку – допустити використання довільних топологий, вводиться додатковий мережевий рівень.

На мережевому рівні сам термін *мережа* наділяють специфічним значенням. У цьому випадку під мережею розуміється сукупність комп'ютерів, з'єднаних між собою відповідно до однієї зі стандартних типових топологій і використовуючих для передачі даних один із протоколів канального рівня, певний для цієї топології.

Усередині мережі доставка даних забезпечується відповідним канальним рівнем, а от доставкою даних між мережами займається мережевий рівень, що і підтримує можливість правильного вибору маршруту передачі повідомлення

навіть у тому випадку, коли характер структури зв'язків між складовими мережами відрізняється від прийнятого в протоколах канального рівня.

Мережі з'єднуються між собою спеціальними пристроями, що називаються маршрутизаторами. ***Маршрутизатор*** – це пристрій, що збирає інформацію про топологію мережевих з'єднань і на її підставі пересилає пакети мережевого рівня в мережу призначення. Щоб передати повідомлення від відправника, що перебуває в одній мережі, одержувачеві, що перебуває в іншій мережі, потрібно зробити деяку кількість *транзитних передач між мережами,* або *хопів (hop* – стрибок), щоразу вибираючи підходящий маршрут. Таким чином, маршрут являє собою послідовність маршрутизаторів, через які проходить пакет.

На рисунку 3.4 показані чотири мережі, зв'язані трьома маршрутизаторами. Між вузлами A та B даної мережі пролягають два маршрути: перший через маршрутизатори 1 та 3, а другий через маршрутизатори 1, 2 і 3.

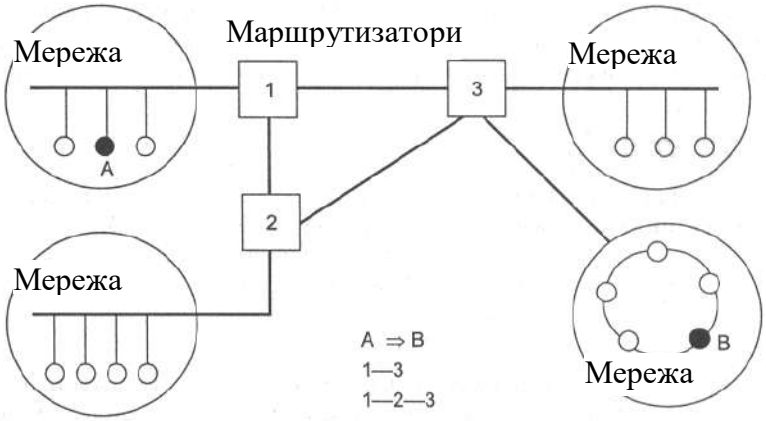


Рисунок 3.4 – Приклад складеної мережі

Проблема вибору найкращого шляху називається ***маршрутизацією,*** і її рішення є однією з головних завдань мережевого рівня. Ця проблема ускладнюється тим, що самий короткий шлях не завжди найкращий. Часто критерієм при вибору маршруту є час передачі даних по цьому маршруту; він залежить від пропускної здатності каналів зв'язку та інтенсивності трафіку, що може змінюватися із часом. Деякі алгоритми маршрутизації намагаються пристосовуватися до змін навантаження, у той час як інші приймають рішення на основі середніх показників за тривалий час. Вибір маршруту може здійснюватися й за іншими критеріями, наприклад надійності передачі.

У загальному випадку функції мережевого рівня ширше, ніж функції передачі повідомлень по зв'язках з нестандартною структурою, які ми зараз розглянули на прикладі об'єднання декількох локальних мереж. Мережевий рівень вирішує також задачу узгодження різних технологій, спрощення адресації у великих мережах і створення надійних і гнучких бар'єрів на шляху небажаного трафіку між мережами.

Повідомлення мережевого рівня прийнято називати ***пакетами*** (packet). При організації доставки пакетів на мережевому рівні використовується поняття

«номер мережі». У цьому випадку адреса одержувача складається зі старшої частини – номера мережі й молодшої – номера вузла в цій мережі. Всі вузли однієї мережі повинні мати ту саму старшу частину адреси, тому терміну «мережа» на мережевому рівні можна дати й інше, більш формальне визначення: мережа – це сукупність вузлів, мережева адреса яких містить той самий номер мережі.

На мережевому рівні визначаються два види протоколів. Перший вид – *мережеві протоколи (routed protocols)* – реалізують просування пакетів через мережу. Саме ці протоколи звичайно мають на увазі, коли говорять про протоколи мережевого рівня. Однак часто до мережевого рівня відносять і інший вид протоколів, що називаються протоколами обміну маршрутною інформацією або просто *протоколами маршрутизації (routing protocols).* За допомогою цих протоколів маршрутизатори збирають інформацію про топологію міжмережевих з'єднань. Протоколи мережевого рівня реалізуються програмними модулями операційної системи, а також програмними й апаратними засобами маршрутизаторів.

На мережевому рівні працюють протоколи ще одного типу, які відповідають за відображення адреси вузла, використовуваного на мережевому рівні, у локальну адресу мережі. Такі протоколи часто називають *протоколами дозволу адрес (Address Resolution Protocol, ARP).* Іноді їх відносять не до мережевого рівня, а до канального, хоча тонкості класифікації не змінюють їхньої суті.

Транспортний рівень

На шляху від відправника до одержувача пакети можуть бути викривлені або загублені. Хоча деякі додатки мають власні засоби обробки помилок, існують і такі, які воліють відразу мати справу з надійним з'єднанням. Транспортний рівень забезпечує додаткам або верхнім рівням стека – прикладному й сеансовому – передачу даних з тим ступенем надійності, який їм потрібний. Модель OSI визначає п'ять класів сервісу, надаваних транспортним рівнем. Ці види сервісу відрізняються якістю надаваних послуг: терміновістю, можливістю відновлення перерваного зв'язку, наявністю засобів мультиплексування декількох з'єднань між різними прикладними протоколами через загальний транспортний протокол, а головне – здатністю до виявлення й виправлення помилок передачі, таких як викриволення, втрата й дублювання пакетів.

Вибір класу сервісу транспортного рівня визначається, з одного боку, тим, у якому ступені завдання забезпечення надійності вирішується самими додатками й протоколами більш високих, ніж транспортний, рівнів, а з іншого боку, цей вибір залежить від того, наскільки надійною є система транспортування даних у мережі, забезпечувана рівнями, розташованими нижче транспортного – мережевим, канальним і фізичним. Так, наприклад, якщо якість каналів передачі зв'язку дуже висока і ймовірність виникнення помилок, не виявлених протоколами більш низьких рівнів, невелика, то розумно скористатися одним з полегшених сервісів транспортного рівня, не обтяжених численними перевірками, квитуванням та іншими прийомами підвищення

надійності. Якщо ж транспортні засоби нижніх рівнів дуже ненадійні, то доцільно звернутися до найбільш розвиненого сервісу транспортного рівня, що працює, використовуючи максимум засобів для виявлення й усунення помилок, включаючи попереднє встановлення логічного з'єднання, контроль доставки повідомлень по контрольних сумах і циклічну нумерацію пакетів, встановлення тайм-аутів доставки й т.п.

Як правило, всі протоколи, починаючи із транспортного рівня й вище, реалізуються програмними засобами кінцевих вузлів мережі – компонентами їх мережевих операційних систем. Як приклад транспортних протоколів можна привести протоколи TCP і UDP стека TCP/IP і протокол SPX стека Novell.

Протоколи нижніх чотирьох рівнів узагальнено називають мережевим транспортом або транспортною підсистемою, тому що вони повністю вирішують завдання транспортування повідомлень із заданим рівнем якості в складених мережах з довільною топологією й різними технологіями. Три верхні рівні, що залишилися вирішують завдання надання прикладних сервісів на підставі наявної транспортної підсистеми.

Сеансовий рівень

Сеансовий рівень забезпечує керування взаємодією: фіксує, яка зі сторін є активною в даний момент, надає засоби синхронізації. Останні дозволяють вставляти контрольні точки в довгі передачі, щоб у випадку відмови можна було повернутися назад до останньої контрольної точки, а не починати все з початку. На практиці деякі додатки використовують сеансовий рівень, і він рідко реалізується у вигляді окремих протоколів, хоча функції цього рівня часто поєднують із функціями прикладного рівня й реалізують в одному протоколі.

Представницький рівень

Представницький рівень має справу з формою подання переданої по мережі інформації, не міняючи при цьому її змісту. За рахунок рівня подання інформація, передана прикладним рівнем однієї системи, завжди зрозуміла прикладному рівню іншої системи. За допомогою засобів даного рівня протоколи прикладних рівнів можуть перебороти синтаксичні розходження в поданні даних або ж розходження в кодах символів, наприклад кодів ASCII і EBCDIC. На цьому рівні може виконуватися шифрування й дешифрування даних, завдяки яким таємність обміну даними забезпечується відразу для всіх прикладних служб. Прикладом такого протоколу є протокол Secure Socket Layer (SSL), що забезпечує секретний обмін повідомленнями для протоколів прикладного рівня стека TCP/IP.

Прикладний рівень

Прикладний рівень – це в дійсності просто набір різноманітних протоколів, за допомогою яких користувачі мережі одержують доступ до поділюваних ресурсів, таких як файли, принтери або гіпертекстові веб-сторінки, а також організують свою спільну роботу, наприклад, по протоколу електронної пошти. Одиниця даних, якою оперує прикладний рівень, звичайно називається *повідомленням.*

Існує дуже велика розмаїтість служб прикладного рівня. Наведемо як приклад хоча б декілька найпоширеніших реалізацій файлових служб: NCP в

операційній системі Novell NetWare, SMB в Microsoft Windows NT, NFS, FTP і TFTP, що входять у стек TCP/IP.

Мережозалежні та мережонезалежні рівні **моделі OSI**

Функції всіх рівнів моделі OSI можуть бути віднесені до однієї із двох груп: або до функцій, що залежать від конкретної технічної реалізації мережі, або до функцій, орієнтованих на роботу з додатками.

Три нижніх рівні – фізичний, канальний і мережевий – є мережозалежними, тобто протоколи цих рівнів тісно пов'язані з технічною реалізацією мережі й використовуваним комунікаційним устаткуванням. Наприклад, перехід на устаткування FDDI означає повну зміну протоколів фізичного й канального рівнів у всіх вузлах мережі.

Три верхніх рівні – прикладний, представницький і сеансовий – орієнтовані на додатки й мало залежать від технічних особливостей побудови мережі. На протоколи цих рівнів не впливають які б то не було зміни в топології мережі, заміна устаткування або перехід на іншу мережеву технологію. Так, перехід від Ethernet на високошвидкісну технологію lOOVG-AnyLAN не вимагає ніяких змін у програмних засобах, що реалізують функції прикладного, представницького й сеансового рівнів.

Транспортний рівень є проміжним, він приховує деталі функціонування нижніх рівнів від верхніх. Це дозволяє розробляти додатки, що не залежать від технічних засобів безпосереднього транспортування повідомлень.

3.3. Віртуалізація (принципи, гіпервізори)

Віртуалізація – надання набору обчислювальних ресурсів або їхнього логічного об'єднання, абстраговане від апаратної реалізації і забезпечує при цьому логічну ізоляцію один від одного обчислювальних процесів, що виконуються на одному фізичному ресурсі.

Прикладом використання віртуалізації є можливість запуску кількох операційних систем на одному комп'ютері: при тому кожен з екземплярів таких гостьових операційних систем працює зі своїм набором логічних ресурсів (процесорних, оперативної пам'яті, пристроїв зберігання), надання яких із загального пулу, доступного на рівні обладнання, управляє хостова операційна система – гіпервізор. Також можуть бути піддані віртуалізації мережі передачі даних, мережі зберігання даних, платформне та прикладне програмне забезпечення (емуляція).

Види віртуалізації

Устаткування

– Емуляція – повна віртуалізація (віртуалізація всієї платформи); наприклад, QEMU або емулятори ігрових консолей.

Операційні системи

– Програмна віртуалізація:

- Динамічна трансляція; при динамічній (бінарній) трансляції проблемні команди гостьової операційної системи перехоплюються гіпервізором.
- Паравіртуалізація: операційна система взаємодіє з програмою гіпервізора, який надає їй гостьовий API замість використання безпосередньо таких ресурсів, як таблиця сторінок пам'яті.
- Вбудована віртуалізація.

– Апаратна віртуалізація – віртуалізація за допомогою спеціальної процесорної архітектури. На відміну від програмної віртуалізації, за допомогою цієї техніки можливе використання ізольованих гостьових систем, керованих гіпервізором безпосередньо.

– Віртуалізація на рівні операційної системи: робота кількох екземплярів простору користувача в рамках однієї ОС. Прикладами можуть бути Docker, LXC

Програмне забезпечення

– Віртуалізація додатків (також віртуалізація робочого оточення): робота окремих додатків у середовищі, відокремленому від основної ОС. Ця концепція тісно пов'язана з портативними програмами. Прикладами можуть бути: Citrix XenApp, Microsoft App-V.

– Віртуалізація сервісів: емуляція поведінки системних компонентів, необхідні запуску програми з метою налагодження та тестування (англ. *Application Under Test*). Замість віртуалізації компонентів повністю, ця технологія віртуалізує лише необхідні частини. Приклади: SoapUI, Parasoft Virtualize.

Пам'ять

– Віртуалізація пам'яті (англ. *memory virtualization*) – Об'єднанням оперативної пам'яті з різних ресурсів в єдиний масив. Реалізації: Oracle Coherence, GigaSpaces XAP.

– Віртуальна пам'ять – ізоляція адресного простору програми від адресного простору. Застосовується у всіх сучасних ОС.

Системи зберігання

– Віртуалізація зберігання даних, представлення набору фізичних носіїв як єдиного фізичного носія:

- Блокова віртуалізація.
- Файлова віртуалізація.

– Розподілена файлова система – будь-яка файлова система, яка дозволяє отримувати доступ до файлів з кількох пристроїв за допомогою комп'ютерної мережі.

– Віртуальна файлова система – рівень абстракції поверх конкретної реалізації файлової системи. Метою VFS є забезпечення однакового доступу клієнтських програм до різних типів файлових систем.

– Гіпервізор зберігання (англ. *storage hypervisor*) – програма, яка управляє віртуалізацією простору для зберігання даних і може об'єднувати різні фізичні простори в єдиний логічний масив [1].

– Віртуалізація пристроїв зберігання даних: віртуалізація жорсткого (логічний диск) або оптичного диска (наприклад, DAEMON Tools).

Бази даних

– Віртуалізація даних (англ. *data virtualization*) – подання даних в абстрактному вигляді, незалежно від систем управління та зберігання даних, що знаходяться нижче, а також їх структури. Це підхід до уніфікації даних з декількох джерел на одному рівні, щоб додатки, засоби звітності та кінцеві користувачі могли отримувати доступ до даних, не потребуючи докладних відомостей про вихідні джерела, місцезнаходження та структури даних. [2]

Мережа

– Віртуалізація мережі – процес об'єднання апаратних та програмних мережевих ресурсів у єдину віртуальну мережу:

- Зовнішня мережа, що з'єднує безліч в одну віртуальну.
- Внутрішня, що створює віртуальну мережу між програмними контейнерами всередині однієї системи.

– Віртуальна приватна мережа – забезпечення одного або кількох мережних з'єднань над іншою мережею.

Віртуалізація операційних систем

Для віртуалізації операційних систем застосовується серія підходів, які за типом реалізації поділяються на програмні та апаратні.

Програмна віртуалізація

Динамічна трансляція

При динамічній (*бінарній*) трансляції проблемні команди гостьової операційної системи перехоплюються гіпервізором. Після того, як ці команди замінюються на безпечні, відбувається повернення управління гостьовою системою.

Паравіртуалізація

Паравіртуалізація – техніка віртуалізації, коли гостьові операційні системи готуються до виконання у віртуалізованому середовищі, навіщо їх ядро трохи модифікується. Операційна система взаємодіє з програмою гіпервізора, який надає їй гостьовий API замість використання безпосередньо таких ресурсів, як таблиця сторінок пам'яті.

Метод паравіртуалізації дозволяє досягти більш високої продуктивності, ніж метод динамічної трансляції.

Метод паравіртуалізації застосовний лише в тому випадку, якщо гостьові операційні системи мають відкриті вихідні коди, які можна модифікувати відповідно до ліцензії, або гіпервізор і гостьова операційна система розроблені одним виробником з урахуванням можливості паравіртуалізації гостьової системи (хоча за умови, що під гіпервізором може бути запущений гіпервізор нижчого рівня, то й паравіртуалізації самого гіпервізора).

Вперше термін виник у проекті Denali.

Вбудована віртуалізація

Переваги:

– Спільне використання ресурсів декількома гостьовими операційними системами (каталоги, принтери тощо).

– Зручність інтерфейсу для вікон додатків з різних систем (вікна додатків, що перекриваються, однакова мінімізація вікон, як у хост-системі).

– При тонкому налаштуванні на апаратну платформу продуктивність мало відрізняється від оригінальної операційної системи. Швидке перемикання між системами (менше однієї секунди).

– Проста процедура поновлення гостьової операційної системи.

–Двостороння віртуалізація (додатки однієї системи запускаються до іншої та навпаки).

Реалізації: BlueStacks Multi-OS (MOS).

Апаратна віртуалізація

Переваги:

– Спрощення розробки програмних платформ віртуалізації за рахунок надання апаратних інтерфейсів керування та підтримки віртуальних гостьових систем. Це зменшує трудомісткість та час на розробку систем віртуалізації.

– Можливість збільшення швидкодії платформ віртуалізації. Управління віртуальними гостьовими системами здійснює безпосередньо невеликий проміжний шар програмного забезпечення, гіпервізор, що дає збільшення швидкодії.

– Покращується захищеність, з'являється можливість перемикання між кількома незалежними запущеними платформами віртуалізації на апаратному рівні. Кожна з віртуальних машин може працювати незалежно, у своєму просторі апаратних ресурсів повністю ізольовано один від одного. Це дозволяє усунути втрати швидкодії на підтримку хостової платформи та збільшити захищеність.

– Гостьова система стає не прив'язана до архітектури хостової платформи та реалізації платформи віртуалізації. Технологія апаратної віртуалізації уможливлює запуск 64-бітових гостьових систем на 32-бітових хостових системах (з 32-бітними середовищами віртуалізації на хостах).

Технології:

– Режим віртуального 8086 (застаріла).

– Intel VT (*VT-x, Intel Virtualization Technology for x86*).

– AMD-V.

Платформи, що використовують апаратну віртуалізацію:

– IBM LPAR.

– VMware.

– Hyper-V.

– Xen.

– KVM.

– Bhyve.

Контейнерна віртуалізація

Контейнерна віртуалізація – віртуалізація на рівні операційної системи – дозволяє запускати ізольовані віртуальні системи на одному фізичному вузлі, але не дозволяє запускати операційні системи з ядрами, відмінними від типу ядра базової операційної системи. При такому підході не існує окремого шару гіпервізора, натомість сама хостова операційна система відповідає за поділ апаратних ресурсів між кількома гостьовими системами (контейнерами) та забезпечує їхню незалежність. Деякі реалізації – FreeBSD Jail (2000), Virtuozzo Containers (2000), Solaris Containers (2005), Linux-VServer, OpenVZ (2005), LXC (2008),iCore Virtual Accounts (2008), Docker (2013).

Області застосування віртуалізації

Віртуальні машини

Віртуальна машина – це оточення, яке представляється для "гостьової" операційної системи, як апаратне. Однак насправді це програмне оточення, яке емулює програмне забезпечення хостової системи. Ця емуляція має бути достатньо надійною, щоб драйвери гостьової системи могли працювати стабільно. При використанні паравіртуалізації, віртуальна машина не емулює апаратне забезпечення, а замість цього пропонує використовувати спеціальний API.

Приклади застосування:

– Тестові лабораторії та навчання: тестуванню у віртуальних машинах зручно піддавати програми, що впливають на налаштування операційних систем, наприклад інсталяційні програми. За рахунок простоти в розгортанні віртуальних машин вони часто використовуються для навчання новим продуктам і технологіям.

– Поширення попередньо встановленого програмного забезпечення: багато розробників програмних продуктів створюють готові образи віртуальних машин із попередньо встановленими продуктами і надають їх на безкоштовній або комерційній основі. Такі послуги надають Vmware VMTN або Parallels PTN.

Віртуалізація ресурсів

Віртуалізація ресурсів (або поділ ресурсів, англ. *partitioning*) може бути представлена як поділ одного фізичного вузла на кілька частин, кожна з яких видно для власника як окремий сервер. Не є технологією віртуальних машин, що здійснюється на рівні ядра операційної системи.

У системах з гіпервізором другого типу обидві операційні системи (гостьова та гіпервізора) забирають фізичні ресурси та вимагають окремого ліцензування. Віртуальні сервери, що працюють на рівні ядра ОС, майже не втрачають швидкодії, що дає можливість запускати на одному фізичному сервері сотні віртуальних, що не вимагають додаткових ліцензій.

Дисковий простір або пропускний канал мережі розділені на кілька менших складових, і тому легше використовуваних ресурсів того ж типу.

Наприклад, до реалізації поділу ресурсів можна віднести OpenSolaris Network Virtualization and Resource Control (Проект Crossbow), що дозволяє створювати кілька віртуальних мережевих інтерфейсів на основі одного фізичного.

Агрегація, розподіл чи додавання безлічі ресурсів у великі ресурси чи об'єднання ресурсів. Наприклад, симетричні мультипроцесорні системи поєднують безліч процесорів; RAID та дискові менеджери поєднують безліч дисків в один великий логічний диск; RAID та мережеве обладнання використовує безліч каналів, об'єднаних так, щоб вони представлялися як єдиний широкосмуговий канал. На мета-рівні комп'ютерні кластери роблять усе перераховане вище. Іноді сюди ж відносять мережеві файлові системи абстраговані від сховищ даних, на яких вони побудовані, наприклад, Vmware VMFS, Solaris / OpenSolaris ZFS, NetApp WAFL.

Віртуалізація додатків

Віртуалізація програм – процес використання програми, перетвореної з потребуючої установки в операційну систему на не вимагає (потрібно тільки запустити). Для віртуалізації програм програмне забезпечення віртуалізатора визначає при установці віртуалізованого додатка, які потрібні компоненти ОС, і емулює їх. Таким чином, створюється необхідне спеціалізоване середовище для цього віртуалізованого додатка і, тим самим, забезпечується ізольованість роботи цього додатка. Для створення віртуальної програми віртуалізоване поміщається в контейнер, оформлений, як правило, у вигляді папки. При запуску віртуального додатка запускається віртуалізоване додаток і контейнер, що є для нього робочим середовищем. Робоче середовище запускається і надає локальні раніше створені ресурси, що включає ключі реєстру, файли та інші компоненти, необхідні для запуску і роботи програми. Таке віртуальне середовище працює як прошарок між програмою та операційною системою, що дозволяє уникнути конфліктів між програмами. Віртуалізацію додатків забезпечують, наприклад, програми Citrix XenApp, SoftGrid та VMware ThinApp.

Переваги:

– ізольованість виконання додатків: відсутність несумісностей та конфліктів;

– щоразу в первозданному вигляді: не захаращується реєстр, немає конфігураційних файлів – необхідно для сервера;

– менші ресурсозатрати проти емуляцією всієї операційної системи.

Віртуалізація серверів

Віртуалізація серверів – це процес поділу фізичного сервера на кілька унікальних та ізольованих віртуальних машин (серверів) за допомогою програмного забезпечення (гіпервізора). На кожному віртуальному сервері можуть виконуватися власні операційні системи незалежно.

Віртуалізація серверів дозволяє:

– Оптимізувати витрати на придбання серверного обладнання. Під кожну задачу виділяється віртуальний сервер із необхідною кількістю ресурсів (ЦПУ, ОЗП та ін.), простої обладнання мінімізуються.

– Спростити супровід інфраструктури. Створення, видалення або обслуговування віртуальної машини зазвичай простіше і швидше, ніж аналогічні операції з фізичним сервером.

– Підвищити стійкість до відмови інфраструктури. Віртуальні машини ізольовані одна від одної, програмний збій однією них не призведе до втрати працездатності сервісів і додатків інших.

Гіпервізор забезпечує ізольоване середовище виконання для кожної віртуальної машини, а також керує доступом ВМ та гостьових ОС до апаратних ресурсів фізичного сервера. Говорячи простими словами, гіпервізор забезпечує паралельне та незалежне функціонування кількох операційних систем на одному комп'ютері.

У класичному підході гіпервізори групуються за двома типами:

– гіпервізори першого типу запускаються безпосередньо на апаратному забезпеченні комп'ютера (залізі),

– гіпервізори другого типу, яким для роботи необхідна наявність хостової операційної системи.

– в останні кілька років класична класифікація зазнає змін – додався гібридний тип гіпервізорів (тип 1.5), який поєднує характеристики першого та другого типів.

Гіпервізори першого типу (native, bare-metal)

Гіпервізор першого типу виконується як контрольна програма безпосередньо на апаратній частині комп'ютера і вимагає ОС загального призначення. У цій архітектурі гіпервізор керує розподілом обчислювальних ресурсів і сам контролює всі звернення віртуальних машин до пристроїв.

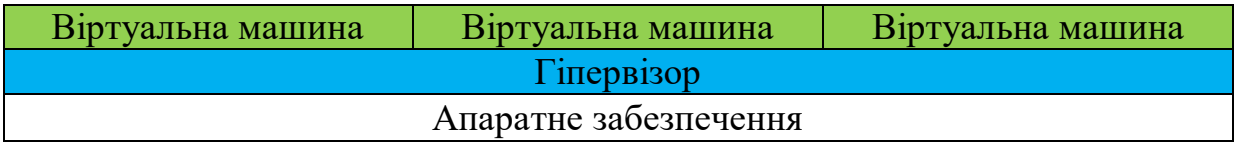


Рисунок 3.5 – Гіпервізор першого типу

Гіпервізори першого типу показують високу швидкодію, проте мають очевидний недолік – необхідність підтримувати драйвери пристроїв призводить до звуження списку сумісного апаратного забезпечення.

Приклади:

– VMWare ESXi;

– KVM (Proxmox VE) – може бути також віднесено до другого типу;

– Xen (Xenserver, Citrix Hypervisor), Hyper-V можуть бути також віднесені до гібридного типу.

Гіпервізори другого типу (hosted)

Гіпервізор другого типу виконується поверх хостової операційної системи (зазвичай Linux). Він управляє гостьовими операційними системами, тоді як емуляцією та управлінням фізичними ресурсами займається хостова ОС.

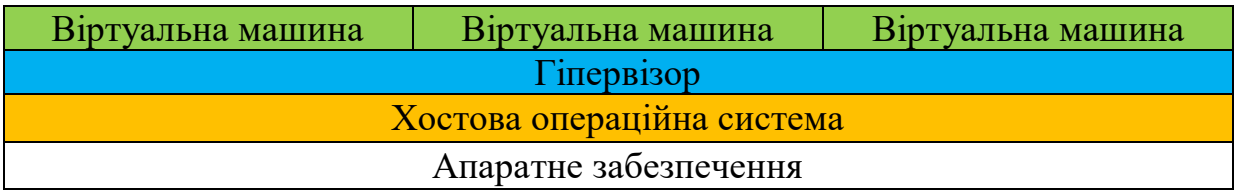


Рисунок 3.6 – Гіпервізор другого типу

Гіпервізори другого типу показують менше щодо гіпервізорів першого типу швидкодію і рідше використовуються в промисловій експлуатації, проте відмінно підходять для завдань навчання та розробки програмного забезпечення.

Приклади:

– Oracle VM VirtualBox, VMWare Workstation;
– KVM (Proxmox VE) – може бути віднесений до першого типу.

Гіпервізори гібридного типу (hybrid)

Гібридний гіпервізор поєднує характеристики гіпервізорів першого і другого типів – він виконується поверх спеціалізованої сервісної (або базової) операційної системи. Сервісна ОС називається батьківським розділом або доменом (parent partition у термінології Hyper-V або domain dom0 у термінології Xen). Після встановлення гіпервізора ядро ОС переходить у режим підтримки віртуалізації та передає керування ресурсами процесора та пам'яті гіпервізору. При цьому батьківський розділ бере на себе функцію обробки звернень до драйверів пристроїв та операцій вводу-виводу.

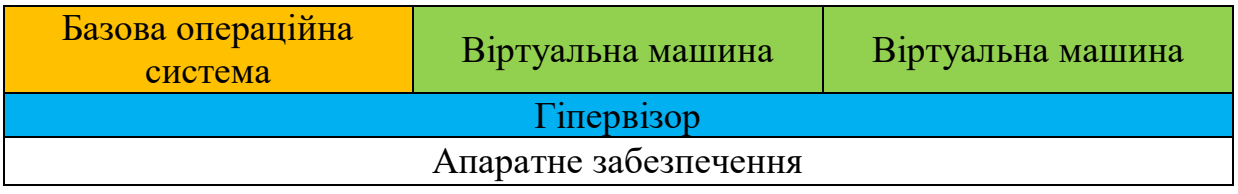


Рисунок 3.7 – Гібридний гіпервізор

Цей підхід є зручним з точки зору сумісності з обладнанням: не потрібно додавати в гіпервізор драйвери пристроїв (розширюється список сумісного апаратного забезпечення). Також гіпервізор звільняється від завдання обробки дзвінків до драйверів пристроїв – ці дзвінки обробляє сервісна ОС.

Приклади: Xen (XenServer, Citrix Hypervisor), Hyper-V – можуть бути віднесені до першого типу

3.4. Архітектура комп’ютерів

Архітектура комп'ютера – концептуальна модель комп'ютерної системи, втілена в її компонентах, їх взаємодії між собою і оточенням, що включає також принципи її проектування та розвитку. Аспекти реалізації (наприклад, технологія, що застосовується при реалізації пам'яті) не є частиною архітектури.

Рівні організації

Вирізняють кілька рівнів організації комп'ютера (комп'ютерної архітектури), від двох і більше:

– **Рівень 0.** Цифровий логічний рівень, це апаратне забезпечення машини, що складається з вентилів. також Логічні елементи (засувки), тригери, регістри.

– **Рівень 1.** Мікроархітектурний рівень, інтерпретація (мікропрограми) чи безпосереднє виконання. Електронні схеми виконують машинно-залежні програми. Сукупність регістрів процесора формує локальну пам'ять. також арифметико-логічний пристрій, пристрій керування. Його завдання – інтерпретація команд рівня 2 (рівня архітектури команд). В даний час на рівні архітектури команд зазвичай знаходяться прості команди, які виконуються за один цикл (такі, зокрема, RISC машини).

– **Рівень 2.** Рівень архітектури системи команд, трансляція (асемблер).

– **Рівень 3.** Рівень операційної системи, трансляція (асемблер). Це гібридний рівень: одна частина команд інтерпретується операційною системою, а інша мікропрограмою. також віртуальна пам'ять, файли.

– **Рівень 4.** Рівень мови асемблера, трансляція (компілятор). Четвертий рівень і вище використовується для написання прикладних програм, з першого до третього – системних програм. Програми у зручному для людини вигляді транслюються на мову рівнів 1-3.

– **Рівень 5.** Мова високого рівня. Програми мовами високого рівня транслюються зазвичай на рівні 3 та 4.

<table>
<tr><td colspan="2"></td><td>Прикладні програми</td><td rowspan="5">Програмне забезпечення</td></tr>
<tr><td rowspan="4">Системне програмне забезпечення</td><td></td><td>Додаткове системне програмне забезпечення</td></tr>
<tr><td rowspan="2">Операційна система</td><td>Користувальницьке оточення</td></tr>
<tr><td>Ядро операційної системи (супервізор)</td></tr>
<tr><td></td><td>Вбудоване програмне забезпечення (firmware)</td></tr>
<tr><td colspan="2"></td><td>Архітектура системи команд</td><td rowspan="3">Апаратна платформа (архітектура комп’ютера)</td></tr>
<tr><td colspan="2"></td><td>Мікропрограма (мікрокод)</td></tr>
<tr><td colspan="2"></td><td>Мікроархітектура</td></tr>
<tr><td colspan="2"></td><td>Цифровий логічний рівень</td><td rowspan="2"></td></tr>
<tr><td colspan="2"></td><td>Фізичні пристрої</td></tr>
</table>

Рисунок 3.8 – Схема, що ілюструє багаторівневу структуру комп'ютера

Класифікація

За типом застосовуваного процесора

– CISC (англ. *complex instruction set computing)* – архітектура з повним набором команд. Такі процесори виконують усі команди, прості та складні, за велику кількість тактів. Команд у таких процесорах багато, і компілятори верхнього рівня рідко використовують усі команди.

– RISC (англ. *reduced instruction set computing*) – архітектура з скороченим набором команд. Такі процесори, загалом, працюють швидше, ніж із CISC-архитектурой, рахунок спрощення архітектури та скорочення кількості команд, але виконання складної команди вона складається з набору простих, що збільшує час виконання команди (за більшу кількість тактів). Варто відзначити, що сучасні процесори RISC по внутрішній складності наближаються, а то й перевершують класичні аналоги CISC.

– MISC (англ. *minimal instruction set computing*) – архітектура з мінімальним набором команд. Такі процесори мають мінімальну кількість команд, всі команди прості і вимагають невеликої кількості тактів на виконання, але якщо виконуються складні обчислення, наприклад, з числами з плаваючою комою, такі команди виконуються за істотно більшу кількість тактів, що перевищує CISC- і RISC-архітектури.

– VLIW (англ. *very long instruction word* – "дуже довга машинна команда") – архітектура з довгою машинною командою, в якій вказується паралельність виконання обчислень. Такі процесори отримали широке застосування у цифровій обробці сигналів.

За принципом поділу пам'яті

– Гарвардська архітектура – характерною рисою є поділ пам'яті програм та пам'яті даних.

– Фон Неймановська архітектура – характерною рисою є спільне зберігання програм та даних.

Розділ № 4. Методи і засоби обробки інформації

4.1. Економне кодування. Префіксний код та його дерево. Алгоритм Шеннона-Фано. Алгоритм Хаффмана. Основні методи економного кодування без втрат послідовної дискретної інформації

4.2. Принципи завадостійкого кодування. Основні характеристики завадостійких кодів. Класифікація завадостійких кодів. Математичний опис процесу кодування і декодування

4.3. Блочні лінійні коди. Коректуючи властивості блочних кодів. Коди з перевіркою на парність. Коди Хеммінга

4.4. Циклічні коди. Засоби опису циклічних кодів. Властивості циклічних кодів по виявленню помилок. Укорочені циклічні коди. Коди Боуза-Чоудхурі-Хоквінгема. Коди Ріда-Соломона. Код Файра

4.1. Економне кодування

Спосіб одержання компактного подання інформації зветься економне кодування.

Теорія економного кодування поєднує в собі кілька різних **напрямків**. У рамках даної теорії методи прийнято розділяти на методи **економного кодування інформації без втрат** (*lossless*) і методи **економного кодування інформації з втратами** (*lossy*). Як слідує з назв, обробка інформації методами першої групи не веде до інформаційних втрат, тоді як використання методів другої групи сполучено з такими втратами.

Методи останньої групи застосовуються до інформації, що містить окремі несуттєві складові (за певних умов ці складові можуть бути частково або повністю вилучені з інформації). Одним із прикладів такої інформації є звукова інформація, призначена для прослуховування. Людський слух, як відомо, сприймає досить обмежений спектр частот, тому зменшення числа збережених звукових гармонік не завжди приводить до погіршення якості звуку.

Принципово інший приклад використання методів економного кодування із втратами – передача телеграфних повідомлень. З метою збільшення швидкості передачі інформації з повідомлень видаляються слова (розділові знаки й т.д.), які не несуть значимого значеннєвого навантаження.

Дана лекція **присвячена** викладу одного з методів першої групи – методів **економного кодування інформації без втрат**. Якщо методи економного кодування із втратами можуть бути орієнтовані на довільний тип інформації, методи економного кодування без втрат використовуються винятково для обробки дискретної інформації.

Уявимо собі деяку гіпотетичну систему кодування, у якій різним символам відповідають коди різної довжини. У методі обмеженого алфавіту довжина коду для всіх символів була однаковою, тобто ми мали справу з так званим рівномірним кодом. Нова система кодування повинна містити в собі зовсім інший тип кодів – **коди змінної довжини**.

У чому ж складається **перевага** нової системи кодування? Виявляється, що використання кодів змінної довжини дозволяє врахувати статистичні особливості появи символів в інформаційному повідомленні. Символам, що зустрічаються часто, доцільно ставити у відповідність короткі коди, а символам, що зустрічаються рідше, – довгі коди. Отримане в такий спосіб інформаційне подання може виявитися істотно більш ефективним у порівнянні з поданням, отриманим із застосуванням рівномірного коду.

Отже, припустимо, що існує спосіб кодування, що дозволяє використовувати кодові комбінації змінної довжини. Задамося питанням: як повинна виглядати залежність довжини коду від імовірності появи символу, що кодується, в інформаційному повідомленні? З теорії, основи якої були закладені К. Шенноном у роботі, слідує, що в системі подання інформації з основою m (при $m = 2$ це двійкова або бінарна система) символу, ймовірність появи якого дорівнює p, оптимально й, що особливо важливо, теоретично припустимо ставити у відповідність код довжини $-\log_m p$. Це означає, наприклад, що символи 128-символьного набору ASCII, що з'являються в потоці інформації з рівною ймовірністю, у двійковій системі подання доцільно кодувати $-\log_2 1/128 = 7$ бітами.

Наведена вище формула лежить в основі теорії економного кодування. Її наслідком є раніше висловлене положення про те, що ефективність подання інформації цілком і повністю залежить від властивостей самої інформації. Для кількісної оцінки цих властивостей Шеннон вводить дві тісно зв'язані між собою характеристики: ентропія (*entropy*) і надмірність (*redundancy*).

Відповідно до цього, оптимальна довжина коду символу визначається ймовірністю його появи на виході джерела інформації. У реальних задачах ми звичайно не знаємо цю ймовірність, однак можемо одержати її оцінку на основі деякої інформаційної моделі.

У даній лекції нас не будуть цікавити способи обчислення імовірнісних оцінок; ми займемося вивченням методик генерації систем кодів змінної довжини по вже заданих імовірнісних розподілах. Такі системи звичайно одержують або з використанням префіксного кодування, або з використанням арифметичного кодування.

Префіксне кодування є найпростішим методом генерації кодів змінної довжини. Коди, одержувані з використанням префіксного кодування, мають цілу довжину в одиницях подання інформації. Перевага префіксного кодування заключається в його простоті й високій продуктивності, а недолік – у неможливості створювати коди нецілої довжини, що, природно, негативно позначається на ефективності кодування. По зрозумілих причинах (Мінімальна довжина префіксного коду дорівнює інформаційній одиниці), найбільші втрати в ефективності при використанні префіксного кодування спостерігаються у випадку частої генерації кодів, теоретично оптимальна довжина яких близька до нуля.

На відміну від префіксного кодування, арифметичне кодування дозволяє генерувати коди як цілої, так і нецілої довжини. Будучи теоретично оптимальним

методом, арифметичне кодування перевершує в ефективності префіксне кодування. Воно також випереджає префіксне кодування у швидкості побудови системи кодів, однак через підвищену складність нерідко помітно уступає у швидкості самого кодування (мається на увазі процес генерації кодової послідовності).

Незважаючи на деякі істотні переваги арифметичного кодування, даний метод до останнього часу був недостатньо розповсюджений на практиці. На сьогоднішній день у більшості комерційних додатків для побудови системи кодів змінної довжини використовується кодування Хаффмана, що є кращим з погляду ефективності, реалізацією префіксного кодування. Арифметичне кодування застосовується лише в тих випадках, коли потрібно домогтися максимально можливої якості інформаційного подання й коли швидкість роботи не має вирішального значення.

Префіксне кодування

Префіксне кодування засноване на виробленні систем кодів змінної довжини, які прийнято називати системами префіксних кодів (або кодів префікса). Особливість цих систем полягає в тому, що в межах кожної з них більше короткі по довжині коди не збігаються з початком (префіксом) більше довгих кодів – так звана властивість префікса.

Розглянемо систему із трьох двійкових кодів: {«0», «10», «11»}. Як видно, жоден із цих кодів не є початком іншого. Таким чином, про дану систему можна говорити як про систему префіксних кодів. Нехай трьом обраним кодам відповідають символи «А», «П» і «Ш». Тоді інформаційному повідомленню «АПАШ» буде відповідати кодова послідовність «010011». Спробуємо відновити вихідне повідомлення по даній кодовій послідовності. Перший нульовий біт можна інтерпретувати тільки як символ «А», тому що коди, що відповідають символам «П» і «Ш», починаються з одиниці. За першим бітом слідує одиничний біт, що може бути початком кодів відразу двох символів: «П» і «Ш». Визначити наступний символ дозволяє значення третього біта, що однозначно вказує на символ «b». На даному етапі відновлена частина повідомлення здобуває вид «АП». Слідом за кодом символу «П» знову треба нульовий біт. Як ми з'ясували, це код, що відповідає символу «А». Завершують кодову послідовність два одиничних біти. Так само, як і в розглянутому вище випадку, значення останнього з них дозволяє однозначно відтворити останній символ закодованого повідомлення – «Ш». Отже, нам удалося правильно декодувати всю кодову послідовність. Як неважко зрозуміти, це стало можливим завдяки виконанню властивості префікса.

Що дає на практиці така система префіксних кодів? У наведеному прикладі символ «a» зустрічається в повідомленні «abac» з відносною частотою 1/2, а символи «b» і «c» – з відносною частотою 1/4. Припустимо, що інформаційне джерело, що породило дане повідомлення, є джерелом без пам'яті. Через брак інших відомостей про джерело, логічно вважати ймовірності появи символів його на виході рівними відносним частотам. Тоді оптимальна довжина коду для символу «a» повинна бути дорівнює $-\log_2 1/2 = 1$ біт, а для символів «b» і «c»

$-\log_2 1/4 = 2$ біта. Як видно, обрана система префіксних кодів перебуває в повній відповідності з передбачуваним імовірнісним розподілом.

Застосування префіксного кодування в розглянутому прикладі дозволило одержати оптимальне з погляду компактності подання інформаційного повідомлення. Однак, якщо до даного повідомлення додати ще один символ «a», використання префіксного кодування вже не дасть оптимального результату. Символ «a» буде зустрічатися в новому повідомленні з відносною частотою 3/5, а символи «b» та «c» – з відносною частотою 1/5. Оптимальні довжини кодів для символів «a», «b» та «c» будуть відповідно рівні $-\log_2 3/5 \approx 0{,}74$, $-\log_2 1/5 \approx 2{,}35$ та $-\log_2 1/5 \approx 2{,}35$ біта. Таким чином, для подання нового повідомлення досить приблизно 6.86 біта. Для порівняння, максимально можлива ефективність префіксного кодування в цьому випадку становить 7 біт.

Системи префіксних кодів звичайно одержують побудовою кодових дерев. Ступінь розгалуження в цих деревах залежить від основі системи подання інформації. Розглянемо випадок двійкової системи подання, якій відповідають бінарні кодові дерева (наступне міркування легко поширюється й на випадок m-*ічної* системи подання). Як відомо, кожний внутрішній вузол бінарного дерева має до двох вихідних ребер. Пронумеруємо ці ребра так, щоб одному з них відповідав двійковий символ «0», а іншому – «1». Так як в дереві не може бути циклів, від кореневого вузла до листового вузла завжди можна прокласти єдиний маршрут. Якщо ребра дерева пронумеровані, то кожному такому маршруту відповідає деяка унікальна двійкова послідовність. Множина всіх таких послідовностей, утворить систему префіксних кодів.

Легко зрозуміти, що будь-якій системі префіксних кодів однозначно відповідає деяке кодове дерево (наприклад, розглянутій системі префіксних кодів {«0», «10», «11»} відповідає кодове дерево, зображене на мал.1). Таким чином, виконання властивості префікса можна інтерпретувати як наявність особливої деревоподібної організації усередині системи кодів змінної довжини. Крім такого геометричного трактування властивості префікса, можлива також і алгебраїчне трактування, що говорить, що система префіксних кодів з натуральними довжинами $l_1 ... l_N$ в системі подання інформації з підставою m може існувати тоді й тільки тоді, коли виконується нерівність Крафта:

$$\sum_{i=1}^{N} m^{-l_i} \le 1.$$

Для того щоб переконатися в тотожності цих, на перший погляд несхожих тверджень, досить помітити, що виконання нерівності Крафта фактично еквівалентно існуванню дерева з N листовими вузлами, що перебувають на відстанях l_i від кореневого вузла.

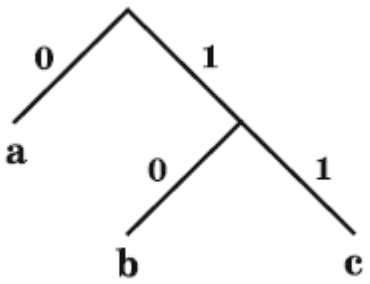


Рисунок 4.1 – Бінарне кодове дерево для системи префіксних кодів {«0», «10», «11»}(коди відповідають символам «a», «b» і «c»)

Кодові дерева необхідно будувати таким чином, щоб довжини маршрутів, що ведуть від кореневого вузла до листових вузлів, були максимально наближені до теоретично оптимальних довжин кодів, що відповідають різним символам інформаційного алфавіту. Помітимо, що мова тут йде лише про довжини маршрутів, але не про самі маршрути. Справа в тому, що нумерація ребер кодового дерева може бути здійснена абсолютно довільним образом, що обумовлює довільність у виборі маршруту, тобто, в остаточному підсумку, довільність у виборі складу префіксного коду. Інакше кажучи, конкретна комбінація нулів і одиниць, яка складає префіксний код, не грає особливої ролі, а визначальне значення має тільки його довжина. Таким чином, для заданого імовірнісного розподілу може бути побудоване відразу кілька кодових дерев, що відповідають різним оптимальним системам префіксних кодів.

Отже, як же будувати ці дерева? Найбільш відомими алгоритмами побудови кодових дерев з конфігурацією, що відповідає заданому ймовірнісному розподілу, є алгоритми Шеннона-Фано й Хаффмана. Як було зазначено вище, система кодів, отримана із застосуванням алгоритму Хаффмана, є кращою з погляду якості інформаційного подання серед всіх можливих систем префіксних кодів. Алгоритм Шеннона-Фано менш ефективний, однак він істотно більше простий і наочний. Крім алгоритмів Шеннона-Фано й Хаффмана, можна також виділити алгоритми Голомба й Райса. Розглянемо найпоширеніші алгоритми префіксного кодування стосовно до двійкової системи подання інформації.

Алгоритм Шеннона-Фано

Розглянутий алгоритм запропонували незалежно друг від друга Р. Фано і К. Шеннон. Алгоритм являє собою рекурсивну процедуру, що дозволяє на основі заданого імовірнісного розподілу появи символів на виході джерела інформації поетапно формувати систему, що відповідає йому, префіксних кодів.

Спочатку кожному символу інформаційного алфавіту ставиться у відповідність код нульової довжини («порожній» код) і вага, рівна ймовірності появи символу на виході інформаційного джерела в рамках обраної інформаційної моделі. Всі символи алфавіту сортуються по убуванню або зростанню їхніх ваг, після чого впорядкований ряд символів у деякому місці ділиться на дві частини так, щоб у кожній з них сума ваг символів була приблизно однакова. До коду символів, що належать однієї із частин, додається

«0», а до коду символів, що належать іншої частини, додається «1» (додається значення, що, формує черговий крайній правий розряд коду). Як неважко зрозуміти, кожна із зазначених частин сама по собі є впорядкованим рядом символів. Кожний із цих рядів, якщо він містить більше одного символу, у свою чергу ділиться на дві частини відповідно до описаного вище принципом, і до коду символів знову додаються відповідні двійкові значення й т.д. Процес завершується тоді, коли у всіх отриманих у такий спосіб рядах залишається рівно по одному символу.

Як видно, алгоритм Шеннона-Фано в дійсності не будує кодове дерево, однак його роботу можна проілюструвати такою побудовою. При поділі групи символів відбувається як би розгалуження деякого вузла бінарного дерева (листовий вузол стає вузлом батьком для двох новостворених дочірніх вузлів), а присвоєння нулів і одиниць рівносильно встановленню відповідності між кодами й маршрутами руху по дереву від кореневого вузла до листового вузла. Робота алгоритму Шеннона-Фано проілюстрована на наступному прикладі (рис. 4.2).

Як же ми ділили на групи ? Досить просто:

Розміщаємо символи по ймовірності появи.

1. ймовірність першої групи (**p1**) і другої (**p2**) дорівнює нулю;
2. **p1** <= **p2** ?
   - так: додати в першу групу символ з початку таблиці;
   - ні: додати в другу групу символ з кінця таблиці;
3. якщо всі символи розділені на групи, то завершити алгоритм, інакше перейти до кроку **2**

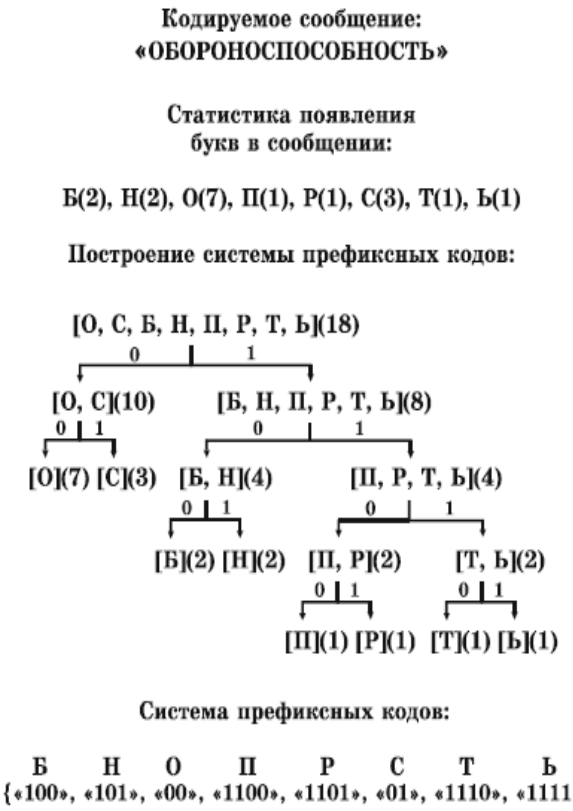


Рисунок 4.2 – Ілюстрація роботи алгоритму Шеннона-Фано на прикладі кириллиці

У цьому випадку використовується інформаційна модель, у якій інформаційне джерело, що породжує, розглядається як джерело без пам'яті. Імовірності появи символів у даній моделі заміняються частотами їхнього входження в інформаційне повідомлення. Надалі така модель буде йменуватися нульовою моделлю.

Наскільки обґрунтований такий спосіб побудови системи кодів змінної довжини? Як виявляється, він не універсальний навіть у рамках префіксного кодування. Для доказу досить знайти оптимальну систему префіксних кодів для 5-ти символів, імовірності появи яких рівні 5/13, 2/13, 2/13, 2/13 і 2/13, і переконатися в тому, що система, отримана з використанням алгоритму Шеннона-Фано, у цьому випадку виявляється менш вигідною.

Проте алгоритм Шеннона-Фано досить ефективний. Нескладно показати, що довжина коду символу з імовірністю появи p, отриманого з використанням даного алгоритму, перевищує теоретично оптимальне значення $-\log_2 p$ менш чим на 1 біт. Ефективність алгоритму знаходить підтвердження й на практиці: як правило, алгоритм Шеннона-Фано дуже незначно уступає в ефективності оптимальному алгоритму префіксного кодування – алгоритму Хаффмана.

Алгоритм Хаффмана

Хаффман запропонував будувати кодове дерево не зверху до низу, як це неявно робиться в алгоритмі Шеннона-Фано, – від кореневого вузла до листових вузлів, а знизу нагору – від листових вузлів до кореневого вузла. Такий підхід виявився найбільш ефективним і одержав досить широке поширення.

На початковому етапі роботи алгоритму кожному символу інформаційного алфавіту ставиться у відповідність вага, рівна ймовірності (частоті) появи даного символу в інформації. Символи містяться в список, що сортується по убуванню ваг. На кожному кроці (ітерації) два останніх елементи списку поєднуються в новий елемент, що потім міститься в список замість двох поєднуваних елементів. Новому елементу списку ставиться у відповідність вага, дорівнює сумі ваг елементів, що заміщаються. Кожна ітерація закінчується впорядкуванням отриманого нового списку, що завжди містить на один елемент менше, ніж старий список. Паралельно з роботою зазначеної процедури здійснюється послідовна побудова кодового дерева. На кожному кроці алгоритму будь-якому елементу списку відповідає кореневий вузол бінарного дерева, що складається з вершин, які відповідають елементам, об'єднанням яких був отриманий даний елемент. При об'єднанні двох елементів списку відбувається об'єднання відповідних дерев в одне нове бінарне дерево, у якому кореневий вузол відповідає новому елементу, що поміщається в список, а елементам списку, що заміщуються, відповідають дочірні вузли цього кореневого вузла. Алгоритм завершує роботу, коли в списку залишається один елемент, що відповідає кореневому вузлу побудованого бінарного дерева. Це дерево називається деревом Хаффмана. Система префіксних кодів може бути отримана шляхом присвоювання конкретних двійкових значень ребрам цього дерева. Приклад побудови дерева Хаффмана наведений на рис. 4.3.

Отже, система кодів, отримана в результаті побудови дерева Хаффмана, є оптимальною системою префіксних кодів. Звідси, однак, у жодному разі не треба висновок про те, що префіксні системи, отримані з використанням інших алгоритмів, завжди менш ефективні. Так, на розглянутих прикладах (див. рис. 4.2 та 1.3) добре видно, що алгоритми Шеннона-Фано й Хаффмана, хоча й будують зовсім різні кодові системи (коди для тих самих символів розрізняються як по довжині, так і по складу), у даному конкретному випадку виявляються однаково ефективними – при використанні кожного із цих алгоритмів об'єм подання повідомлення «ОБОРОНОСПОСОБНОСТЬ» дорівнює 48 бітам. Таким чином, алгоритм Хаффмана є не єдиним алгоритмом, що дозволяє будувати оптимальні системи префиксних кодів, однак єдиним до кінця універсальним алгоритмом – на відміну від інших алгоритмів, даний алгоритм завжди оптимальний.

Основний **недолік** алгоритму Хаффмана полягає в складності процесу побудови системи кодів. Багато альтернативних алгоритмів префіксного кодування, зокрема алгоритм Шеннона-Фано, представляються щодо цього більш кращими. Справедливості заради помітимо, що дана особливість рідко враховується при виборі алгоритму кодування, тому що, при необхідності частих перебудувань системи кодів, як правило, застосовуються спеціалізовані підходи.

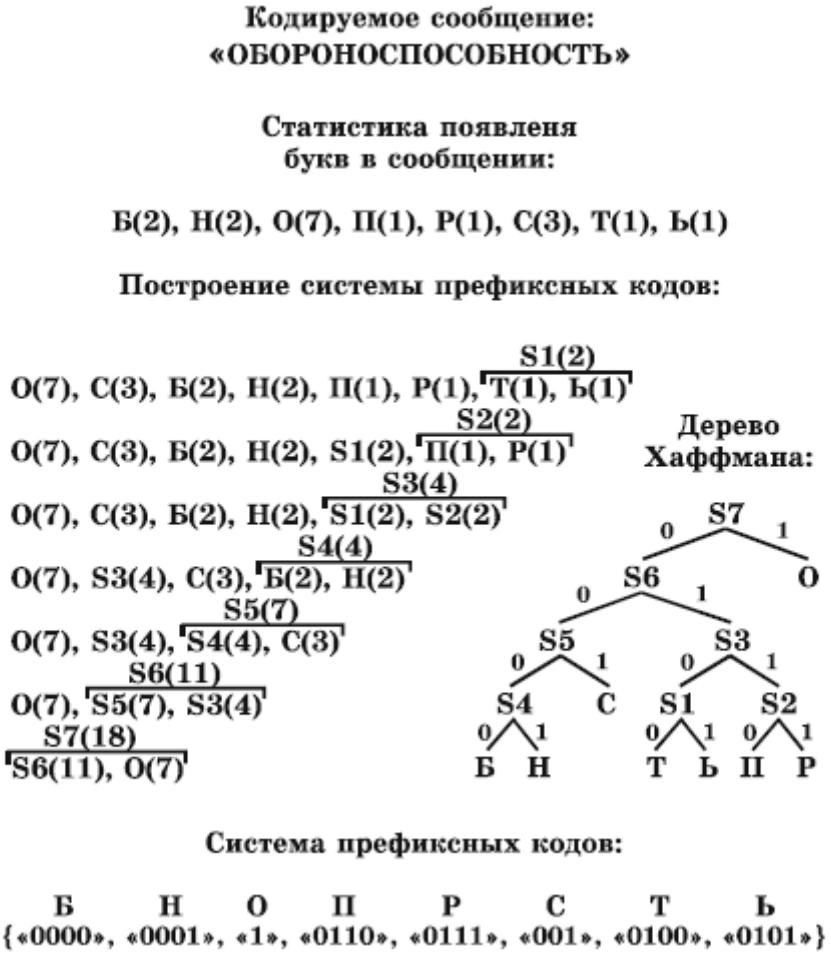


Рисунок 4.3 – Ілюстрація роботи алгоритму Хаффмана на прикладі кирилиці

Алгоритм Хаффмана є найпоширенішим алгоритмом генерації коду змінної довжини. Протягом багатьох років кодування Хаффмана, засноване на найпростішій нульовій інформаційній моделі, виступало в ролі самостійного алгоритму економного кодування.

Сьогодні алгоритм Хаффмана використовується винятково як спосіб одержання систем кодів змінної довжини. Він знаходить своє втілення в більшості утиліт стиску й архівації інформації.

Основні методи економного кодування без втрат послідовної дискретної інформації

Методи цієї групи підрозділяються в такий спосіб:

1. Статистичні методи.

1.1. Метод PPM

1.2. Метод CTW

1.3. Метод DMC

1.4. Економне кодування, засноване на використанні штучних нейронних мереж

2. Словникові методи
2.1. Алгоритми сімейства LZ77
2.2. Алгоритми сімейства LZ78
2.3. Алгоритми групи LZRW
2.4. Комбіновані алгоритми сімейства LZ77
2.5. Алгоритм LZP
3. Контекстні методи
3.1. Асоціативне кодування (метод ACB)
3.2. Метод Барроуза-Уілера

Методи перших двох груп будуються на основі відповідно статистичних і словникових моделей. Вони досить численні й представляють майже всі існуючі підходи в області економного кодування дискретної інформації. Методи третьої групи менш численні й погано піддаються класифікації по типу інформаційної моделі. На сьогоднішній день контекстна група містить у собі тільки два методи, в одному з яких використовується модель, яку варто скоріше віднести до словникових моделей, а в іншому – модель особливого типу, що не є ні словниковою, ні статистичною. Причиною виділення даних методів в окрему групу послужило те, що вони оперують інформаційними об'єктами – контекстами даних. Розглянемо докладніше основні методи кожної з перерахованих груп.

Статистичні методи

Для здійснення ефективного економного кодування повідомлень, що надходять із виходу джерела інформації, потрібне знання його характеристик. При розгляді джерел з пам'яттю, як ми знаємо, за такі характеристики прийнято брати умовні ймовірності появи символів у повідомленні слідом за різними символьними послідовностями. У випадку, коли немає ніякої додаткової інформації про джерело, визначити ці ймовірності можна тільки шляхом статистичного аналізу його інформаційної вибірки. Даний **принцип** лежить в основі статистичних методів економного кодування. Послідовність символів, які безпосередньо передують деякому символу в інформаційному повідомленні, прийнято називати **контекстом цього символу**, а довжину цієї послідовності – **порядком контексту**. На основі статистики, що збирається під час обробки інформації, статистичний метод дозволяє оцінити ймовірність появи в поточному контексті довільного символу або послідовності символів. Оцінка ймовірності визначає довжину коду, що, як правило, генерується з використанням арифметичного кодування. Статистичні методи здебільшого є адаптивними методами. Обчислення імовірнісних оцінок здійснюється тим самим способом на етапах кодування й декодування, що дозволяє не зберігати опис інформаційної моделі. Статистичні методи відрізняються способом одержання оцінок умовних ймовірностей появи символів у різних контекстах. На сьогоднішній день можна виділити чотири основних способи одержання таких оцінок, які лягли в основу відповідно чотирьох статистичних методів: методу PPM, методу DMC, методу CTW і методу, заснованого на використанні

нейронних мереж. Найбільше поширення серед перерахованих методів одержав запропонований ще в середині 80-х років метод PPM, довгий час практично що безроздільно був найбільш ефективним методом економного кодування. Метод DMC, хоча й з'явився практично одночасно з методом PPM, все-таки не одержав такого широкого поширення. Він має меншу ефективність у порівнянні з методом PPM і становить інтерес в основному тільки з ідейної точки зору. Два методи, що залишилися відносяться до сучасних статистичних методів економного кодування. Метод CTW став результатом цілеспрямованих теоретичних досліджень по пошуку так званого «універсального» методу економного кодування. На відміну від методу CTW, метод економного кодування, заснований на використанні нейронних мереж, спочатку взагалі не мав прямого відношення до області економного кодування. Він розроблявся як загальний метод моделювання й пророкування в рамках зовсім іншої дисципліни – теорії штучних нейронних мереж. Обидва зазначених методів відбивають найбільш перспективні напрямки надалі розвитку статистичного підходу в економному кодуванні й уже сьогодні можуть скласти конкуренцію методу PPM.

Словникові методи

У попередньому викладі інформаційні закономірності розглядалися як чисто імовірнісні. Альтернативне трактування має на увазі використання так званого комбінаторного підходу. У новому трактуванні проявом інформаційних закономірностей є присутність в інформації одних символів або символьних комбінацій і повна відсутність інших. Помітимо, що в цьому випадку ми не говоримо про імовірнісні міжсимвольні взаємозв'язки, а просто констатуємо факт наявності або відсутності окремих символьних ланцюжків в інформації.

Кодування в рамках комбінаторного підходу ґрунтується на побудові кодових систем, що містять коди тільки тих інформаційних послідовностей, які реально породжуються інформаційним джерелом. Методи, що представляють у явному виді зазначений підхід, – методи словникової групи, уперше описані в роботах А. Лемпела і Я. Зіва

Словникові методи використовують моделі, основу яких становить інформаційна структура, іменована словником. Під час роботи словникового методу словник містить у собі частини вже обробленої інформації, що виступають як матеріал, на основі якого здійснюється кодування. У процесі кодування складові символьної послідовності, що надходить із виходу кодуємого джерела, кодуються за допомогою посилань на ідентичні їм елементи словника (збіги). Словникові методи відрізняються друг від друга способом організації словника, схемою пошуку збігів і видом посилання на знайдений збіг.

Розбивка оброблюваної послідовності на кодуємі складові являє собою важкорозв'язну задачу, від оптимальності рішення якої у високому ступені залежить ефективність словникового методу.

Розглянемо цю проблему на конкретному прикладі. Припустимо, що необхідно обробити послідовність символів «АПАШ», і при цьому відомо, що словник містить чотири рядки: «А», «АП», «Ш», «ПАШ». Очевидно, що

послідовність можна розбити на складовими двома різними способами: «АПАШ» = «АП» + «А» + «Ш» або «АПАШ» = «А» + «ПАШ». В основі першого способу, називаного «жадібним» розбором (*greedy parsing*), лежить вибір найбільш довгого збігу при послідовній розбивці послідовності ліворуч праворуч. Другий спосіб, іменований оптимальним розбором (*optimal parsing*), полягає в знаходженні найкращої розбивки із всіх можливих. Через колосальну обчислювальну складність оптимальний розбір не використовується на практиці. Замість нього в більшості випадків використовується «жадібний» розбір, що легко реалізуємо й, крім того, зручний при послідовній обробці інформації. Однак «жадібний» розбір не оптимальний з погляду ефективності. Для її підвищення рекомендується робити пошук збігів, починаючи не тільки з першої оброблюваної позиції, але й декількох наступних позицій. Збіг варто вибирати, керуючись міркуваннями оптимальності довжини одержуваної кодової комбінації. Даний підхід прийнятий називати ледачим пошуком або ледачим зіставленням (*lazy matching*).

Контекстні методи

Сутність марківського ланцюга як процесу породження інформації полягає в наявності взаємозв'язку між повідомленням і його передісторією, тобто, дотриманням строгої термінології, між повідомленням і його контекстом. Однак, якщо повідомлення залежать від контекстів, у яких вони з'являються, можна стверджувати, що вони також залежать і від наступних за ними повідомлень. У зв'язку із цим доцільно трохи розширити поняття контексту й називати контекстом повідомлення не тільки те, що безпосередньо передує йому, але також і те, що безпосередньо йде за ним. Для проведення розходження між цими, загалом кажучи, неідентичними об'єктами назвемо перший з них **лівобічним контекстом**, а другий – **правобічним контекстом**.

Головне, що відрізняє два даних типи контекстів – це хронологічний порядок їхнього проходження: лівосторонній контекст деякого повідомлення завжди передує його правобічному контексту.

Розглянемо два методи економного кодування, в основу яких був покладений облік залежності між символьним контекстом і його доповненням. Незважаючи на ідейну спільність, ми маємо справу із зовсім різними підходами, в одному з яких генерація оброблюваної інформації розглядається як послідовний процес, а в іншому – як одноразовий акт. Метод АСВ, що представляє перший підхід, призначений для послідовної обробки інформації, що надходить на вхід кодера відповідно до умовної хронології її народження. Так само, як і більшість розглянутих методів, метод АСВ ставиться до потокових методів економного кодування. Представником другого, менш стандартного підходу є метод Барроуза-Уілера. Особливість даного методу – непослідовна обробка інформації, що можлива тільки при наявності на будь-якому етапі роботи всього об'єму оброблюваної інформації. Зазначені методи є сучасними високоефективними методами економного кодування, уже сьогодні застосовуваними в реальних додатках і маючими непогані перспективі для подальшого практичного використання.

4.2. Принципи завадостійкого кодування. Основні характеристики завадостійких кодів. Класифікація завадостійких кодів. Математичний опис процесу кодування і декодування

Принципи завадостійкого кодування. Основні характеристики завадостійких кодів

Розглянемо загальну постановку задачі завадостійкого кодування повідомлень.

Від джерела інформації надходить послідовність елементарних повідомлень x_i. Кодування полягає в тому, що послідовність символів джерела заміняється послідовністю m-ічних кодових символів (надалі будемо розглядати тільки двійкові коди, для яких m=2). Зазначене перетворення є взаємнооднозначним, що й дозволяє здійснити в приймачі декодування, тобто відновити повідомлення по прийнятій кодовій комбінації.

У результаті дії перешкод деякі кодові символи в приймачі виділяються перекрученими – одиничні елементи комбінації сприймаються як нульові й навпаки.

Може бути передбачений і режим стирання символів, коли рішення про прийом деяких з них не може бути виконане з необхідною надійністю (упевненістю).

Завадостійке кодування повідомлень має своєю метою перетворення повідомлень x_i, i=1,…,m у послідовність кодових символів x_j, j=1, …, n, що володіє властивістю або виявлення присутності в ній помилок, або виявлення й виправлення цих помилок.

Відразу відзначимо, що не існує кодів кінцевої довжини, що дозволяють виявити й, тим більше, виправити всі можливі помилки. Можна побудувати лише коди, що виявляють або виправляють деяке число помилок певного виду (звичайно найбільш ймовірних або найнебезпечніших).

Визначена мета може бути досягнута тільки введенням надмірності, тобто збільшення числа кодових символів у переданій послідовності стосовно символів, що забезпечують однозначне подання переданих повідомлень (інформаційним символам). Наявність додаткових (надлишкових) символів дозволяє накласти на передані послідовності символів (кодові комбінації) додаткові зв'язки (умови) між ними, перевірка яких на прийомній стороні дає можливість виявити й виправити помилки. Вся сукупність можливих кодових комбінацій у цьому випадку називається завадостійким (коригувальним або надлишковим) кодом.

При використанні завадостійкого коду передаються в канал не всі кодові комбінації, що можна сформувати з наявного числа розрядів, а лише що мають певну властивість і що **називаються дозволеними**. Інші комбінації, що не використовуються, називаються **забороненими**. Введення додаткових розпізнавальних ознак в комбінації, що передаються дозволяє істотно підвищити правильність класифікації.

Завадостійкі коди поділяються на:

– коди, що **виявляють** помилки;

– коди, що **виправляють** помилки.

При використанні кодів, що виявляють помилки вся численність n-розрядних комбінацій розбивається на дві підмножини, що не перехрещуються. Одна підчисленність називається **дозволеною**, а інша – **забороненою**. Передаються тільки дозволені кодові комбінації, що мають певною властивістю. Якщо прийнята кодова комбінація відноситься до дозволених, то вважається, що помилки немає. На прийомній стороні відомо, які з комбінацій є дозволеними, а які забороненими. Тому, якщо передана комбінація в результаті помилки перетвориться в деяку заборонену комбінацію, то така помилка буде виявлена, а за певних умов і виправлена. При побудові кодів, що виправляють помилки вся численність кодових комбінацій розбивається на ряд підмножин, що не перехрещуються. В кожній з підмножин одна дозволена комбінація. При прийомі будь-якої комбінації з даної підмножин споживачу видається дозволена комбінація цієї підмножин.

Можливості по виявленню або виправленню помилок визначаються числом позицій, на яких відрізняються дозволені кодові комбінації, т. т. **кодовою відстанню**.

Кодова відстань між i-ю і j-ю кодовими комбінаціями (**відстань за Хеммінгом**) визначається за формулою:

$$d_{ij} = \sum_{k=1}^{n} (x_{ik} \oplus x_{jk}),$$

де x_{ik} і x_{jk} – значення символів k – й позиції i – й і j – й кодових комбінацій. Число відмінних від 0 символів у кодовому слові x_i називається його **вагою** w_i.

Наприклад, між кодовими комбінаціями 1100101 і 1011100, що відрізняються символами в чотирьох розрядах l=(0111001), відстань дорівнює чотирьом.

Для будь-якого коду $1 \le d \le n$. Мінімальна відстань між дозволеними комбінаціями в даному коді називається **мінімальною кодовою відстанню** й позначається d_{min}.

Таким чином, якщо код має кодову відстань d_{min}, то це позначає, що дозволені комбінації цього коду відрізняються друг від друга не менш чим в d_{min} символах і, отже, тільки поява d_{min} і більше помилок у прийнятій комбінації можуть перевести її в іншу дозволену комбінацію.

З іншого боку, якщо число помилок у комбінації буде менше ніж d_{min}, то стає зрозумілим, що така комбінація помилок буде неодмінно приводити до забороненої комбінації.

В загальному випадку необхідна кодова відстань для забезпечення **виявлення всіх помилок кратності до** t_0 **включно** визначається вираженням $t_0 = d + 1$.

При **виправленні помилок кратності до** t_u **включно** кодова відстань повинна бути рівна $d = 2t_u + 1$. З цих виразів видно, що $t_0 = 2t_u$.

Необхідна кодова відстань при **виправленні помилок кратності до** t_u **включно і виявлення помилок кратності від** $t_u + 1$ **до** t_0 **повинна** бути рівна $d \geq t_u + t_0 + 1$. Необхідна кодова відстань, а отже, і завадостійкість коду визначається **надмірністю коду**, т. є. числом введених перевірочних символів.

Визначимо кількість перевірочних розрядів, необхідну для виправлення t_u **помилок**. Для цього необхідно, щоб за допомогою перевірочних розрядів можна було описати наступні ситуації:

– помилка буде відсутня – 1-й випадок;

– одинока помилка – C_n^1 випадків;

– двократна помилка – C_n^2 випадків;

....

– помилка кратності t_u – $C_n^{t_u}$ випадків,

де C_n^i – число сполучень (комбінацій) з n по i. Таким чином, кількість перевірочних розрядів для виправлення помилок кратності t_u і менш визначається з наступної нерівності:

$$2^k \geq \sum_{i=0}^{t_u} C_n^i, \Rightarrow k \geq \log_2 \sum_{i=0}^{t_u} C_n^i.$$

Даним вираженням можна скористуватися і для знаходження числа перевірочних розрядів для виявлення помилок. Для цього необхідно використати той факт, що число помилок, що виявляються в два рази більше числа помилок, що виправляються.

Отже, для виявлення t_0 помилок кількість перевірочних одиничних елементів повинно задовольняти нерівності:

$$k \geq \log_2 \sum_{i=0}^{t_o/2} C_n^i.$$

Важливими показниками ефективності коду є **коефіцієнти помилок**, що виявляються $K_{ВП}$ та не виявляються $K_{НВ}$, під якими розуміють відношення числа кодових комбінацій з виявленими (невиявленими) помилками до числа всіх можливих комбінацій. Помилки не виявляються, коли кодова комбінація, що передається під впливом завад перетворюється в іншу дозволену. Число всіх дозволених комбінацій при m інформаційних розрядах рівно 2^m. Отже, при передачі будь якої кодової комбінації можливе число випадків невиявлених помилок буде рівно $N_{НП} = 2^m\text{-}1$. Оскільки число всіх можливих помилкових комбінацій рівно 2^n, де n – кількість розрядів у кодовій комбінації, то вираження для визначення величини $K_{НП}$ буде мати вигляд:

$$K_{НП} = \frac{2^m - 1}{2^n} = \frac{1}{2^{n-m}} - \frac{1}{2^n} = \frac{1}{2^k} - \frac{1}{2^n},$$

де $k = n - m$ – число надлишкових розрядів. Так як число всіх заборонених кодових комбінацій рівно $2^n - 2^m$, то коефіцієнт може бути визначений з вираження:

$$K_{вп} = \frac{2^n - 2^m}{2^n} = 1 - \frac{1}{2^k}.$$

Класифікація завадостійких кодів

Коди поділяються (рис. 4.4) на:

– блочні (блокові);

– безперервні.

До **блочних** відносяться коди, у яких кожному повідомленню ставиться в однозначну відповідність блок з n символів. **Безперервні** коди представляють безперервну послідовність інформаційних і перевірочних розрядів.

Блочні коди діляться на:

– рівномірні;

– нерівномірні.

Рівномірні коди діляться на:

– систематичні;

– несистематичні.

Під **систематичними** розуміють код, в якому розряди можуть бути поділені на перевірочні і інформаційні. При цьому їхні місця в кодовій комбінації цілком визначені. Несистематичні коди цю властивість не мають.

Окрім цього, коди діляться на:

– лінійні;

– нелінійні.

Лінійні коди це такі, у яких сума за модулем 2 дозволених комбінацій дасть дозволену комбінацію того же коду. Нелінійні коди означену властивість не мають. Передані повідомлення визначаються m інформаційними символами. Надлишкові (контрольні, перевірочні) k символів доповнюють кодову комбінацію до $n = m + k$ символів, у силу чого такі блокові коди позначають як (n,m) коди

Більшість кодів, що застосовуються на практиці, відноситься до лінійних. Найбільше поширення серед блокових кодів знайшли коди з перевіркою на парність, з повторенням символів, рівноважні коди, коди Хеммінга, коди Ріда-Малера й, найбільш великий клас кодів – циклічні коди. До останнього класу належать коди Боуза-Чоудхури-Хоквингема (БЧХ) і коди Ріда-Соломона (РС), що одержали найбільше поширення в техніці військового зв'язку.

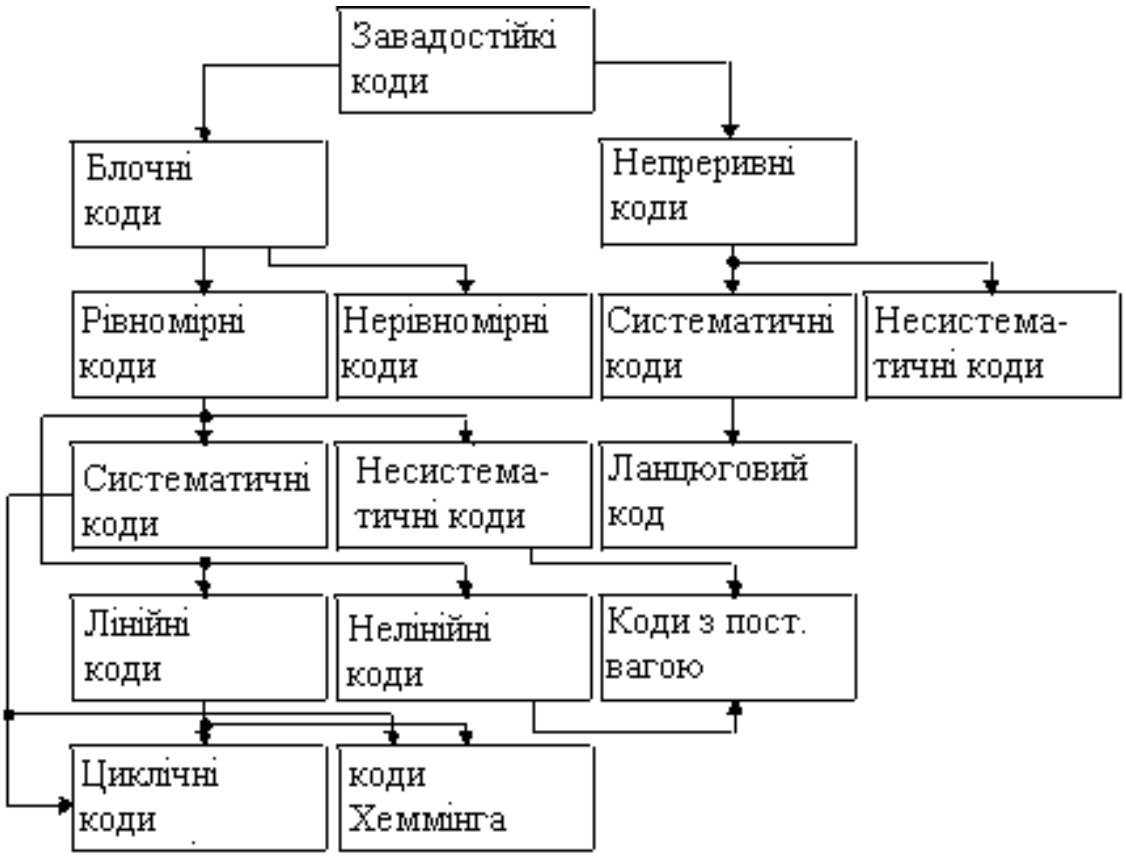


Рисунок 4.4 – Класифікація завадостійких кодів

Математичний опис процесу кодування і декодування

При завданні коду звичайно вказують, які інформаційні елементи беруть участь в формуванні кожного з k перевірочних розрядів. Наприклад, для коду з n = 5, m =3, k = 2 кожний перевірочний розряд $П_i$ визначається складанням за модулем 2 по правилу:

$$П_1 = I_1 \oplus I_2;\ П_2 = I_2 \oplus I_3,$$

де I_i – інформаційні розряди.

Комбінація такого коду записується в вигляді $П_2, П_1, I_3, I_2, I_1$. При завданні коду можна вказати всі дозволені для цього коду комбінації. Для лінійних кодів засіб завдання можна значно спростити. Для m інформаційних розрядів число всіх дозволених кодових комбінацій буде рівно 2^m. Виберемо з усіх кодових комбінацій тільки лінійно незалежні. Під **лінійно незалежними кодовими комбінаціями** розуміють такі, сума за модулем 2 яких (в будь-якому поєднанні) не рівна нулю. Для наведеного прикладу такими комбінаціями можуть бути комбінації вигляду:

1) 01001	2) 01001	3) 01001
11010	10011	10011
10100	01110	00111

Всі інші кодові комбінації можна отримати складанням за модулем 2 лінійних незалежних комбінацій. Звичайно лінійно незалежні кодові комбінації записують в вигляді матриці розміром $n \times m$, яку називають **породжуючою матрицею** і позначають $G(n \times m)$. Найбільш часто породжуючі матриці записують так званій **канонічній формі**. При цьому перші або останні m стовпчиків утворять одиничну матрицю. Інші стовпчики вказують правила формування перевірочних розрядів. Так, для наведеного прикладу породжуюча матриця в канонічній формі має вигляд:

$$G(5,3) = \left\| \begin{matrix} 10100 \\ 11010 \\ 01001 \end{matrix} \right\|.$$

З прикладу видно, що останні три стовпчика складають одиничну матрицю; другий стовпчик вказує, що при формуванні першого перевірочного розряду беруть участь перший і другій інформаційні розряди. Перший стовпчик вказує, що при формуванні другого перевірочного розряду беруть участь другій і третій інформаційні розряди. Позначають породжуючу матрицю, що написана в канонічній формі, наступним чином:

$$G(n,m) = \left\| R_{k \times m} \cdot I_m \right\| \quad \text{або} \quad G(n,m) = \left\| I_m \cdot R_{k \times m} \right\|.$$

Процес кодування математично записується в вигляді добутку матриці – рядка, що відображає кодову комбінацію, яка передається, на породжуючу матрицю. Припустимо, що кодова комбінація, яка передається, записана в вигляді вектору:

$$I = \left\| I_m I_{m-1} \ldots I_2 I_1 \right\|.$$

Тоді процес кодування запишеться в вигляді:

$$F = IG(n,m) = \left\| \underbrace{\Pi_k \Pi_{k-1} \ldots \Pi_1}_{\begin{matrix}\text{перевір.} \\ \text{розряди}\end{matrix}} \; \underbrace{I_m I_{m-1} I_{m-2} \ldots I_2 I_1}_{\begin{matrix}\text{інформ.} \\ \text{розряди}\end{matrix}} \right\|.$$

В результаті кодування отримаємо комбінацію, де перші m розрядів – інформаційні, а останні k розрядів – перевірочні Π_j.

Процес декодування математично описують добутком перевірочної матриці $H(n,m)$ і вектору-стовпчика, що відображає прийняту кодову комбінацію $F = F^T + E^T$, де E^T – вектор помилки

$$C = H(n,m)(F^T + E^T), \tag{4.1}$$

де:

C – результат декодування (синдром);

$(\ )^T$ – знак транспонування.

Оскільки зв'язок між породжуючою і перевірочною матрицями визначається рівністю:

$$G(n,m)\,H^T(n,m) = H(n,m)\,G^T(n,m) = 0,$$

то рівність (4.1) буде мати вигляд:

$$C = H(n,m)\,E^T = E\,H^T(n,m).$$

Якщо позначити h_i – i – й стовпчик перевірочної матриці, то: $H(n,m) = \|h_1 h_2 \ldots h_n\|$.

Вектор помилки ($E = \|0010 \ldots 010 \ldots 0\|$) містить **1** на тих позиціях, символи на яких викривлені. Нехай ці позиції мають номери $n_1, n_2, \ldots n_\ell$. Тоді буде справедливо рівність:

$$C = H(n,m)\,E^T = \sum_{i=1}^{\ell} h_{\nu_i}.$$

Отже, якщо необхідно виявити ℓ помилок, то повинно бути виконана умова:

$$\sum_{i=1}^{\ell} h_{\nu_i} \neq 0$$

при будь-якому поєднанні ℓ викривлених символів. Якщо необхідно виправити ℓ помилок, то сума: $\sum_{i=1}^{\ell} h_{\nu_i}$ для будь-яких ℓ конкретних стовпчиків перевірочної матриці повинна бути цілком певною, і не співпадати з аналогічною сумою для інших ℓ стовпчиків. Так, наприклад, при виправленні одинокої помилки всі стовпчики перевірочної матриці повинні бути різноманітні, т. т. $h_i \neq h_j$ при будь-яких i i j, $i \neq j$. Якщо необхідно виправити одиноку помилку і виявити пакет, який складається з трьох і двох символів, то необхідно виконати наступні умови:

– $h_i \neq h_j$ при $i \neq j$ (для виправлення одинокої помилки);

– $h_i + h_{i+1} \neq 0; h_i + h_{i+1} \neq h_j$ при будь-яких i i j (для виявлення пакету з двох помилок);

– $h_i + h_{i+1} + h_{i+2} \neq 0; h_i + h_{i+1} + h_{i+2} \neq h_j$ при будь-яких i i j (для виявлення пакету з трьох помилок).

Матриці $H(n,m)$ і $G(n,m)$ можна змінити ролями. Тоді матриця $H(n,m)$ буде породжуючою, а $G(n,m)$ – перевірочною. Коди, взаємозв'язані між собою таким чином, називають **дуальними** (подвійними).

4.3. Блочні лінійні коди. Коректуючи властивості блочних кодів. Коди з перевіркою на парність. Коди Хеммінга

Блочні лінійні коди

Коректуючи властивості блочних кодів

У цілому в процесі передачі можна розрізняти три ситуації: перекручування (помилки) відсутні, перекручування виявляються (прийнята заборонена комбінація) і перекручування не виявляються – одна дозволена комбінація переходить в іншу дозволену.

Говорять, що в каналі відбулася помилка кратності t, якщо в кодовій комбінації прийнято помилково t символів.

У результаті можна дійти висновку, що максимальне число помилок, що вірогідно виявляється в комбінації коригувального коду, пов'язане з кодовою відстанню наступним співвідношенням:

$$t_{виявл} = d_{min} - 1$$

При $d_{min} \le t_{виявл}+1$ або при $t \ge t_{виявл}$ прийнята кодова комбінація може виявитися дозволеною й помилка не буде виявлена. Однак і при $t \ge t_{виявл}$ можливі ситуації, коли комбінація виявляється забороненою, тобто частково будуть виявлятися й помилки кратності більшої, ніж $t_{виявл}$ (але це вже не вірогідно).

Як приклад розглянемо властивості, що виявляють, трьохразрядного коду. При $d_{min}=1$ дозволені комбінації – це всі комбінації коду 000, 001, 010, 011, 100, 101, 110, 111.

Будь-яка одиночна помилка трансформує кожну із цих комбінацій в іншу дозволену, отже достовірне виявлення помилок неможливо.

При $d_{min}=2$ підмножина дозволених комбінацій може бути утворена за принципом парності в них числа одиниць: 000, 011, 101, 110. До заборонених віднесемо інші комбінації: 001, 010, 100, 111. Жодна із заборонених кодових комбінацій при одиночній помилці не переходить в іншу дозволену комбінацію, тобто при $d_{min}=2$ код вірогідно виявляє всі одиночні помилки. Що стосується помилок більш високої кратності, то частина з них виявляється, а частина ні. Так виявляються всі трикратні помилки, однак дворазові помилки переводять одну дозволену кодову комбінацію в іншу й не можуть бути виявлені. Збільшення кодової відстані до $d_{min}=3$ дозволяють використовувати для передачі тільки дві кодові комбінації 000 і 111 або 001 і 110 і т.д., але зате тут уже й дворазова помилка не може перевести одну дозволену кодову комбінацію в іншу.

Модель трикратного коду можна використовувати й для пояснення принципів використання надмірності для виправлення помилок.

Основою методики, що викладається, є припущення про те, що чим більше кратність помилки, тим вона менше ймовірна. Це припущення гарно погоджується з біноміальною моделлю помилок у дискретному каналі зв'язку.

У цьому випадку при помилках найбільшу ймовірність будуть мати помилкові комбінації віддалені від переданої дозволеної на відстані d=1, менш імовірними будуть переходи в комбінації віддалені від переданої на відстані d=2 і т.д.

У результаті в процесі прийому-передачі кодових комбінацій по каналу зв'язку з помилками кожна з дозволених (переданих) комбінацій буде трансформуватися в деяку множину прийнятих кодових комбінацій, локалізованих у методиці Хемминга навколо переданої дозволеної кодової комбінації (якщо її відображати точкою відповідного n-мірного простору). Збільшуючи відстань між центрами цих областей в n-мірному просторі (точками, що відповідають дозволеним кодовим комбінаціям), можна реалізувати процедуру виправлення помилок заданої кратності, якщо ухвалювати рішення щодо декодування тієї дозволеної комбінації, відстань якої від прийнятої (забороненої) кодової комбінації виявляється мінімальним (декодування по найменшій відстані). Цей метод декодування є оптимальним для симетричного каналу (для інших може бути й не оптимальним)

Легко тепер зрозуміти, що максимальне число помилок, що **імовірно виправляються**, у комбінації коригувального коду пов'язане з кодовою відстанню коду нерівністю (якщо d_{min} – непарне):

$$t_{випр} \le (d_{min}-1)/2,$$

і, якщо d_{min} – парне:

$$t_{випр} \le d_{min}/2 - 1.$$

Дійсно, для виправлення помилок кратності t необхідно включити в кожну із зазначених вище підмножин всі заборонені кодові комбінації, що відстоять від дозволеної на відстань d=t. Для того, щоб сусідні підмножини не перетиналися, відстань між найближчими дозволеними комбінаціями повинне бути не менше 2t+1.

Таким чином, код має властивість **виявляти й виправляти t-кратні помилки**, якщо виконується умова

$$d_{min} \ge 2t+1 \qquad (4.2)$$

Звернемося знову до трьохразрядного коду. За дозволені комбінації приймемо 000 і 111. Тоді дозволеної комбінації 000 відповідає підмножина заборонених комбінацій 001, 010, 100, що утворяться за рахунок виникнення однократної помилки. Подібним же чином дозволеної комбінації 111 відповідає підмножина заборонених комбінацій 110, 101, 011.

При однократному перекручуванні кожної із двох дозволених комбінацій прийнята комбінація не вийде за межі “своєї” підмножини й помилка буде виправлена. Що стосується подвійних помилок, то вони виявляються, однак при їхньому виправленні приймаються невірні рішення. Потрійні помилки не виявляються взагалі.

Завадостійке кодування можна застосовувати й у дискретних каналах зі стиранням. Якщо в прийнятій комбінації перекручених символів немає, а є тільки $t_{ст}$ стертих (непізнаних) символів, то при виконанні умови $t_{ст} \le d_{min}-1$ ці символи можуть бути відновлені при декодуванні по мінімуму відстані. Той самий код може декодуватися з виправленням помилок і стирань. **У загальному випадку код з відстанню d_{min} виправляє будь-які $t \le t_{ст}$ стирань і будь-які $t \le t_{випр}$ помилок, якщо $d_{min} \ge 2t_{випр} + t_{ст} + 1$.**

Крім сполучень помилок і стирань, що виявляються й виправляються, кратність яких визначається кодовою відстанню, коди з корекцією часто виправляють або виявляють і багато інших сполучень помилок великої кратності.

Матеріал, розглянутий вище, показує важливу роль кодової відстані d_{min} коду як основного показника його здатності, що виявляє й виправляє. Збільшуючи довжину коду n і зберігаючи число дозволених кодових комбінацій, можна одержати як завгодно велике значення d_{min}. Але зі збільшенням n зменшується швидкість передачі повідомлень. Якщо довжина коду n задана, то будь-яке значення $d_{min} \leq n$ можна одержати, зменшуючи число дозволених комбінацій, але при цьому зменшується й кількість повідомлень, які можна закодувати. Отже, задачу пошуку найкращого коду необхідно формулювати так: при заданих n і N_p знайти код, що має можливо велике значення d_{min}.

Характеристикою коригувального коду, що вказує ступінь подовження кодової комбінації, є **надмірність**. Відносна надмірність може бути виражена співвідношенням:

$$\eta_m = \frac{n-m}{n}$$

відносна швидкість коду:

$$R_n = \frac{m}{n} = 1 - \eta_m$$

Коди, що забезпечують задану коригувальну здатність при мінімальній надмірності, називаються оптимальними.

Загального методу відшукання оптимальних кодів на данний час не існує.

Кодова відстань d_{min} повністю характеризує стійкість коду щодо заданого рівня перешкод. Однак у реальних умовах завадостійкість коду зручно описувати статистичними показниками. До їхнього числа ставляться: імовірність правильного прийому $P_{пр}$, імовірність помилки $P_{пом}$. Ці ймовірності можна визначити, знаючи структуру коду й статистику перешкод.

$$P_{пр} = \sum_{i=0}^{t} C_n^i p_0^i (1-p_0)^{n-i}; P_{ош} = \sum_{i=t+1}^{n} C_n^i p_0^i (1-p_0)^{n-i} = 1 - P_{пр}$$

Часто на перший план виходить не оптимальність коду, а складність технічної реалізації.

Таким чином, завадостійке кодування – найбільш діючий засіб збільшення вірогідності зв'язку.

Кодова відстань d_{min} коду є основним показником його що виявляє й виправляє здатності, при цьому максимальне число помилок, що виявляються вірогідно, у комбінації коригувального коду дорівнює $t_{виявл} = d_{min} - 1$, а що виправляються – $t_{випр} \leq (d_{min}-1)/2$.

Коди з перевіркою на парність

При побудові таких кодів послідовність розрядів, що передається розбивається на групи. В найбільш простому випадку перевірка на парність здійснюється в кожній групі, в результаті чого число одиниць в групі доводиться

до парного. Перевірочна матриця коду з перевіркою на парність має вигляд: $H(n, n-1) = 111...1$.

Основним недоліком коду є невиявлення помилок парної кратності. Тому такі коди знаходять застосування в тих ланках АСУ, де найбільш ймовірні одинокі помилки, наприклад, в ланці АПД – ЕОМ. Помилки ж, що виникають в каналі зв'язку, мають тенденцію до згуртовування. Для усунення цього недоліку групи розрядів (кодові комбінації) записуються в вигляді матриці. Після цього здійснюється перевірка на парність стовпчиків отриманої матриці.

За наявності однієї групової помилки довжиною не більш числа елементів рядку матриці в кожну перевірку буде входити не більш одного викривленого розряду (відбудеться декореляція помилок). Помилки не будуть виявлені, якщо викривлене число розрядів в стовпчику є парним.

Якщо помилки незалежні, то даний код еквівалентний коду з перевіркою на парність по рядкам. Якщо помилки корельовані, то за рахунок перевірки рознесених розрядів (за рахунок декореляції помилок) даний код буде більш завадостійким.

Для підвищення виявляючої спроможності, перевірка на парність може бути проведена водночас по стовпчикам і діагоналям або по рядкам і стовпчикам. Останній код називають **матричним**. В даному коді перевірочні розряди формуються по наступним правилам:

$$
\begin{array}{llll}
a_{11} \; a_{12} \ldots a_{1q} & b_1 & b_i = a_{i1} + a_{i2} + \ldots + a_{iq}; \\
a_{21} \; a_{22} \ldots a_{2q} & b_2 & c_j = a_{1j} + a_{2j} + \ldots + a_{\ell j}; \\
\ldots\ldots\ldots\ldots & \vdots & \\
a_{\ell 1} \; a_{\ell 2} \ldots a_{\ell q} & b_\ell & c_{q+1} = c_1 + c_2 + \ldots + c_q; \\
\hline
 & & \text{або} \\
c_1 \quad c_2 \ldots c_q & c_{q+1} & c_{q+1} = b_1 + b_2 + \ldots + b_\ell .
\end{array}
$$

При такій побудові коду будуть виявлені всі однократні, двократні і трикратні помилки, а також всі непарні помилки і деякі парні помилки більшої кратності. Код знаходить застосування для виявлення помилок в накопичувачах на магнітних стрічках в ЕОМ.

Матричні коди можуть використовуватися в поєднанні з іншими кодами. При цьому кожний рядок матриці є дозволеною комбінацією будь якого коду. В цьому випадку говорять про добуток двох кодів. Добуток кодів використовується і для виправлення помилок.

Коди Хеммінга

Як показано вище, для виправлення одинокої помилки необхідно, щоб всі стовпчики перевірочної матриці були різноманітні. Якщо число перевірочних символів рівно k, то кількість різноманітних ненульових векторів (для двійкового коду) рівно $2^k - 1$. Коди, у яких довжина кодової комбінації визначається по вираженню $n = 2^k - 1$, число перевірочних розрядів рівно

$k = 3, 4 \ldots$, називають **кодами Хеммінга.** Часто до кодів **Хеммінга** відносять коди, у яких кожний стовпчик перевірочної матриці в двійковому коді відображає номер цього стовпчика.

Так, наприклад, код **Хеммінга (7,4)** має наступну перевірочну матрицю:

$$H(7,4) = \begin{matrix} 1\,2\,3\,4\,5\,6\,7 \\ \left\| \begin{matrix} 1\,0\,1\,0\,1\,0\,1 \\ 0\,1\,1\,0\,0\,1\,1 \\ 0\,0\,0\,1\,1\,1\,1 \end{matrix} \right\| \end{matrix}$$

При такій перевірочній матриці в випадку викривлення одного розряду в результаті декодування отримаємо номер позиції, на якій відбулася помилка. Перевірочні символи в коді **Хеммінга** встановлюються на позиції, що входять тільки в одну перевірку. Такими позиціями є 1, 2, 4.

Для виправлення одинокої і виявлення дворазової помилки додається перевірка на парність всіх позицій кодової комбінації. Перевірочна матриця в цьому випадку має вигляд:

$$H(7,4) = \left\| \begin{matrix} 1\,0\,1\,0\,1\,0\,1 \\ 0\,1\,1\,0\,0\,1\,1 \\ 0\,0\,0\,1\,1\,1\,1 \\ 1\,1\,1\,1\,1\,1\,1 \end{matrix} \right\|$$

Останній рядок цієї матриці забезпечує загальну перевірку на парність. Якщо відбудеться одинока помилка, то загальна перевірка на парність дасть **1**. Інші ж перевірки покажуть номер викривленого розряду. Якщо викривлені два розряди, то загальна перевірка на парність дасть **0**. Інші ж перевірки вкажуть на якусь позицію, але не на ту, на якій відбулися помилки.

Практична реалізація коду Хемінга

Теоретичні відомості. Розглянемо задачу побудови коду, що складається із 16-ти кодових слів виду $a_1a_2a_3a_4$, де a_i=0 або 1, в якому можливе виявлення та виправлення помилок.

Для розв'язку використаємо три допоміжні (перевірочні) символи, тобто кожне з 16-ти кодових слів кодуємо двійковим словом довжини 7: $a_1a_2a_3a_4a_5a_6a_7$. Нашу задачу можливо переформулювати, як визначення одного із чисел 0,1...7, які б вказували на місце похибки (0 – немає похибки). Накладемо умови (у вигляді рівностей за **mod 2**) на перевірочні символи:

$$a_5=a_2+a_3+a_4$$
$$a_6=a_1+a_3+a_4$$
$$a_7=a_1+a_2+a_4$$

Для виявлення похибки достатньо обчислити суму:

$$S_1=a_4+a_5+a_6+a_7.$$

Якщо $S_1=1$ то похибка є, інакше "немає".

При наявності похибки перевіримо, чи не міститься вона серед a_1 чи a_7. Для цього обчислимо $S_2=a_2+a_3+a_6+a_7$.

Якщо $S_1=S_2=1$ то похибка в a_6 або a_7.
Якщо $S_1=1$, $S_2=0$ то похибка в a_4 або a_5.
Якщо $S_1=0$, $S_2=1$ то похибка в a_2 або a_3.
Якщо $S_1=S_2=0$ то похибка в a_1 або немає.

Для визначення місця похибки слід обчислити суму

$$\mathbf{S_3=a_1+a_3+a_5+a_7.}$$

Тобто матимемо три перевірочні відношення

$$\mathbf{S_1=a_4+a_5+a_6+a_7 \neq 0}$$
$$\mathbf{S_2=a_3+a_2+a_6+a_7 \neq 0}$$
$$\mathbf{S_3=a_1+a_3+a_5+a_7 \neq 0}$$

які шляхом порівняння з 0(mod 2) "обчислюють" або відсутність похибки, або вказують її місце. Положення одиничної похибки визначається числом $\mathbf{S_1S_2S_3}$ в двійковій системі лічби. Таким чином маємо код (4,7) Хемінга довжина слова 7 та 4 інформаційні символи.

Якщо виявляти подвійну похибку, то слід виконати перевірку:

$$\mathbf{S_0=a_0+a_1+a_2+a_3+a_4+a_5+a_6+a_7 \neq 0}$$

де $\mathbf{a_0}$ – додатковий (четвертий) перевірочний символ, значення обчислємо за формулою:

$$\mathbf{a_0=a_1+a_2+a_3+a_4+a_5+a_6+a_7 \ (mod\ 2)}$$

Попередні $\mathbf{a_5, a_6, a_7}$ допомагали виявити та виправити одиночну похибку.

Якщо виникла подвійна похибка, то $\mathbf{S_0=0(mod\ 2)}$ та хоча б одне із чисел $\mathbf{S_1,S_2,S_3}$ буде не нульовим. Виправлення такої похибки неможливе. Побудована множина кодових слів зветься розширеним кодом (4,8) Хемінга (довжина слова 8 та з них інформаційними символами).

4.4. Циклічні коди. Засоби опису циклічних кодів. Властивості циклічних кодів по виявленню помилок. Укорочені циклічні коди. Коди Боуза-Чоудхурі-Хоквінгема. Коди Ріда-Соломона. Код Файра

Засоби опису циклічних кодів

Розглянемо циклічні коди. До них відносяться:

– Укорочені циклічні коди.

– Коди Боуза-Чоудхурі-Хоквінгема.

– Коди Ріда-Соломона.

– Код Файра.

Назва цього класу кодів відбулася від основної з властивостей, яка полягає в тому, що результатом порозрядної перестановки (циклічного зсуву) дозволеної кодової комбінації стає також дозволена комбінація.

Циклічні коди зручно описувати багаточленами змінної x. При цьому показники ступеня відповідають номерам розрядів, а коефіцієнтами цього багаточлену є **0** і **1** кодової комбінації, що відображається. Наприклад, комбінацію 1001101 можна записати в вигляді: $x^6 + x^3 + x^2 + 1$.

В теорії циклічних кодів операції над кодовими комбінаціями зводяться до алгебраїчних операцій з отриманими багаточленами в відповідності з законами звичайної алгебри багаточленів, за винятком того, що складання і віднімання замінюється складанням за модулем **2**.

Принцип виявлення помилок циклічним кодом полягає в наступному. В якості дозволених приймаються такі комбінації, що без залишку діляться на заздалегідь вибрану комбінацію, яка відображається породжуючим (утворюючим) багаточленом $P(x)$ ступеня k. Прийнята кодова комбінація підлягає діленню на $P(x)$.

Якщо комбінація викривлена, то утвориться залишок, не рівний нулю, що і забезпечує виявлення помилок.

При кодуванні багаточлен $G(x)$, відповідний m – розрядній інформаційній комбінації беззайвого коду, умножається на x^k, що підвищує ступінь багаточлену від $m-1$ до $n-1$. Після цього добуток $G(x)\,x^k$ ділиться на породжуючий багаточлен $P(x)$ і залишок від ділення $R(x)$ складеться з добутком $G(x)\,x^k$. В результаті одержується кодовий багаточлен $F(x) = G(x)\,x^k + R(x)$, відповідний комбінації циклічного коду.

Операція складання $G(x)\,x^k + R(x)$ означає приписування перевірочних символів на відведені для них k позицій.

Отриманий багаточлен $F(x)$ відповідає дозволеній кодовій комбінації, так як він ділиться без залишку на утворюючий багаточлен $P(x)$. Справді, оскільки $G(x)\,x^k = \varphi(x)\,P(x) + R(x)$, де $\varphi(x)$ - частка від ділення $G(x)\,x^k$ на $P(x)$, то справедлива (з урахуванням заміни алгебраїчного складання на складання за модулем **2**) рівність:

$$G(x)\,x^k + R(x) = \varphi(x)\,P(x) = F(x),$$

що і вимагалося довести.

Прийняту комбінацію, яку позначимо $F'(x)$, можна уявити в вигляді двох доданків: переданого кодового багаточлену $F(x)$ і багаточлену помилки $E(x)$, т. т. $F'(x) = F(x) + E(x)$. Цей багаточлен підлягає діленню на $P(x)$, і по наявності залишку приймається рішення про вірність прийнятої комбінації. Якщо ділення здійснюється без залишку, то приймається рішення про то, що інформація не викривлена.

Циклічні коди можуть задаватися перевірочними або породжуючими матрицями. Так, кожний стовпчик канонічної форми перевірочної матриці можна визначити шляхом знаходження залишків від ділення одночлену $x^i (0 \le i \le n-1)$ на багаточлен $P(x)$.

Наприклад, перевірочна матриця $H(7,4)$ буде мати вигляд:

$$H(7,4) = \|h_1 h_2 h_3 h_4 h_5 h_6 h_7\| = \begin{matrix} 1\,2\,3\,4\,5\,6\,7 \\ \left\|\begin{matrix} 1\,0\,0\,1\,0\,1\,1 \\ 0\,1\,0\,1\,1\,1\,0 \\ 0\,0\,1\,0\,1\,1\,1 \end{matrix}\right\| \end{matrix} \qquad (4.3)$$

В деяких джерелах інформації перевірочна матриця циклічного коду визначається через так звану **матрицю переходів** S. Ця матриця визначається видом утворюючого багаточлену і засобом побудови кодуючих і декодуючих пристроїв. Так, ця матриця може мати наступний вигляд:

$$S = \left\|\begin{matrix} 0\,0\,0\,0\ldots 0\,a_1 \\ 1\,0\,0\,0\ldots 0\,a_2 \\ \ldots\ldots\ldots \\ 0\,0\,0\,0\ldots 1\,a_k \end{matrix}\right\|,$$

де a_k – коефіцієнти в вираженні утворюючого багаточлену.

Наприклад: Написати матрицю переходів при $P(x) = x^3 + x + 1$. Багаточлен $P(x)$ можна написати в вигляді:

$$P(x) = a_4 x^3 + a_3 x^2 + a_2 x + a_1 x^0$$

при $a_4 = 1; a_3 = 0; a_2 = 1; a_1 = 1$. Тоді матриця переходів буде мати вигляд:

$$S = \left\|\begin{matrix} 0\,0\,1 \\ 1\,0\,1 \\ 0\,1\,0 \end{matrix}\right\| \qquad (4.4)$$

Кожний стовпчик перевірочної матриці $h_j^T = \|h_{1j}h_{2j}\ldots h_{kj}\|$ одержується шляхом перемноження матриці S^{j-1} на перший стовпчик матриці H, т. т. $h_j = S^{j-1}h_1$.

Зазвичай в якості першого стовпчика береться матриця $h_1^T = \|100\ldots0\|$. Тоді перевірочну матрицю можна записати в вигляді:

$$H(n,m) = \|I_1, Sh_1, S^2h_1, \ldots, S^{n-1}h_1\| = \|I, S, S^2, \ldots, S^{n-1}\|h_1,$$

де I – одинична матриця.

В результаті декодування отримаємо:

$$C = H(n,m)[п_1п_2п_3\ldots п_kC_mC_{m-1}\ldots C_1]^T = \\ = \|I\,п_1 + Sп_2 + S^2п_3 + \ldots + S^{k-1}п_k + S^kC_m + \ldots + S^{n-1}C_1\|h_1. \qquad (4.5)$$

Властивості циклічних кодів по виявленню помилок

1. Якщо утворюючий багаточлен містить більш одного члена, то циклічний код виявляє всі одиночні помилки. При поданні циклічного коду багаточленами одиночна помилка, описується одночленом $E(x) = x^i$, де i вказує номер викривленого розряду $(0 \le i \le n-1)$. Оскільки одночлен не ділиться на багаточлен без залишку, то помилка буде виявлена.

2. Циклічний код з утворюючим багаточленом $P(x) = x+1$ виявляє всі непарні помилки. Використовуючи правила побудови перевірочної матриці для $P(x) = x+1$, отримаємо: $H = \|111\ldots1\|$.

При такій перевірочній матриці залишок визначається сумою за модулем **2** всіх елементів прийнятої кодової комбінації (перевірка на парність). Тому все викривлення на непарній кількості позицій будуть виявлені. Доказати цю властивість можна і іншим засобом. Відомо, що помилки непарної кратності відображаються багаточленом:

$$E(x) = x^{\alpha}(x^i + \ldots + x^j + 1),$$

в якому число ненульових членів не парно. Так як при діленні такого багаточлена $E(x)$ на багаточлен $P(x) = x+1$ залишок завжди буде рівний **1**, то означені помилки будуть виявлені.

3. Циклічний код виявляє всі одиночні і дворазові помилки, якщо розрядність коду n не більше довжини циклу $\ell_ц$ утворюючого багаточлена, який використовується, т. т. $n \le \ell_ц$. Під **довжиною циклу багаточлена** розуміють мінімальний показник ступеня двочлена $x^{\ell_ц}+1$, при якому цей двочлен ділиться без залишку на утворюючий багаточлен $P(x)$. Дворазова помилка описується двочленом вигляду:

$$E(x) = x^i + x^j = x^j(x^{i-j}+1),$$

де $i \ne j$, $1 \le i-j \le n-1$.

При $n \le \ell_ц$ завжди справедлива нерівність $i - j < \ell_ц$, бо $(i-j)_{макс} = n-1$. З визначення довжини циклу слідує, що двочлен $E(x)$ не ділиться без залишку на $P(x)$. Якщо довжина кодової комбінації більше довжини циклу, т. т. $n > \ell_ц$, то все викривлення, котрі відображаються багаточленом помилки $E(x) = C(x)(x^{\ell_ц + 1})$, не будуть виявлені. Тут $C(x)$ - багаточлен будь-якого ступеня. Отже, при вибраному багаточлену P(x) ступеня k з довжиною циклу $\ell_ц$ число інформаційних символів в кодовій комбінації повинно задовольняти співвідношенню $m \le \ell_ц - k$ (так як $n = m + k$).

4. Циклічний код з багаточленом $P(x)$ ступеня k виявляє всі групові помилки тривалістю в k розрядів і менш. Будь-яка помилка в k розрядів описується багаточленом ступеня $k-1$, т. т.:

$$E(x) = x^i(x^{k-1} + x^{k-2} + \ldots + 1).$$

Багаточлен ступеня $k-1$ на багаточлени ступеню k не ділиться і, таким чином, помилка виявляється.

5. Циклічний код з утворюючим багаточленом $P(x)$ ступеня k не виявляє $\frac{1}{2^{k-1}}$ частину помилок $k+1$- й кратності. В розглядуваному випадку багаточлен помилки має вигляд:

$$E(x) = x^i E_1(x)$$

де $(0 \le i \le m)$, причому $E_1(x)$ має ступінь k. Загальне число можливих багаточленів ступеня k рівно 2^{k-1}. З цих багаточленів лише один співпадає по вигляду з $P(x)$ і ділиться на нього без залишку, а інші – не діляться. Отже, $\frac{1}{2^{k-1}}$ частина розглядуваних помилок не виявляється.

Приклад: Використовується циклічний код з утворюючим багаточленом: $P(x) = x^3 + x^2 + 1$.

Помилки четвертої $(k+1=4)$ кратності описуються чотирма багаточленами $(2^{k-1} = 2^2 = 4)$: $x^3 + x^2 + x + 1;\ x^3 + x^2 + 1;\ x^3 + x + 1;\ x^3 + 1$.

З усіх чотирьох варіантів помилок не виявляється помилка, що описується багаточленом: $E_1(x) = x^3 + x^2 + 1$.

Отже, відносна частина помилок, що не виявляються, четвертої кратності рівна: $\frac{1}{2^{k-1}} = \frac{1}{2^{3-1}} = \frac{1}{4}$.

6. Циклічний код з утворюючим багаточленом $P(x)$ ступеня k не виявляє $\frac{1}{2^k}$ частину помилок більш $k+1$- й кратності. Помилки кратності більш $k+1$ описуються багаточленом: $E(x) = x^i E_1(x)$,

де $E(x)$ – багаточлен ступеня $k+s;\ i = 1, 2, 3, \ldots;\ s = 1, 2, 3, \ldots$.

При діленні будь-якого з багаточленів ступеня k+s утворяться різноманітного вигляду залишки, ступінь яких не перевищує $k-1$. З загального числа залишків, рівного 2^k, тільки один дорівнює нулю, що свідчить про невиявлення помилки. Отже, відносна частина помилок, що не виявляються, кратності вище $k+1$ рівна $\frac{1}{2^k}$.

Аналізуючи перераховані властивості циклічного коду, можна побачити, що хист коду по виявленню і виправленню помилок повністю визначається вибраним утворюючим багаточленом $P(x)$. При виявленні помилок стандартні багаточлени мають вигляд:

$$P(x) = x^8 + x^2 + x + 1 \Rightarrow (d = 4) \text{ при довжині кодової комбінації } n \le 2^7;$$

$$P(x) = x^{16} + x^{15} + x^{13} + x^{11} + x^5 + x^3 + x + 1 \Rightarrow (d = 6) \text{ при } n \le 2^7;$$

$$P(x) = x^{16} + x^{12} + x^5 + 1 \Rightarrow (d = 4) \text{ при } n \le 2^{15}.$$

Розроблений ряд методик по вибору породжуючого багаточлену $P(x)$. В літературі коди називають по прізвищам вчених, що запропонували ту або іншу методику. Так отримали свою назву коди **Боуза-Чоудхурі-Хоквінгема** (БЧХ), коди **Ріда-Соломона**, коди **Файра** та інші.

Укорочені циклічні коди

Циклічні коди припускають рівність розрядності кодової комбінації, що формується, довжині циклу утворюючого багаточлена, т. т. $n = \ell_ц$. Однак ця вимога на практиці важко здійснюється, оскільки розрядність комбінацій, що видаються джерелом інформації, нерідко відрізняється від доцільної, в результаті чого $n < \ell_ц$. В цих випадках циклічний код перетворюють і використають так званий **скорочений циклічний код**, що одержується з циклічного шляхом винятку в ньому певного числа розрядів.

При цьому число стовпчиків перевірочної матриці $H(n,m)$ зменшується на величину, яка дорівнює числу інформаційних розрядів, що виключаються, причому виключаються стовпчики з найвищими номерами. Властивості коду по виявленню помилок при цьому не змінюються.

Коди Боуза-Чоудхурі-Хоквінгема

Коди Боуза-Чоудхурі-Хоквінгема (БЧХ) відносяться до класу циклічних і призначені для виправлення t_u-кратних помилок в n-розрядної кодової комбінації. Породжуючий багаточлен $P(x)$ визначається вираженням:

$$P(x) = \text{нзк}\{f_1(x), f_2(x), \ldots, f_{2t_u}(x)\},$$

де нзк – найменше загальне кратне; $f_i(x)$ – мінімальні багаточлени коренів $P(x)$ При цьому $f_1(x)$ мінімальний багаточлен кореня α з довжиною циклу $\ell_ц = n$;

$f_2(x)$ – мінімальний багаточлен кореня α^2; $f_i(x)$ – мінімальний багаточлен кореня α^i(гляди додаток 1).

Оскільки α^i (при парному i) є коренем того же багаточлена, коренем якого є α, то вираження для породжуючого багаточлена буде мати вигляд:

$$P(x) = \prod_{i=1,3,5}^{2t_u-1} f_i(x).$$

Багаточлен $f_1(x)$ визначається за формулою:

$$f_1(x) = (x - \alpha) \prod_{j=1,2,4}^{\nu} (x - \alpha^{2j}),$$

де ν визначається з умови $2(\nu+2) - \ell_ц = 1$.

Наприклад, для $f_1(x) = x^3 + x + 1$ елемент $\alpha = 010$ є його коренем. Елементи α^2, α^4 також будуть його коренями. Елемент α^8 буде рівний α^1, так як довжина циклу багаточлена $f_1(x)$ рівна 7. Отже,

$$f_1(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^4).$$

Розкривши дужки, отримаємо:

$$f_1(x) = x^3 + x + 1.$$

Багаточлен $f_3(x)$ визначається по вираженню:

$$f_3(x) = (x - \alpha^3) \prod_{j=1,2,4}^{\nu} (x - \alpha^{3\cdot 2j}),$$

де ν визначається з умови $2(\nu+2) - j\ell_ц = 3;\ j = 1,2,3$ і т. д.

Приклад: Визначити породжуючий багаточлен для коду БЧХ, що виправляє помилки кратності до двох включно. Довжина кодової комбінації $n = 15$.

Виберемо неприводимий над полем $GF(2)$ багаточлен $f_1(x) = x^4 + x + 1$, довжина циклу якого рівна $\ell_ц = 15$. Його корені є елементи поля $GF(2^4)$. Примітивний корінь – α. Елементи α^2, α^4 також є корні багаточлену $f_1(x)$. Так як повинні бути виправлені дворазові помилки, то породжуючий багаточлен рівний:

$$P(x) = f_1(x)\, f_3(x).$$

Елемент α^3 є коренем багаточлена $f_3(x)$. Коренями цього багаточлена є також елементи $\alpha^6, \alpha^{12}, \alpha^{24} = \alpha^9$.

Отже:

$$f_2(x) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^9)(x - \alpha^{12}).$$

Враховуючи, що $\alpha^4 + \alpha + 1 = 0$ і $\alpha^{15} = 1$ розкривши дужки, отримаємо:

$$f_2(x) = x^4 + x^3 + x^2 + x + 1.$$

Тоді породжуючий багаточлен буде рівний:

$$P(x) = f_1(x)\, f_2(x) = x^8 + x^7 + x^5 + x^4 + 1.$$

В результаті коренями багаточлена $P(x)$ є:

$$\alpha, \alpha^2, \alpha^4, (\alpha)^3, (\alpha^2)^4, (\alpha^4)^3, (\alpha^5)^3.$$

Якщо необхідно виправити не двократні помилки, а помилки кратності до t_u включно, то корні необхідно зводити в ступінь до $2\,t_u$ - 1.

Для загального випадку існує така теорема. Якщо α – примітивний елемент поля $GF(2^k)$, то код, породжений багаточленом $P(x)$, є БЧХ – кодом тоді і тільки тоді, коли елементи: $\alpha, \alpha^3, \alpha^5, \ldots, \alpha^{2t_u-1}$ є коренями цього багаточлена.

Ґрунтуючись на цій теоремі, можна запропонувати наступну методику вибору багаточлена $P(x)$ для коду БЧХ.

Задана довжина кодової комбінації $n = 2^z - 1$.

1. Двочлен $2^{2^{Z-1}} + 1$ завжди розкладається на неприводимі багаточлени у полі $GF(2)$.

2. З отриманих співмножників вибирають багаточлен $f_1(x)$ ступеня Z і довжиною циклу $\ell_{ö} = n$. Шляхом ділення $x^i (i = 1, \ldots, n-1)$ на цей багаточлен знаходять всі корені двочлену $x^{2^z - 1} + 1$.

3. Визначають приналежність коренів до отриманих при розкладі на множники багаточленам.

4. Корні багаточлену $f_1(x)$ зводять в непарні ступені від **1** до $2\,t_u - 1$, в результаті одержують набір корнів, що повинен мати утворюючий багаточлен $P(x)$.

5. Виявляють багаточлени, яким належать отримані корні.

6. Вибрані багаточлени перемножують і одержують вираз для $P(x)$.

Приклад: Визначимо $P(x)$ для коду БЧХ при $n = 15 = 2^4 - 1$ і $t_u = 3$.

1. Розкладемо на множники двочлен:

$$x^{2^4 - 1} + 1 = f_1(x)\, f_2(x)\, f_3(x)\, f_4(x)\, f_5(x) =$$

$$= (x+1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1) \cdot (x^4 + x^3 + x^2 + x + 1).$$

2. З співмножників вибираємо неприводимий багаточлен $f_3(x) = x^4 + x + 1$ і шляхом ділення $x^i (i = 1, 2, \ldots, 14)$ на $f_3(x)$ визначаємо всі корені двочлену $x^{2^4 - 1} + 1$.

3. Визначаємо приналежність коренів до співмножників.

Корні $\alpha^1, \alpha^2, \alpha^4, \alpha^8$ належать до $f_3(x)$.

4. Зводимо корені багаточлена $f_3(x)$ в ступені від **1** до $2 \cdot 3 - 1 = 5$.

Так як $\alpha^1, \alpha^2, \alpha^4, \alpha^8$ є коренями багаточлена: $f_3(x) = x^4 + x + 1$; $\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$ є коренями багаточлена: $f_5(x) = x^4 + x^3 + x^2 + x + 1$; α^5, α^{10} є коренями багаточлена: $f_2(x) = x^2 + x + 1$, то:

$$P(x) = f_2(x)\, f_3(x)\, f_5(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1.$$

Коди Ріда-Соломона

Коди **Ріда-Соломона** є недвійковим підкласом кодів БЧХ. Вони визначені над полем $GF(q) = GF(2^k)$. Довжина кодової комбінації рівна: $n = q - 1$. Породжуючий багаточлен визначається за формулою:

$$P(x) = (x - \alpha)(x - \alpha^2)\ldots(x - \alpha^{2t_u}),$$

де α – примітивний елемент поля $GF(q)$.

В результаті одержується код з $d - 1$ перевірочними символами.

Приклад: Виберемо $P(x)$ для коду **Ріда-Соломона** з $n = 7$, що виправляє дворазові і однократні помилки. Нехай поле $GF(8)$ задане табл. П.1. Тоді:

$$P(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^3)(x - \alpha^4) = x^4 + \alpha^3 x^3 + x^2 + \alpha x + \alpha^3.$$

Слідує відзначити, що коефіцієнти багаточлена є елементами з поля $GF(8)$.

Приклад: Виберемо $P(x)$ для коду **Ріда-Соломона** з $n = 15$ і $t_u = 2$. Поле $GF(16)$ задане табл. П.3. Тоді:

$$P(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^3)(x - \alpha^4) = x^4 + \alpha^{13} x^3 + \alpha^6 x^2 + \alpha^3 x + \alpha^{10}.$$

Таким чином, в коді **Ріда-Соломона** коефіцієнти при змінних не є двійковими числами, як це було в коді БЧХ, що дозволяє здійснити кодування недвійкової інформації.

Код Файра

Код Файра – це циклічний код, що забезпечує виправлення пакетів помилок тривалістю b та менш розрядів. Породжуючий багаточлен даного коду визначається за формулою:

$$P(x) = (x^{2b-1} + 1)\, P_1(x),$$

де $P_1(x)$ – примітивний багаточлен над полем $GF(q)$, ступінь якого не менше довжини пакету помилок b, що виправляється, і який не ділить двочлен $x^{2b-1} + 1$ без залишку.

Довжина кодової комбінації приймається рівної $n = \ell_ц(2b - 1)$, де $\ell_ц$ – довжина циклу багаточлена $P_1(x)$. Наприклад, $P(x) = x^4 + x + 1$ багаточлен, що не приводиться, в полі $GF(2)$, довжина циклу цього багаточлену $\ell_ц = 15$. Нехай $b = 4$. Очевидно, що $2b - 1 = 7$ не ділиться на 13. Тоді утворюючий багаточлен буде мати вигляд:

$$P(x) = (x^4 + x + 1)(x^7 + 1) = x^{11} + x^8 + x^7 + x^4 + x + 1.$$

Перемноження $P_1(x)$ на двочлен $x^{2b-1} + 1$ являє собою введення додаткової перевірки кодової комбінації на парність, що дасть в деякому роді зображення пакету помилок. Який-небудь пакет помилок тривалістю b та менш символів буде залишати по меншій мірі $b-1$ перевірок не заторкнутими, і тому можна визначити, який символ стоїть в початку пакету. Положення пакету помилок в кодовій комбінації визначається за рахунок багаточлена $P_1(x)$

.

Розділ 5. Операційні системи

5.1 Архітектура операційних систем.
5.2. Процеси і потоки в операційних системах.
5.3. Керування пам’яттю в операційних системах.
5.4. Файлові системи.
5.5. Захисні механізми операційних систем (Unix, Windows Server 2022, Windows 10/11)

5.1. Архітектура операційних систем

Операційна система, скор. **ОС** (англ. *operating system, OS*) – комплекс взаємозалежних програм, призначених для управління ресурсами комп'ютера та організації взаємодії з користувачем.

У логічній структурі типової обчислювальної системи операційна система займає становище між пристроями з їхньою мікроархітектурою, машинною мовою і, можливо, власними (вбудованими) мікропрограмами (драйверами) – з одного боку – і прикладними програмами з іншого.

Розробникам програмного забезпечення операційна система дозволяє абстрагуватися від деталей реалізації та функціонування пристроїв, надаючи мінімально необхідний набір функцій (див. інтерфейс програмування додатків).

У більшості обчислювальних систем операційна система є основною, найбільш важливою (іноді й єдиною) частиною системного програмного забезпечення. З 1990-х років найбільш поширеними операційними системами є системи сімейства Windows, Unix і UNIX-подібні системи.

Функції

Основні функції:

– Виконання запитів програм (введення та виведення даних, запуск та зупинення інших програм, виділення та звільнення додаткової пам'яті та ін.).

– Завантаження програм на оперативну пам'ять та його виконання.

– Стандартизований доступ до периферійних пристроїв (пристрою введення-виведення).

– Управління оперативною пам'яттю (розподіл між процесами, організація віртуальної пам'яті).

– Керування доступом до даних на енергонезалежних носіях (таких як жорсткий диск, оптичні диски та ін), організованим у тій чи іншій файловій системі.

– Забезпечення інтерфейсу користувача.

– Збереження інформації про помилки системи.

Додаткові функції:

– Паралельне чи псевдопаралельне виконання завдань (багатозадачність).

– Ефективний розподіл ресурсів обчислювальної системи між процесами.

– Розмежування доступу різних процесів до ресурсів.

– Організація надійних обчислень (неможливість одного обчислювального процесу навмисно або помилково вплинути на обчислення в іншому процесі), заснована на розмежуванні доступу до ресурсів.

– Взаємодія між процесами: обмін даними, взаємна синхронізація.

– Захист самої системи, а також даних користувача та програм від дій користувачів (зловмисних або через незнання) або додатків.

– Розрахований на багато користувачів режим роботи і розмежування прав доступу (автентифікація, авторизація).

Поняття

Існують дві групи визначень операційної системи: «набір програм, керуючих обладнанням» та «набір програм, керуючих іншими програмами». Обидві вони мають свій точний технічний зміст, який пов'язаний із питанням, у яких випадках потрібна операційна система.

Є програми обчислювальної техніки, котрим операційні системи зайві. Наприклад, вбудовані мікрокомп'ютери, що містяться в багатьох побутових приладах, автомобілях (іноді по десятку в кожному), найпростіших стільникових телефонах, постійно виконують лише одну програму, що запускається після вмикання. Багато простих ігрових приставок – також спеціалізованих мікрокомп'ютерів – можуть обходитися без операційної системи, запускаючи при включенні програму, записану на вставленому в пристрій «картриджі» або компакт-диску.

Операційні системи потрібні:

– якщо потрібний універсальний механізм збереження даних;

– для надання програм системних бібліотек з підпрограмами, що часто використовуються;

– для розподілу повноважень;

– потрібна можливість імітації «одночасного» виконання кількох програм на одному комп'ютері;

– для керування процесами виконання окремих програм.

Таким чином, сучасні універсальні операційні системи можна охарактеризувати насамперед як:

– що використовують файлові системи (з універсальним механізмом доступу до даних),

– розраховані на багато користувачів (з поділом повноважень),

– багатозадачні (з розподілом часу).

Багатозадачність і розподіл повноважень вимагають певної ієрархії привілеїв компонентів у операційній системі. У складі операційної системи розрізняють три групи компонентів:

– ядро, що містить планувальник; драйвери пристроїв, які безпосередньо керують обладнанням; мережна підсистема; файлова система;

– системні бібліотеки;

– оболонка з утилітами.

Більшість програм, як системних (що входять до операційної системи), так і прикладних, виконуються в непривілейованому («користувальницькому»)

режимі роботи процесора і отримують доступ до обладнання (і, за необхідності, до інших ресурсів ядра, а також ресурсів інших програм) тільки за допомогою системних викликів. Ядро виконується у привілейованому режимі: саме в цьому сенсі кажуть, що система (точніше, її ядро) управляє обладнанням.

У визначенні складу операційної системи значення має критерій операційної цілісності (замкнутості): система має дозволяти повноцінно використовувати (включаючи модифікацію) свої компоненти. Тому до повного складу операційної системи включають і набір інструментальних засобів (від текстових редакторів до компіляторів, налагоджувачів та компонувальників).

Ядро

Ядро – центральна частина операційної системи, що управляє виконанням процесів, ресурсами обчислювальної системи та надає процесам координований доступ до цих ресурсів. Основними ресурсами є процесорний час, пам'ять та пристрої введення-виведення. Доступ до файлової системи та мережна взаємодія також можуть бути реалізовані лише на рівні ядра.

Як основний елемент операційної системи, ядро є найнижчим рівень абстракції для доступу додатків до ресурсів обчислювальної системи, необхідним для їх роботи. Як правило, ядро надає такий доступ виконуваним процесам відповідних додатків за рахунок використання механізмів міжпроцесної взаємодії та звернення до системних викликів ОС.

Описана завдання може відрізнятися залежно від типу архітектури ядра та її реалізації.

Об'єкти ядра ОС:

– процеси,
– файли,
– події,
– потоки,
– семафори,
– м'ютекси,
– канали,
– файли, що проецуються до пам’яті.

Типи архітектур ядер операційних систем

Монолітне ядро

Монолітне ядро надає багатий набір обладнання абстракції. Всі частини монолітного ядра працюють в одному адресному просторі. Це така схема операційної системи, коли всі компоненти її ядра є складовими частинами однієї програми, використовують загальні структури даних і взаємодіють друг з одним шляхом безпосереднього виклику процедур. Монолітне ядро – найстаріший спосіб організації операційних систем. Прикладом систем із монолітним ядром є більшість UNIX-систем.

– Переваги: Швидкість роботи, спрощена розробка модулів.

– Недоліки: Оскільки ядро працює в одному адресному просторі, збій в одному з компонентів може порушити працездатність усієї системи.

Приклади: Традиційні ядра UNIX (такі як BSD), Linux; ядро MS-DOS, ядро KolibriOS.

Деякі старі монолітні ядра, особливо систем класу UNIX / Linux, вимагали перекомпіляції за будь-якої зміни складу обладнання. Більшість сучасних ядер дозволяє під час роботи підвантажувати *модулі*, що виконують частину функцій ядра. У цьому випадку компоненти операційної системи є не самостійними модулями, а складовими частинами однієї великої програми, яка називається монолітним ядром (monolithic kernel), яке є набором процедур, кожна з яких може викликати кожну. Усі процедури працюють у привілейованому режимі.

Модульне ядро

Модульне ядро – сучасна, вдосконалена модифікація архітектури монолітних ядер операційних систем.

На відміну від «класичних» монолітних ядер, модульні ядра зазвичай не вимагають повної перекомпіляції ядра при зміні складу апаратного забезпечення комп'ютера. Натомість модульні ядра надають той чи інший механізм підвантаження модулів ядра, що підтримують те чи інше апаратне забезпечення (наприклад, драйверів). При цьому підвантаження модулів може бути як динамічною (виконуваної «на льоту», без перезавантаження ОС, у працюючій системі), так і статичної (виконується при перезавантаженні ОС після переконфігурування системи на завантаження тих чи інших модулів).

Приклади: OpenVMS;

Мікроядро

Мікроядро надає лише елементарні функції управління процесами та мінімальний набір абстракцій для роботи з обладнанням. Більша частина роботи здійснюється за допомогою спеціальних процесів користувача, званих *серверами*. Вирішальним критерієм «мікроядерності» є розміщення всіх або багатьох драйверів і модулів у сервісних процесах, іноді з явною неможливістю завантаження будь-яких модулів розширення у власне мікроядро, а також розробки таких розширень.

– Переваги: Стійкість до збоїв обладнання, помилок у компонентах системи. Основна перевага мікроядерної архітектури – високий рівень модульності ядра операційної системи. Це значно спрощує додавання до нього нових компонентів. У мікроядерній операційній системі можна, не перериваючи її роботи, завантажувати і вивантажувати нові драйвери, файлові системи і т.д. Компоненти ядра операційної системи нічим принципово не відрізняються від програм користувача, тому для їх налагодження можна застосовувати звичайні засоби. Мікроядерна архітектура підвищує надійність системи, оскільки помилка лише на рівні непривілейованої програми менш небезпечна, ніж відмова лише на рівні режиму ядра.

– Недоліки: Передача даних між процесами потребує накладних витрат.

Класичні мікроядра надають лише дуже невеликий набір низькорівневих примітивів, або системних викликів, що реалізують базові послуги операційної системи.

Сервісні процеси (в прийнятій у сімействі UNIX термінології – «демони ») активно використовуються в різних ОС для завдань типу запуску програм з

розкладу (UNIX і Windows NT), ведення журналів подій (UNIX і Windows NT), централізованої перевірки паролів і зберігання пароля поточного інтерактивного користувача у спеціально обмеженій області пам'яті (Windows NT). Тим не менш, не слід вважати ОС мікроядерними лише через використання такої архітектури.

Приклади: Symbian OS; Windows CE; Mach, що використовується в GNU/Hurd та Mac OS X; QNX; AIX; Minix; ChorusOS; AmigaOS; MorphOS.

Екзоядро

Екзоядро – ядро операційної системи, що надає лише функції для взаємодії між процесами, безпечного виділення та звільнення ресурсів. Передбачається, що API для прикладних програм надаватимуться зовнішніми по відношенню до ядра бібліотеками (звідки і назва архітектури).

Можливість доступу до пристроїв на рівні контролерів дозволить ефективніше вирішувати деякі завдання, які погано вписуються в рамки універсальної ОС, наприклад, реалізація СУБД матиме доступ до диска на рівні секторів диска, а не файлів та кластерів, що позитивно позначиться на швидкодії.

Наноядро

Наноядро – архітектура ядра операційної системи, в рамках якої вкрай спрощене та мінімалістичне ядро виконує лише одне завдання – обробку апаратних переривань, що генеруються пристроями комп'ютера. Після обробки переривань від апаратури наноядро посилає інформацію про результати обробки (наприклад, отримані з клавіатури символи) вищележачому програмному забезпеченню за допомогою того ж механізму переривань. Прикладом є KeyKOS – найперша ОС на наноядрі. Перша версія вийшла ще 1983 року.

Гібридне ядро

Гібридні ядра – це модифіковані мікроядра, що дозволяють прискорити роботу запускати «несуттєві» частини у просторі ядра. Приклад: ядра ОС Windows сімейства NT.

Комбінація різних підходів

Усі розглянуті підходи до побудови операційних систем мають свої переваги та недоліки. Найчастіше сучасні операційні системи використовують різні комбінації цих підходів. Так, наприклад, зараз ядро Linux є монолітною системою з окремими елементами модульного ядра. При компіляції ядра можна дозволити динамічне завантаження і вивантаження багатьох компонентів ядра – про модулів. У момент завантаження модуля його код завантажується лише на рівні системи та зв'язується з іншою частиною ядра. Всередині модуля можуть використовуватися будь-які функції, що експортуються ядром.

Існують варіанти ОС GNU, в яких замість монолітного ядра застосовується ядро Mach (таке ж, як у Hurd), а поверх нього працюють в просторі користувача ті ж самі процеси, які при використанні Linux були б частиною ядра. Іншим прикладом змішаного підходу може бути можливість запуску операційної системи з монолітним ядром під керуванням мікроядра. Так влаштовані 4.4 BSD і MkLinux, засновані на мікроядрі Mach. Мікроядро забезпечує управління віртуальною пам'яттю та роботу низькорівневих драйверів. Всі інші функції, зокрема взаємодія з прикладними програмами, здійснюються монолітним ядром.

Даний підхід сформувався в результаті спроб використовувати переваги мікроядерної архітектури, зберігаючи наскільки можна добре налагоджений код монолітного ядра.

Змішане ядро, в принципі, поєднує переваги монолітного ядра і мікроядра: здавалося б, мікроядро і монолітне ядро – крайності, а змішане – золота середина. У них можна додавати драйвера пристроїв двома методами: і всередину ядра, і в простір. Але практично концепція змішаного ядра часто підкреслює як переваги, а й недоліки обох типів ядер.

Приклади: Windows NT, DragonFly BSD.

5.2. Процеси і потоки в операційних системах

Процес є ідентифікованою абстракцією сукупності взаємопов'язаних системних ресурсів на основі окремого та незалежного віртуального адресного простору в контексті якої організується виконання потоків. Стандарт ISO 9000:2000 Definitions визначає процес як сукупність взаємопов'язаних та взаємодіючих дій, що перетворюють вхідні дані у вихідні.

Комп'ютерна програма як така – лише пасивна послідовність інструкцій. У той час як процес – безпосереднє виконання цих інструкцій.

Також, процесом називають програму, що виконується, і всі її елементи: адресний простір, глобальні змінні, регістри, стек, відкриті файли і так далі.

Представлення процесу

Зазвичай процес у обчислювальній системі представлений (також кажуть, «володіє») такими ресурсами:

- чином виконуваного машинного коду, асоційованого з програмою;
- пам'яттю (зазвичай деякою областю віртуальної пам'яті), яка включає:
  - виконуваний код;
  - вхідні та вихідні дані процесу;
  - стек викликів (для відстеження активних підпрограм);
  - купу для зберігання проміжних результатів обчислень, що генеруються під час виконання;
- дескрипторами ресурсів операційної системи, виділеними для процесу, наприклад, файл;
- файловими дескрипторами (в термінології ОС Unix) або «хендлами» (в термінології ОС Windows);
- атрибутами безпеки, такими як власник та набір повноважень процесу (допустимих операцій);
- станом процесора (контекстом), таким як:
  - вміст регістрів;
  - схема перетворення віртуальних адрес у фізичні;
  - і т.д.

Контекст поточного процесу вивантажується в пам'ять, коли перемикається на інший процес.

Операційна система зберігає більшу частину інформації про процеси в таблиці процесів.

У операційних системах, підтримують потоки виконання (нитки), потоки також мають власні ресурси. Зазвичай це лише стан процесора, хоча потоки можуть використовувати інші ресурси.

Для зниження ймовірності впливу процесів один на одного та ймовірності відмови системи (наприклад, взаємних блокувань або пробуксування) операційна система забезпечує ізоляцію процесів та виділяє необхідні їм ресурси. Також операційна система надає механізми для взаємодії процесів безпечними та передбачуваними способами.

Подання процесу у пам'яті

У цьому розділі розглянуто уявлення процесу в пам'яті операційної системи Linux та архітектури x86. Подібне уявлення мало відрізняється від багатьох інших багатозадачних операційних систем та архітектур. Наприклад в amd64, спадкоємці x86, стек викликів так само зростає зверху вниз, але розмір адресного простору збільшений до 2^{48} байт.

Linux використовує плоску модель пам'яті, і тому в даній архітектурі кожному процесу доступно 2^{32} байт пам'яті. Вся віртуальна пам'ять ділиться на простір користувача та простір ядра. Простір ядра займає один гігабайт пам'яті, починаючи з найстаршої адреси. Все інше простір, тобто три гігабайти відведено під простір користувача.

На схемі праворуч показано уявлення простору користувача будь-якого процесу. Простір ядра єдине всім процесів, оскільки у операційній системі може існувати лише один екземпляр ядра. Після запуску програми в оперативну пам'ять імпортуються команди процесора (машинний код) та ініціалізовані дані. Водночас у старші адреси імпортуються аргументи запуску та змінні оточення.

В області ініціалізованих даних зберігаються дані, доступні лише читання. Це може бути, наприклад, рядкові літерали.

У сфері неініціалізованих даних, як правило, зберігаються глобальні змінні.

Купа (heap) використовується виділення пам'яті під час роботи програми. У Linux для цього існує системний виклик mmap.

Область стека використовується для виклику процедур.

Також важливою деталлю є наявність випадкового відступу між стеком і верхньою областю, а також між областю ініціалізованих даних та купою. Робиться це з метою безпеки, наприклад, для запобігання вбудовуванню в стек інших функцій.

Бібліотеки, що динамічно підключаються, і відображення файлів розташовуються між стеком і купою.

Ієрархія процесів

У багатозадачних операційних системах з'явилася можливість працювати одночасно з кількома процесами. Операційні системи з витісняючою багатозадачністю дозволяли домогтися відчуття роботи кількох процесів одночасно. При цьому були потрібні засоби управління декількома процесами.

Unix

Unix – одна з перших багатозадачних ОС. Кожен процес має унікальний числовий ідентифікатор PID. Процеси в ній мають деревоподібну ієрархію, де коренем є процес init с PID 1. Новий процес можна створити системним викликом fork, він буде точною копією процесу батька. Будь-який процес крім init завжди має процес батька (атрибут PPID (англ. *Parent PID*)); процеси, батько яких завершив свою роботу, стають дочірніми процесами init.

Процеси також об'єднуються у **групи**. За керування ідентифікатором групи (PGID) відповідають системні виклики setpgidta getpgid. PGID дорівнює PID'у лідера групи. Процес нащадок успадковує групу батьків. Групи використовуються для керування завданнями.

Групи процесів об'єднуються у **сесії**. За створення нової сесії відповідає системний виклик setsid. Процеси з однієї групи не можуть належати різним сесіям. Тому лідер групи не може стати лідером сесії: під час створення сесії дочірній процес автоматично стає лідером сесії та лідером нової групи. Сесії використовують для відстеження всіх процесів, запущених після входу користувача.

Кожна сесія може мати не більше одного **керуючого терміналу**. Емулятор терміналу має дочірнім процесом оболонку команд (найчастіше bash або sh), яка перед запуском стає лідером нової сесії та встановлює собі керуючим термінал.

Створення процесу

Найпростішою операційній системі не потрібно створення нових процесів, оскільки в них працює одна-єдина програма, що запускається під час включення пристрою. У складніших системах треба створювати нові процеси. Зазвичай вони створюються:

– При запуску ОС (наприклад, коли відбувається ініціалізація драйверів пристроїв).

– З появою запиту створення процесу – відбувається у разі, коли працюючий процес виконує системний виклик.

Стан процесу

Процес, крім головного робочого стану, може бути в інших станах, наприклад очікування.

Linux

Процес в ОС Linux може бути в одному з наступних станів:

– **R –** *(running/runnable)* – процес виконується або чекає своєї черги виконуватися;

– **D** – безперервний сон – процес очікує певної події;

– **S** – сон, що переривається – процес очікує певної події або сигналу;

– **T** – зупинка – процес припинений, наприклад, відладчиком;

– **Z –** *(zombie)* – процес вже завершився, але ще не передав батьківському процесу свій код повернення.

Завершення процесу

Мінімум 2 етапи завершення:

1. Процес видаляється з усіх черг планування, тобто ОС більше не планує виділення будь-яких ресурсів процесу,

2. Збір статистики про спожиті процесом ресурси з подальшим видаленням його з пам'яті.

Причини завершення процесу:

– Звичайний вихід.
– Вихід за винятком чи помилкою.
– Недостатній обсяг пам'яті.
– Перевищення ліміту відведеного програмі часу.
– Вихід за межі відведеної області пам'яті
– Неправильна команда (дані програми інтерпретуються як інструкції для процесора).
– Помилка захисту (виконання непривілейованої команди).
– Завершення батьківського процесу.
– Помилка введення- виведення.
– Втручання оператора.

Потік виконання

Потік виконання (тред; від англ. *thread* – нитка) – Найменша одиниця обробки, виконання якої може бути призначене ядром операційної системи. Реалізація потоків виконання та процесів у різних операційних системах відрізняється один від одного, але в більшості випадків потік виконання знаходиться всередині процесу. Декілька потоків виконання можуть існувати в рамках того самого процесу і спільно використовувати ресурси, такі як пам'ять, тоді як процеси не поділяють цих ресурсів. Зокрема, потоки виконання поділяють послідовність інструкцій процесу (його код) та його *контекст* – значення змінних (регістрів процесора і стека викликів), які вони мають у будь-який момент часу.

Як аналогію потоки виконання процесу можна уподібнити кільком разом працюючим кухарям. Всі вони готують одну страву, читають ту саму кулінарну книгу з одним і тим самим рецептом і дотримуються його вказівок, причому не обов'язково всі вони читають на одній і тій же сторінці.

На одному процесорі *багатопотоковість* зазвичай відбувається шляхом тимчасового мультиплексування (як і у разі багатозадачності): процесор перемикається між різними потоками виконання. Це перемикання контексту зазвичай відбувається досить часто, щоб користувач сприймав виконання потоків чи завдань як одночасне. У багатопроцесорних і багатоядерних системах потоки чи завдання можуть реально виконуватися одночасно, у своїй кожен процесор чи ядро обробляє окремий потік чи завдання.

Багато сучасних операційних систем підтримують як тимчасові нарізки від планувальника процесів, і багатопроцесорні потоки виконання. Ядро операційної системи дозволяє програмістам управляти потоками виконання через інтерфейс системних викликів. Деякі реалізації ядра називають *потоком*

ядра, інші ж – *легковажним процесом* (англ. *light-weight process*, LWP), що є особливим типом потоку виконання ядра, який спільно використовує одні й ті ж стани і дані.

Програми можуть мати *користувальницький простір потоків виконання* при створенні потоків за допомогою таймерів, сигналів або іншими методами, що дозволяють перервати виконання та створити тимчасове нарізування для конкретної ситуації (Ad hoc).

Відміна від процесів

Потоки виконання відрізняються від традиційних процесів багатозадачної операційної системи тим, що:

– процеси, як правило, незалежні, тоді як потоки виконання існують як складові елементи процесів;

– процеси несуть значно більше інформації про стан, тоді як кілька потоків виконання всередині процесу спільно використовують інформацію про стан, а також пам'ять та інші обчислювальні ресурси;

– процеси мають окремі адресні простори, тоді як потоки виконання спільно використовують їх адресний простір;

– процеси взаємодіють лише через надані системою механізми зв'язків між процесами;

– перемикання контексту між потоками виконання в одному процесі, як правило, швидше, ніж перемикання контексту між процесами.

Такі системи, як Windows NT і OS/2, як кажуть, мають «дешеві» потоки виконання та «дорогі» процеси. В інших операційних системах різниця між потоками виконання і процесами не така велика, за винятком витрат на перемикання адресного простору, що передбачає використання буфера асоціативної трансляції.

Багатопотоковість

Багатопотоковість, як широко поширена модель програмування та виконання коду, дозволяє кільком потокам виконуватися в рамках одного процесу. Ці потоки виконання спільно використовують ресурси процесу, але можуть працювати самостійно. Багатопотокова модель програмування надає розробникам зручну абстракцію паралельного виконання. Однак, мабуть, найцікавіше застосування технології є в тому випадку, коли вона застосовується до одного *процесу*, що дозволяє його *паралельне виконання багатопроцесорної* системи.

Ця перевага багатопотокової програми дозволяє їй працювати швидше на комп'ютерних системах, які мають кілька процесорів, процесор з кількома ядрами або на кластері машин – через те, що потоки виконання програм природно піддаються дійсно паралельному виконанню процесів. У цьому випадку програмісту потрібно бути дуже обережним, щоб уникнути стану гонки та іншої неінтуїтивної поведінки. Для того, щоб правильно маніпулювати даними, потоки виконання повинні часто проходити через рандеву процедуру, щоб обробляти дані в правильному порядку. Потокам виконання можуть також

знадобитися м'ютекси (які часто реалізуються з використанням семафорів), щоб запобігти одночасній зміні загальних даних або їх читання під час процесу зміни. Необережне використання таких примітивів може призвести до тупикової ситуації.

Іншим використанням багатопотоковості, що застосовується навіть для однопроцесорних систем, є можливість застосування реагування на введення даних. В однопотокових програмах, якщо основний потік виконання заблокований виконанням тривалого завдання, вся програма може опинитися в замороженому стані. Переміщаючи такі тривалі завдання до *робочого потоку*, який виконується паралельно з основним потоком, стає можливим для додатків продовжувати реагувати на дії користувача під час виконання завдань у фоновому режимі. З іншого боку, в більшості випадків багатопотоковість – не єдиний спосіб зберегти чутливість програми. Те саме може бути досягнуто через асинхронне введення-виведення або сигнали в UNIX.

Операційні системи планують виконання потоків одним із двох способів:

1. *Пріоритетна багатопотоковість*, взагалі кажучи, вважається більш досконалим підходом, оскільки вона дозволяє операційній системі визначити, коли має відбуватися перемикання контексту. Недолік пріоритетної багатопотоковості полягає в тому, що система може зробити перемикання контексту в невідповідний час, що призводить до інверсії пріоритету та інших негативних ефектів, яких можна уникнути, застосовуючи кооперативну багатопотоковість.

2. *Кооперативна багатопотоковість* покладається самі потоки і цурається управління, якщо потоки виконання перебувають у точках зупинки. Це може створити проблеми, якщо потік виконання очікує на ресурс, поки він не стане доступним.

До кінця 1990-х процесори в настільних комп'ютерах не мали підтримки багатопотоковості, оскільки перемикання між потоками, як правило, відбувалося повільніше, ніж повне перемикання контексту процесу. Процесори у вбудовуваних системах, які мають більш високі вимоги до поведінки в реальному часі, можуть підтримувати багатопотоковість за рахунок зменшення часу на перемикання між потоками, можливо, шляхом розподілу виділених реєстрових файлів для кожного потоку виконання замість збереження/відновлення загального регістрового файлу. Наприкінці 1990-х ідея виконання інструкцій кількох потоків одночасно, відома як одночасна багатопотоковість, під назвою Hyper-Threading, досягла настільних комп'ютерів із процесором Intel Pentium 4. Потім вона була виключена з процесорів архітектури Intel Core та Core 2, але пізніше відновлена в архітектурі Core i7.

Критики багатопотоковості стверджують, що збільшення використання потоків має суттєві недоліки:

Хоча здається, що потоки виконання – це невеликий крок від послідовних обчислень, за суттю вони є величезним стрибком. Вони відмовляються від найбільш важливих та привабливих властивостей послідовних обчислень: зрозумілості, передбачуваності та детермінізму. Потоки виконання, як модель

обчислень, є недетермінованими, і зменшення цього недетермінізму стає завданням програміста.

Процеси, потоки виконання ядра, користувальницькі потоки та файбери

Процес є «найважчою» одиницею планування ядра. Власні ресурси для процесу виділяються операційною системою. Ресурси включають пам'ять, дескриптори файлів, роз'єми, дескриптори пристроїв та вікна. Процеси використовують адресний простір і файли ресурсів в режимі розподілу часу тільки через явні методи, такі як успадкування дескрипторів файлів і сегментів пам'яті, що розділяється. Процеси, як правило, попередньо перетворені на багатозадачний спосіб виконання.

Потоки виконання ядра належать до «легких» одиниць планування ядра. Усередині кожного процесу існує принаймні один потік виконання ядра. Якщо у процесі можуть існувати кілька потоків виконання ядра, всі вони спільно використовують загальну пам'ять і файл ресурсів. Якщо процес виконання планувальника операційної системи є пріоритетним, то потоки виконання ядра теж пріоритетно багатозадачними. Потоки виконання ядра немає власних ресурсів, крім стека викликів, копії регістрів процесора, включаючи лічильник команді локальну пам'ять потоку виконання (якщо вона є). Ядро може призначити по одному потоку виконання для кожного логічного ядра системи (оскільки кожен процесор поділяє сам себе на кілька логічних ядер, якщо він підтримує багатопотоковість, або підтримує лише одне логічне ядро на кожне фізичне ядро, якщо не підтримує багатопотоковість), а може виконувати свопінг заблокованих потоків виконання. Однак потоки виконання ядра вимагають набагато більше часу, ніж потрібно на свопінг потоків користувача виконання.

Потоки виконання іноді реалізуються в користувальницькому просторі бібліотек, в цьому випадку вони називаються *користувальницькими потоками виконання*. Ядро не знає про них, так що вони управляються і плануються в просторі користувача. У деяких реалізаціях *користувальницькі потоки виконання* ґрунтуються на кількох верхніх *потоках виконання ядра*, щоб використовувати переваги багатопроцесорних машин (моделі M: N). Під терміном «потік виконання» за умовчанням (без кваліфікатора «ядра» або «користувач») мається на увазі «потік виконання ядра». Користувальницькі потоки виконання, реалізовані за допомогою віртуальних машин, називають також «зеленими потоками виконання». Користувальницькі потоки виконання, як правило, можна швидко створювати, і ними легко керувати, але вони не можуть використовувати переваги багатопотоковості та багатопроцесорності. Вони можуть блокуватися, якщо всі пов'язані з ним потоки виконання ядра зайняті, навіть якщо деякі потоки користувача готові до запуску.

Файбери є ще більш «легкими» блоками планування, що належать до кооперативної багатозадачності: виконуваний файбер повинен явно «поступитися» право іншим файберам на виконання, що робить їх реалізацію набагато легше, ніж реалізацію потоків виконання ядра або потоків користувача. Файбери можуть бути заплановані для запуску в будь-якому потоці виконання

всередині процесу. Це дозволяє додаткам отримати підвищення продуктивності за рахунок управління плануванням самого себе, замість покладатися на планувальник ядра (який може бути не налаштований на таке застосування). Паралельні середовища програмування, такі як OpenMP, зазвичай реалізують свої завдання за допомогою файберів.

Проблеми потоків виконання та файберів

Паралелізм та структури даних

Потоки виконання одного і того ж процесу спільно використовують один і той же адресний простір. Це дозволяє одночасно виконуваним кодам бути щільно пов'язаними та зручно обмінюватися даними без накладних витрат та складності міжпроцесної взаємодії. При спільному доступі декількох потоків навіть до простих структур даних виникає небезпека виникнення стану гонки в тому випадку, якщо для оновлення даних потрібно більше однієї інструкції процесора: два потоки виконання можуть спробувати одночасно оновити структури даних і отримати в результаті дані, стан яких відрізняється від очікуваного. Помилки, спричинені станом гонки, буває дуже важко відтворити та ізолювати.

Щоб уникнути цього, прикладні програмні інтерфейси (API) потоків виконання пропонують примітиви синхронізації, такі як м'ютекси для блокування структур даних від одночасного доступу. На однопроцесорних системах потік виконання, який звернувся до заблокованого м'ютексу, повинен зупинити роботу і, отже, ініціювати перемикання контексту. На багатопроцесорних системах потік виконання може замість опитування м'ютексу зробити захоплення спінлока. Обидва способи можуть знижувати продуктивність і змушувати процесор в SMP-системах конкурувати за шину пам'яті, особливо якщо рівень модульності блокувань занадто високий.

Введення-виведення та планування

Реалізація користувацьких потоків виконання та файберів, як правило, проводиться повністю в користувальницькому просторі. В результаті переключення контексту між потоками користувача і файберами в одному і тому ж процесі дуже ефективно, оскільки взагалі не вимагає ніякої взаємодії з ядром. Переключення контексту проводиться локально шляхом збереження регістрів процесора, що використовуються працюючим потоком користувача або файбером, і потім завантаженням регістрів, необхідних для нового виконання. Оскільки планування відбувається в просторі користувача, політика планування може бути легко адаптована до вимог конкретної програми.

Однак використання блокувань системних викликів для потоків користувача (на відміну від потоків виконання ядра) і файберів має свої проблеми. Якщо потік користувача або файбер виконує системний виклик, інші потоки виконання та файбери процесу не можуть працювати до завершення цієї обробки. Типовий приклад такої проблеми пов'язаний із виконанням операцій введення-виведення. Більшість програм розраховані на синхронне виконання введення-виводу. При ініціації введення-виведення робиться системний виклик, і він не повертається до його завершення. У проміжку весь процес блокується

ядром і не може виконуватися, позбавляючи можливості роботи інші потоки користувачів і файбери цього процесу.

Загальним рішенням цієї проблеми є забезпечення окремого API для введення-виведення, який реалізує синхронний інтерфейс з використанням внутрішнього неблокуючого введення-виводу, і запуск іншого потоку користувача або файбера на час обробки введення-виведення. Подібні рішення можуть бути передбачені для системних викликів, що блокують. Крім того, програма може бути написана так, щоб уникнути використання синхронного введення-виводу або інших блокуючих системних викликів.

У SunOS 4.x реалізовані так звані легковажні процеси або LWP. У NetBSD 2.x+ та DragonFly BSD реалізовані LWP як потоки виконання ядра (модель 1:1). У SunOS 5.2 і до SunOS 5.8, а також в NetBSD 2 і до NetBSD 4 реалізована дворівнева модель, що використовує один або кілька потоків користувача для кожного потік виконання ядра (модель M:N). У SunOS 5.9 та наступних версіях, а також у NetBSD 5 ліквідовано підтримку користувацьких потоків виконання, відбулося повернення до моделі 1:1. У FreeBSD 5 реалізовано модель M:N. У FreeBSD 6 підтримуються обидві моделі: 1:1 та M:N, і користувач може вибрати, яку з них він використовуватиме в даній програмі, використовуючи /etc/libmap.conf. У FreeBSD починаючи з версії 7 модель 1:1 стала використовуватися за умовчанням, а FreeBSD 8 і наступних версіях модель M:N не підтримується зовсім.

Використання потоків виконання ядра спрощує код користувача, переміщуючи деякі з найскладніших аспектів багатопотокового в ядро. Від програми не потрібно планування потоків виконання та явних захоплень процесора. Код користувача може бути записаний у звичному процедурному стилі, включаючи виклики блокуючого API без позбавлення доступу до процесора інших потоків виконання. Тим не менш, потоки виконання ядра можуть викликати перемикання контексту між потоками виконання в будь-який час і тим самим наразити на небезпеку появи помилок гонки і одночасності, які могли б не виникати. На SMP-системах це ще більше посилюється, оскільки потоки виконання ядра можуть у сенсі виконуватися одночасно різних процесорах.

Моделі

1:1 (потоки виконання лише на рівні ядра)

Потоки виконання, створені користувачем моделі 1-1, відповідають диспетчованим сутностям ядра. Це найпростіший варіант реалізації потоковості. У Windows API цей підхід використовувався з самого початку. У Linux звичайна бібліотека C реалізує цей підхід (через бібліотеку потоків POSIX, а більш старших версіях через Linux Threads). Такий самий підхід використовується ОС Solaris, NetBSD та FreeBSD.

N:1 (потоки виконання рівня користувача)

У моделі N:1 передбачається, що це потоки виконання рівня користувача відображаються на єдину плановану сутність рівня ядра, і нічого не знає склад прикладних потоків виконання. При такому підході перемикання контексту

може бути зроблено дуже швидко, і, крім того, він може бути реалізований навіть на простих ядрах, які не підтримують багатопотоковість. Однак, одним із головних недоліків його є те, що в ньому не можна отримати жодної вигоди з апаратного прискорення на багатопотокових процесорах або багатопроцесорних комп'ютерах, тому що тільки один потік виконання може бути запланований на будь-який момент часу. Ця модель використовується у GNU Portable Threads.

M:N (змішана потоковість)

У моделі M:N кілька M прикладних потоків виконання відображаються на деяке число N сутностей ядра або «віртуальних процесорів». Модель є компромісною між моделлю рівня ядра («1:1») та моделлю рівня користувача («N:1»). Взагалі кажучи, «M:N» потоковість системи є більш складною для реалізації, ніж ядро або потоки користувача виконання, оскільки зміна коду як для ядра, так і для користувальницького простору не потрібно. У M:N реалізації бібліотека потоків відповідає за планування потоків користувача виконання на наявних планованих сутностях. У цьому переключення контексту потоків робиться дуже швидко, оскільки модель дозволяє уникнути системних викликів. Тим не менш, збільшується складність та ймовірність інверсії пріоритетів,

5.3. Керування пам’яттю в операційних системах

З поняттям керування пам’яттю в ОС пов'язані такі технології:
– Функції керування пам'яттю в ОС.
– Типи адрес.
– Методи розподілу пам'яті в ОС.
– Принцип кешування даних у ОС.

Функції керування пам'яттю в ОС

Операційна система вирішує такі завдання:
– Відстеження вільної та зайнятої пам'яті.
– Виділення та звільнення пам'яті за запитами процесів.
– Забезпечує налаштування адрес.
– Підтримка механізму віртуальної пам'яті.

Типи адрес

Для ідентифікації змінних та команд використовуються:
– символьні імена (мітки);
– віртуальні адреси;
– фізичні адреси.

Символьні імена

Символьні імена надає користувач під час написання програми.

Віртуальні адреси

Віртуальні адреси виробляє компілятор. Оскільки відомо, у якому місці оперативної пам'яті буде завантажена програма, то компілятор надає змінним і командам віртуальні (умовні) адреси, зазвичай вважаючи за умовчанням, що

програма буде розміщена, починаючи з нульової адреси. Сукупність віртуальних адрес процесу називається **віртуальним адресним простором**. Кожен процес має власний віртуальний адресний простір.

Фізичні адреси

Фізичні адреси відповідають номерам осередків оперативної пам'яті, де насправді розташовані або будуть розташовані змінні та команди. Перехід від віртуальних адрес до фізичних може здійснюватися двома способами.

У першому випадку заміну віртуальних адрес на фізичні робить спеціальна системна програма – завантажувач, що переміщає. Переміщаючий завантажувач на підставі наявних у нього вихідних даних про початкову адресу фізичної пам'яті, в яку належить завантажувати програму, та інформації, наданої компілятором про адресно-залежні константи програми, виконує завантаження програми, поєднуючи її із заміною віртуальних адрес фізичними.

Другий спосіб полягає в тому, що програма завантажується в пам'ять у незміненому вигляді у віртуальних адресах, при цьому операційна система фіксує зміщення дійсного розташування програмного коду щодо адресного віртуального простору. Під час виконання програми при кожному зверненні до оперативної пам'яті виконується перетворення віртуальної адреси на фізичну.

Другий спосіб є більш гнучким, він допускає переміщення програми під час її виконання, в той час як завантажувач, що переміщає, жорстко прив'язує програму до спочатку виділеної їй ділянці пам'яті. Разом про те використання переміщуючого завантажувача зменшує накладні витрати, оскільки перетворення кожної віртуальної адреси відбувається лише один раз під час завантаження, тоді як у другому випадку – щоразу під час звернення за цією адресою.

Іноді (зазвичай у спеціалізованих системах) заздалегідь точно відомо, в якій області оперативної пам'яті виконуватиметься програма, і компілятор видає код, що виконується, відразу у фізичних адресах.

Методи розподілу пам'яті в ОС

Виділяють такі методи розподілу пам'яті:

Методи розподілу пам'яті без використання дискового простору

Розподіл пам'яті фіксованими розділами

Підсистема керування пам’яттю у разі виконує такі задачи:

– порівнюючи розмір програми, що надійшла виконання, і вільних розділів, вибирає відповідний розділ;

– здійснює завантаження програми та налаштування адрес.

Переваги:

– із загальною чергою – простота;

– с окремими чергами – більша продуктивність.

Недоліки:

– Неефективне розподілення пам'яті (великі незаповнені фрагменти).

– Розмір програми може бути більшим за розмір розділу.

– Перед запуском можна розділити розділи.

Розподіл пам'яті розділами змінної величини

З непереміщуваними розділами

ОС створює під кожну задачу розділ необхідного розміру, коли завдання завершується, розділ звільняється.

Переваги:

– Знімається необхідність організації черг.

– Більше шансів одержати пам'ять потрібного розміру.

– Економічніше.

Недоліки:

– Фрагментація (вільний блок пам'яті виявляється розрізаний) – не будь-яка програма може бути запущена.

З розділами, що переміщаються

Фрагментація стиснення (переміщення): при кожному звільненні пам'яті розділи зміщуються у бік старших (молодших) адрес.

Перевага: немає фрагментації.

Недолік: зниження продуктивності.

Способи упорядкування адрес

Виділяють такі способи упорядкування адрес:

– Налаштування адрес, коли програма запущена (завантажувач, що переміщається).

– Динамічне перетворення віртуальних адрес на фізичні.

Способи боротьби із фрагментацією

У певні моменти часу відбувається стиск у бік молодших адрес. ОС послідовно переглядає зайняті програмами блоки, знаходить розрив і зміщує адресу. Ця схема ефективна у разі динамічного перетворення; якщо використовується завантажувач, що переміщається, то відбувається повний перерахунок адрес, який є дуже ресурсомістким.

Методи розподілу пам'яті з використання дискового простору

Метод оверлєєв

Був використаний та реалізований в ОС MS DOS. Програміст розбиває додаток на кілька частин (оверлєїв), що вміщуються у доступну пам'ять (640 кб). Спочатку відбувається завантаження 0-го оверлея, потім він вивантажується і завантажується перший, і так далі. Програма міститься на диску, активний оверлей – в оперативній пам'яті, а всі механізми забезпечуються програмістом. Механізм потребує ретельного проектування програм.

Сторінковий розподіл віртуальної пам'яті

Адресний простір процесу поділяється на сторінки фіксованих розділів. Фізична пам'ять у системі теж ділиться на сторінки, аналогічні віртуальній пам'яті. До кожного процесу ОС створює службову структуру – таблицю сторінок (дає однозначне відображення віртуальних сторінок у фізичні).

При активізації чергового процесу спеціальний регістр процесора завантажується адресу таблиці сторінок даного процесу.

При кожному зверненні до пам'яті читання з таблиці сторінок інформації про віртуальну сторінку, до якої відбулося звернення. Якщо ця віртуальна

сторінка знаходиться в оперативній пам'яті, то виконується перетворення віртуальної адреси на фізичну. Якщо потрібна віртуальна сторінка в даний момент вивантажена на диск, то відбувається так зване сторінкове переривання. Процес, що виконується, переводиться в стан очікування, і активізується інший процес з черги готових. Паралельно програма обробки переривання сторінок знаходить на диску необхідну віртуальну сторінку і намагається завантажити її в оперативну пам'ять. Якщо у пам'яті є вільна фізична сторінка, то завантаження виконується негайно, якщо ж вільних сторінок немає, вирішується питання, яку сторінку слід вивантажити з оперативної пам'яті.

Прапори

Види прапорів:

– час обробки;
– було звернення чи ні;
– ознака сторінок, що не вивантажуються;
– частота використання.

Розглянемо механізм перетворення віртуальної адреси у фізичну при сторінковій організації пам'яті.

Віртуальна адреса при сторінковому розподілі може бути представлена у вигляді пари (p, s), де p – номер віртуальної сторінки процесу (нумерація сторінок починається з 0), а s – усунення в межах віртуальної сторінки. Враховуючи, що розмір сторінки дорівнює 2 ступеня до, зсув s може бути отримано простим відділенням k молодших розрядів в двійковій запису віртуальної адреси. Старші розряди, що залишилися, є двійковим записом номера сторінки p.

При кожному зверненні до оперативної пам'яті апаратними засобами виконуються такі дії:

– на підставі початкової адреси таблиці сторінок, номера віртуальної сторінки та довжини запису в таблиці сторінок визначається адреса потрібного запису в таблиці,
– із цього запису витягується номер фізичної сторінки
– до номера фізичної сторінки приєднується зміщення.

Таблицю сторінок прагнуть розміщувати в "швидких" пристроях, що запам'ятовують. Це може бути, наприклад, набір спеціальних регістрів або пам'ять, що використовує зменшення часу доступу асоціативний пошук і кешування даних.

Сторінковий розподіл пам'яті може бути реалізований у спрощеному варіанті, без вивантаження сторінок на диск. І тут всі віртуальні сторінки всіх процесів постійно перебувають у оперативної пам'яті. Такий варіант сторінкової організації хоч і не надає користувачеві віртуальної пам'яті, але виключає фрагментацію.

Переваги:

– немає фрагментації
– пам'ять використовується оптимально
– механізм не вимагає жодних дій з боку програми

– швидке перетворення віртуальних адрес у фізичні.

Недоліки:

– при малих сторінках високі витрати при зберіганні таблиці сторінок

– немає можливості вказати тип інформації, що міститься, тому не можна встановити права доступу.

Сегментний розподіл пам'яті

Віртуальний адресний простір процесу ділиться на сегменти, розмір яких визначається програмістом з урахуванням змістового значення інформації, що міститься в них. Окремий сегмент може бути підпрограмою, масивом даних і т.п. Іноді сегментація програми виконується за замовчуванням компілятором.

При завантаженні процесу частина сегментів поміщається в оперативну пам'ять (при цьому для кожного з цих сегментів операційна система підшукує потрібну ділянку вільної пам'яті), а частина сегментів розміщується в дисковій пам'яті. Сегменти однієї програми можуть займати в оперативній пам'яті безмежні ділянки. Під час завантаження система створює таблицю сегментів процесу (аналогічну таблиці сторінок), в якій для кожного сегмента вказується початкова фізична адреса сегмента в оперативній пам'яті, розмір сегмента, правила доступу, ознака модифікації, ознака звернення до даного сегменту за останній інтервал часу та інша інформація. Якщо віртуальні адресні простори кількох процесів включають один і той же сегмент, то в таблицях сегментів цих процесів робляться посилання на ту саму ділянку оперативної пам'яті,

Система з сегментної організацією функціонує аналогічно системі зі сторінковою організацією: іноді відбуваються переривання, пов'язані з відсутністю необхідних сегментів у пам'яті, за необхідності звільнення пам'яті деякі сегменти вивантажуються, при кожному зверненні до оперативної пам'яті виконується перетворення віртуального адреси на фізичний. Крім того, при зверненні до пам'яті перевіряється, чи доступ доступного типу до даного сегменту.

Віртуальна адреса при сегментної організації пам'яті може бути представлена парою (g, s), де g – номер сегмента, а s – усунення в сегменті. Фізична адреса виходить шляхом додавання початкової фізичної адреси сегмента, знайденого в таблиці сегментів за номером g, і зміщення s.

Недоліком цього методу розподілу пам'яті є фрагментація лише на рівні сегментів і повільніше проти сторінковою організацією перетворення адреси.

Сегментно-сторінкова організація поділу пам'яті

Даний метод є комбінацією сторінкового та сегментного розподілу пам'яті і, внаслідок цього, поєднує в собі переваги обох підходів. Віртуальний простір процесу ділиться на сегменти, а кожен сегмент ділиться на віртуальні сторінки, які нумеруються в межах сегмента. Оперативна пам'ять поділяється на фізичні сторінки. Завантаження процесу виконується операційною системою посторінково, при цьому частина сторінок розміщується в оперативній пам'яті, частина на диску. Для кожного сегмента створюється своя таблиця сторінок, структура якої повністю збігається зі структурою таблиці сторінок, що використовується при розподілі сторінок. Для кожного процесу створюється

таблиця сегментів, де вказуються адреси таблиць сторінок всім сегментів даного процесу.

Переваги: цей механізм підтримується процесорами, тому працює швидше.

Недолік: великі обсяги таблиць.

Принцип кешування даних у ОС

Кеш-пам'ять – це спосіб організації спільного функціонування двох типів пристроїв, що відрізняються часом доступу і вартістю зберігання даних, який дозволяє зменшити середній час доступу до даних за рахунок динамічного копіювання в "швидкий" запам’ятовуючий пристрій (ЗП) найбільш часто використовуваної інформації з "повільного" ЗП.

Кеш-пам'яттю часто називають не тільки спосіб організації роботи двох типів пристроїв, що запам'ятовують, але і один з пристроїв – "швидке" ЗП. Воно коштує дорожче і зазвичай має порівняно невеликий обсяг. Важливо, що механізм кеш-пам'яті є прозорим для користувача, який не повинен повідомляти жодної інформації про інтенсивність використання даних і не повинен брати участь у переміщенні даних із ЗП одного типу в ЗП іншого типу, все це робиться автоматично системними засобами.

У системах, оснащених кеш-пам'яттю, кожен запит до оперативної пам'яті виконується відповідно до наступного алгоритму:

– Проглядається вміст кеш-пам'яті з метою визначення, чи не знаходяться потрібні дані в кеш-пам'яті; кеш-пам'ять не є адресованою, тому пошук потрібних даних здійснюється за вмістом – значенням поля "адреса в оперативній пам'яті", взятому із запиту.

– Якщо дані виявляються в кеш-пам'яті, вони зчитуються з неї, і результат передається в процесор.

– Якщо потрібних даних немає, вони разом зі своєю адресою копіюються з оперативної пам'яті в кеш-пам'ять, і результат виконання запиту передається в процесор. При копіюванні даних може виявитися, що в кеш-пам'яті немає вільного місця, тоді вибираються дані, до яких в останній період було найменше звернень, для витіснення з кеш-пам'яті. Якщо дані, що витісняються, були модифіковані за час знаходження в кеш-пам'яті, то вони переписуються в оперативну пам'ять. Якщо ці дані були модифіковані, їх місце у кеш-пам'яті оголошується вільним.

На практиці в кеш-пам'ять зчитується не один елемент даних, до якого відбулося звернення, а цілий блок даних, це збільшує ймовірність так званого "попадання в кеш", тобто знаходження потрібних даних у кеш-пам'яті.

5.4. Файлові системи

Файлова система (англ. *file system*) – порядок, що визначає спосіб організації, зберігання та іменування даних на носіях інформації в комп'ютерах, а також в іншому електронному обладнанні: цифрових фотоапаратах, мобільних телефонах і т. п. Файлова система визначає формат вмісту та спосіб фізичного зберігання інформації, яку прийнято групувати як файлів. Конкретна файлова система визначає розмір імен файлів (і каталогів), максимальний можливий розмір файлу та розділу, набір атрибутів файлу. Деякі файлові системи надають сервісні можливості, наприклад розмежування доступу або шифрування файлів.

Файлова система пов'язує носій інформації з одного боку та API доступу до файлів – з іншого. Коли прикладна програма звертається до файлу, вона не має жодного уявлення про те, яким чином розташована інформація в конкретному файлі, так само як і про те, на якому фізичному типі носія (CD, жорсткому диску, магнітній стрічці, блоці флеш-пам'яті або іншому) він записаний. Все, що знає програма – це ім'я файлу, його розмір та атрибути. Ці дані вона одержує від драйвера файлової системи. Саме файлова система встановлює, де і як буде записано файл на фізичному носії (наприклад, жорсткому диску).

З погляду операційної системи (ОС), весь диск є набором кластерів (як правило, розміром 512 байт і більше). Драйвери файлової системи організують кластери у файли та каталоги (реально є файлами, що містять список файлів у цьому каталозі). Ці ж драйвери відстежують, які з кластерів нині використовуються, які вільні, які позначені як несправні.

Однак файлова система не обов'язково безпосередньо пов'язана з фізичним носієм інформації. Існують віртуальні файлові системи, а також мережні файлові системи, які є лише способом доступу до файлів, що знаходяться на віддаленому комп'ютері.

Основні функції файлових систем

Основними функціями файлової системи є:

– розміщення та впорядкування на носії даних у вигляді файлів;
– визначення максимально підтримуваного обсягу даних носії інформації;
– створення, читання та видалення файлів;
– призначення та зміна атрибутів файлів (розмір, час створення та зміни, власник та творець файлу, доступний тільки для читання, прихований файл, тимчасовий файл, архівний, виконуваний, максимальна довжина імені файлу тощо);
– визначення структури файлу;
– пошук файлів;
– організація каталогів для логічного організації файлів;
– захист файлів під час системного збою;
– захист файлів від несанкціонованого доступу та зміни їхнього вмісту.

Класифікація файлових систем

За призначенням файлові системи можна класифікувати на нижченаведені категорії.

– Для носіїв з довільним доступом (наприклад, жорсткий диск): FAT32, HPFS, ext2 та ін. Оскільки доступ до дисків у кілька разів повільніше, ніж доступ до оперативної пам'яті, для збільшення продуктивності в багатьох файлових системах застосовується асинхронний запис змін на диск. Для цього застосовується або журналювання, наприклад, в ext3, ReiserFS, JFS, NTFS, XFS, або механізм soft updates та ін. Журналювання поширене в Linux, застосовується в NTFS. Soft updates – у BSD-системах.

– Для носіїв з послідовним доступом (наприклад, магнітні стрічки): QIC та ін.

– Для оптичних носіїв – CD і DVD: ISO9660, HFS, UDF та ін.

– Віртуальні файлові системи: AEFS та ін.

– Мережеві файлові системи: NFS, CIFS, SSHFS, GmailFS та ін.

– Для флеш-пам'яті: YAFFS, ExtremeFFS, exFAT.

– Дещо випадають із загальної класифікації спеціалізовані файлові системи: ZFS (власне файловою системою є лише частина ZFS), VMware VMFS (т.з. кластерна файлова система, яка призначена для зберігання інших файлових систем) та ін.

Завдання файлової системи

Основні функції будь-якої файлової системи націлені на вирішення наступних завдань:

– найменування файлів;

– програмний інтерфейс роботи з файлами для програм;

– відображення логічної моделі файлової системи на фізичну організацію сховища даних;

– організація стійкості файлової системи до збоїв живлення, помилок апаратних та програмних засобів;

– зміст параметрів файлу, необхідні правильної його взаємодії коїться з іншими об'єктами системи (ядро, докладання тощо.).

У розрахованих на багато користувачів системах з'являється ще одне завдання: захист файлів одного користувача від несанкціонованого доступу іншого користувача, а також забезпечення спільної роботи з файлами, наприклад, при відкритті файлу одним з користувачів, для інших цей же файл тимчасово буде доступний в режимі «тільки читання».

Файлова система (ФС) дозволяє оперувати не нулями та одиницями, а більш зручними та зрозумілими об'єктами – файлами. Для зручності роботи з файлами використовуються їх символьні ідентифікатори – імена. Сам вміст файлів записано в *кластери* (*clusters*) – дрібні одиниці даних, якими оперує файлова система, розмір їх кратний 512 байтам (512 байт – розмір сектора жорсткого диска, мінімальної одиниці даних, яка зчитується з диска або записується на диск). Для організації інформації крім імені файлу використовуються також каталоги (або папки), як абстракція, що дозволяє

групувати файли за певним критерієм. За своєю суттю каталог – це файл, що містить інформацію про вкладені в нього каталоги і файли.

Вся інформація про файли зберігається в спеціальних областях розділу (томи) – файлових довідниках. Структура цих довідників залежить від типу файлової системи. Довідник файлів дозволяє асоціювати числові ідентифікатори файлів та додаткову інформацію про них (дата зміни, права доступу, ім'я тощо) з безпосереднім вмістом файлу, що зберігається в іншій області розділу (томи).

На жорстких дисках комп'ютерів під керуванням систем сімейства Windows використовуються два типи файлових систем: **FAT** (FAT16 та FAT32) та **NTFS**.

5.5. Захисні механізми операційних систем

Захист ОС сімейства Unix

Захист ОС сімейства Unix у загальному випадку базується на трьох основних механізмах:

– ідентифікації та автентифікації користувача при вході до системи;

– розмежування прав доступу до файлової системи, в основі якої лежить реалізація дискреційної моделі доступу;

– аудит, тобто. реєстрація подій.

При цьому відзначимо, що для різних клонів ОС сімейства Unix можливості механізмів захисту можуть незначно відрізнятися, однак розглядатимемо ОС Unix у загальному випадку, без урахування деяких незначних особливостей окремих ОС цього сімейства.

Побудова файлової системи та розмежування доступу до файлових об'єктів має особливості, властиві цьому сімейству ОС. Розглянемо стисло ці особливості. Усі дискові накопичувачі (томи) поєднуються в єдину ***віртуальну файлову систему*** шляхом операції монтування тома. При цьому вміст тома проектується на вибраний каталог файлової системи. Елементами файлової системи є також всі пристрої, що підключаються до комп'ютера, що захищається (монтуються до файлової системи). Тому розмежування доступу до них здійснюється через файлову систему.

Кожен файловий об'єкт має індексний дескриптор, у якому зберігається інформація про розмежування доступу до цього файлового об'єкта. Права доступу поділяються на три категорії: доступ для власника, доступ для групи та доступ для інших користувачів. У кожній категорії визначаються права на читання, запис та виконання (у разі каталогу – перегляд).

Користувач має унікальні символьний ідентифікатор (ім'я) та числовий ідентифікатор (UID). Символьний ідентифікатор пред'являється користувачем під час входу до системи, числової використовується операційною системою визначення прав користувача у системі (доступ до файлів тощо.).

Принципові недоліки захисних механізмів ОС сімейства Unix

Розглянемо у випадку недоліки реалізації системи захисту ОС сімейства Unix у частині невиконання вимог захисту конфіденційної інформації, безпосередньо пов'язані з можливістю НСД до інформації.

Спочатку відзначимо, що у ОС сімейства Unix, внаслідок реалізованої нею концепції адміністрування (не централізована), неможливо забезпечити замкнутість (чи цілісність) програмного середовища. Це пов'язано з неможливістю встановлення атрибуту "виконання" на каталог (для каталогу цей атрибут обмежує можливість "огляду" вмісту каталогу). Тому при розмежуванні адміністратором доступу користувачів до каталогів, користувач, як "власник" створюваного ним файлу, може занести у свій каталог файл, що виконується і, як його "власник", встановити на файл атрибут "виконання", після чого запустити записану ним програму. Ця проблема безпосередньо пов'язана з концепцією захисту інформації, що реалізується в ОС.

Не повному обсязі реалізується дискреційна модель доступу, зокрема, що неспроможні розмежовуватися права доступу користувача "root" (UID = 0), тобто. даний суб'єкт доступу виключається із схеми управління доступом до ресурсів. Відповідно всі процеси, що їм запускаються, мають необмежений доступ до ресурсів, що захищаються. З цим недоліком системи захисту пов'язано безліч атак, зокрема:

– несанкціоноване одержання прав root;

– запуск з правами root власного виконуваного файлу (локально чи віддалено впровадженого), причому несанкціонована програма отримує повний доступом до ресурсів і т.д.

Крім того, в ОС сімейства Unix неможливо вбудованими засобами гарантовано видаляти залишкову інформацію. Для цього у системі абсолютно відсутні відповідні механізми.

Слід зазначити, більшість ОС даного сімейства не мають можливості контролю цілісності файлової системи, тобто. не містять відповідних інтегрованих засобів. У разі додатковими утилітами то, можливо реалізований контроль конфігураційних файлів ОС за розкладом у той час, як найважливішою можливістю даного механізму вважатимуться контроль цілісності програм (додатків) їх запуском, контроль файлів даних користувача тощо.

Щодо реєстрації (аудиту), то в ОС сімейства Unix не забезпечується реєстрація видачі документів на "тверду копію", а також деякі інші вимоги до реєстрації подій.

Якщо ж трактувати вимоги до управління доступом у загальному випадку, то при захисті комп'ютера у складі ЛОМ необхідно управління доступом до вузлів мережі. Однак вбудованими засобами захисту деяких ОС сімейства Unix управління доступом до вузлів не реалізується.

З наведеного аналізу видно, що багато механізмів, необхідних з погляду виконання формалізованих вимог, більшістю ОС сімейства Unix не реалізується в принципі, або реалізується лише частково.

Механізми безпеки Windows Server 2022

Безпека була в центрі уваги в останніх збірках **Windows**, як і у випадку з **Windows Server 2022**. Він поєднує можливості безпеки для **Windows Server**, а також підтримує багаторівневу безпеку для активізації механізму активного захисту від просунутих загроз і атак. Ось дві ключові функції безпеки, які ви можете очікувати в **Windows Server 2022**:

– Безпечне підключення.

– Сервер із захищеним ядром.

Безпечне підключення

Безпечне (Secure) підключення є обов'язковим та дуже необхідним для серверів, особливо в сучасному світі, де щодня відбуваються нові кібератаки. Щоб забезпечити встановлення безпечних з'єднань, у **Windows Server 2022** реалізовані такі функції:

HTTPS і TLS 1.3 включені в Windows Server 2022 за замовчуванням. (HTTPS and TLS 1.3 є в Windows Server 2022 заборонено.) Остання версія протоколу безпеки Інтернету – **Transport Layer Security** (**TLS**) 1.3. Він забезпечує безпечний канал зв'язку між двома кінцевими точками за рахунок шифрування даних. Тепер, увімкнувши **HTTPS** (HTPPS) і **TLS 1.3** у **Windows Server 2022**, він гарантує, що дані клієнтів, підключених до сервера, захищені. Від старих криптографічних механізмів відмовляються та використовуються нові алгоритми безпеки.

Безпечний DNS (Secure DNS) – ще одна гарна розширена функція, що забезпечує безпечне підключення. **DNS-over-HTTPS** (**DoH**) тепер підтримується **DNS-клієнтом** (DNS Client) у **Windows Server 2022**. **DoH шифрує** (DoH) DNS – (DNS) запити з використанням протоколу **HTTPS** та зберігає конфіденційність трафіку, що ще більше підвищує безпеку. Крім того, за його допомогою можна запобігти підслуховуванню.

Для шифрування та підпису **Server Message Block** (**SMB) у** (SMB) **Windows Server** тепер підтримуються **криптографічні набори AES-256-GCM та AES-256-CCM** (AES-256-GCM and AES-256-CCM cryptographic suites). **Надійне** (Strong) шифрування є потребою у обчисленнях, оскільки зловмисники продовжують знаходити нові способи злому алгоритмів безпеки. Використання пакетів **AES-256-GCM** та **AES-256-CCM** забезпечує більш високий рівень шифрування. Тим не менш, **AES-128** для сумісності з попередніми версіями, як і раніше, підтримується.

Для **загальних томів кластера** (Cluster Shared Volumes) (**CSV**) та рівня **шини сховища** (Storage Bus Layer) (**SBL**) буде жорстке та покращене шифрування та підписання внутрішньовузлових з'єднань сховища, що підтримуються відмовостійкими кластерами **Windows Server.** В основному це означає, що користувачі тепер можуть шифрувати або підписувати обмін даними між сходом і заходом усередині кластера за допомогою **Storage Spaces Direct**.

У **Windows Server 2022 Datacenter**: Azure Edition та підтримуваних клієнтах **Windows підтримується** (Windows) **SMB через QUIC на додаток до TLS 1.3** (SMB over QUIC in addition to TLS 1.3). Це гарантує, що користувачі та програми мають безпечний доступ до даних із прикордонних файлових серверів.

Крім того, більше немає необхідності в **VPN** для мобільних та віддалених користувачів, щоб отримати доступ до своїх файлових серверів через **SMB**, перебуваючи у **Windows**.

Захищений основний сервер

Захищене основне обслуговування забезпечує додатковий рівень захисту від нових загроз та викликів. Він заснований на трьох основних параметрах, які полягають у наступному:

– Спрощена безпека.
– Розширений захист.
– Превентивний захист.

Спрощена безпека (Simplified Security)

Не буде жодних труднощів у налаштуванні функцій безпеки захищених основних серверів. Ви можете легко налаштувати **Windows Server** з **Центру адміністрування Windows** (Windows Admin Center).

Розширений захист (Advanced Protection)

Оскільки захищені базові сервери повністю використовують апаратне забезпечення, вбудоване ПЗ та можливості операційної системи, забезпечується покращений захист від поточних та майбутніх загроз. Він має широкий підхід у областях, які включають:

– **Апаратний корінь довіри** (Hardware root-of-trust): Trusted Platform Module 2.0 (**TPM 2.0**) забезпечує використання захищених основних серверів. Він забезпечує апаратний корінь довіри, який підвищує рівень безпеки, що забезпечується такими можливостями, як **BitLocker**.

– **Захист вбудованого програмного забезпечення:** (Firmware Protection:) Оскільки вбудоване програмне забезпечення працює з вищими привілеями і пов'язане з безліччю вразливостей безпеки, поліпшення захисту вбудованого програмного забезпечення є потребою години. Такі функції, як **технологія Dynamic Root (DRTM)**, **захист** DMA і **системи із захищеним ядром, можуть забезпечити захист вбудованого ПЗ.** (DMA)

– **Безпека на основі віртуалізації (VBS):** (Virtualization-based security (VBS)) **VBS** та цілісність коду на основі гіпервізора (**HVCI**) підтримуються захищеними центральними серверами.

Превентивний захист (Preventative Defense)

Захищені головні сервери активно захищають систему від зловмисників.

Механізми безпеки Windows 10/11

Безпека Windows створена на основі принципів «Нікому не довіряй» для захисту даних і доступу їх будь-якого місця. Забезпечує безпеку та ефективність вашої роботи.

Механізми безпеки Windows 10/11 включають у себе наступні розділи:

"Нікому не довіряй» та Windows

Апаратна безпека

– Довірений платформний модуль.

– Захист від вбудованого програмного забезпечення System Guard у Захиснику Windows.

– Безпечний запуск System Guard у Захиснику Windows та захист SMM.

– Захист цілісності коду на основі віртуалізації.

– Захист DMA для ядра.

Безпека операційної системи

– Безпека системи.

– Шифрування та захист даних.

– Базові параметри безпеки Windows.

– Посібник з віртуальних приватних мереж.

– Брандмауер Windows Defender.

– Захист від вірусів та погроз.

Безпека додатків

– Управління програмами та захист на основі віртуалізації.

– Управління додатком.

– Application Guard.

– Пісочниця Windows.

– Фільтр SmartScreen у Microsoft Defender.

– S/MIME для Windows.

Безпека користувача та захищене посвідчення

– Windows Hello для бізнесу.

– Захист від крадіжки облікових даних у Windows.

– Захист облікових даних домену.

– Credential Guard у Захиснику Windows.

– Втрачені та забуті паролі.

– Управління доступом.

– Смарт-картки.

Хмарні служби

– Управління мобільними пристроями.

– Azure Active Directory.

– Ваш обліковий запис Майкрософт.

– OneDrive.

– Сімейна безпека.

Основи безпеки

– Життєвий цикл розробки захищених програм (Майкрософт).

– Програма Microsoft Bug Bounty.

– Загальні критерії сертифікації.

– Перевірка на відповідність стандарту FIPS 140.

Елементи управління конфіденційністю

Розглянемо усі ці елементи більш детально.

Нульова довіра та працездатність пристроїв Windows

Організаціям потрібна модель безпеки, яка ефективніше адаптується до складності сучасного робочого середовища. IT-адміністраторам необхідно використовувати гібридне робоче місце, одночасно захищаючи людей, пристрої, програми та дані скрізь, де вони знаходяться. Реалізація моделі «Нікому не довіряй» для забезпечення безпеки допомагає усунути сучасні складні середовища.

Принципи нульової довіри:

– **Явним чином перевірте.** Завжди виконувати автентифікацію та авторизацію на основі всіх доступних точок даних, включаючи посвідчення користувача, розташування, працездатність пристрою, службу або робоче навантаження, класифікацію даних та моніторинг аномалій.

– **Використовуйте найменш привілейований доступ**. Обмеживши доступ користувачів за допомогою JIT-доступу та JIT-доступу, адаптивних політик на основі ризиків та захисту даних для захисту даних та підтримки продуктивності.

– **Припустимо, що порушення безпеки**. Запобігайте отриманню доступу зловмисниками, щоб звести до мінімуму потенційні збитки даним та системам. Захист привілейованих ролей, перевірка наскрізного шифрування, використання аналітики для отримання видимості та виявлення загроз для підвищення захисту.

Концепція перевірки «**Нікому не** довіряй» явно застосовується до ризиків, які є як пристроями, так і користувачами. Windows забезпечує **атестацію** працездатності пристроїв та **можливості** умовного доступу, які використовуються для надання доступу до корпоративних ресурсів.

Умовний доступ оцінює сигнали ідентифікації, щоб переконатися, що користувачі є користувачами, які вони говорять, перш ніж їм буде надано доступ до корпоративних ресурсів.

Windows 11 підтримує атестацію працездатності пристроїв, допомагаючи переконатися, що пристрої перебувають у працездатному стані та не були змінені. Ця можливість допомагає користувачам отримувати доступ до корпоративних ресурсів незалежно від того, чи знаходяться вони в офісі, вдома чи у дорозі.

Атестація допомагає перевірити посвідчення та стан важливих компонентів, а також переконатися, що пристрій, вбудоване програмне забезпечення та процес завантаження не були змінені. Відомості про вбудоване програмне забезпечення, процес завантаження та програмне забезпечення використовуються для перевірки стану безпеки пристрою. Ці дані криптографічно зберігаються в модулі довіреної платформи (TPM) для спільної обробки даних системи безпеки. Після атестації пристрою йому може бути надано доступ до ресурсів.

Атестація працездатності пристроїв у Windows

Під час завантаження може виникнути багато ризиків безпеки, оскільки цей процес може бути найбільш привілейованим компонентом усієї системи.

Процес перевірки використовує віддалену атестацію як безпечний канал для визначення та подання працездатності пристрою. Віддалена атестація визначає:

– Якщо пристрій може бути довіреним.

– Правильність завантаження операційної системи.

– Якщо в операційній системі увімкнено правильний набір функцій безпеки.

Ці визначення виконуються за допомогою захищеного кореня довіри за допомогою довіреного платформного модуля (TPM). Пристрої можуть підтвердити, що TPM увімкнено і що пристрій не було незаконно змінено.

Windows включає безліч функцій безпеки, які допомагають захистити користувачів від шкідливих програм та атак. Однак довіра до компонентів безпеки Windows може бути досягнута лише в тому випадку, якщо платформа завантажується належним чином і не була змінена. Windows використовує безпечне завантаження UEFI, антишкідливе програмне забезпечення раннього запуску (ELAM), динамічний корінь довіри для вимірювань (DRTM), довірене завантаження та інші низькорівневі функції безпеки обладнання та вбудованого програмного забезпечення. Коли комп'ютер увімкнеться до запуску захисту від шкідливих програм, Windows підтримуватиме відповідну конфігурацію обладнання, щоб забезпечити безпеку. Вимірювана та довіреназавантаження, реалізована завантажувачами та BIOS, перевіряє та криптографічно записує кожен крок завантаження у ланцюжку. Ці події прив'язані до співпроцесора безпеки (TPM), який виступає як корінь довіри. Віддалена атестація – це механізм, за допомогою якого служба зчитує та перевіряє ці події для надання перевіряється, ненаправлено та незаконно змінено стійкий звіт. Дистанційна атестація є довіреним аудитором завантаження системи, що дозволяє певним сутностям довіряти пристрою.

Нижче наведено зведення дій щодо атестації та нульової довіри на стороні пристрою.

1. На кожному етапі процесу завантаження, наприклад завантаження файлу, оновлення спеціальних змінних тощо, такі відомості, як ґеші файлів і підпис, вимірюються в PRS TPM. Вимірювання прив'язані специфікацією довіреної групи обчислень (TCG), яка визначає, які події можуть бути записані, та формат кожної події.

2. Після завантаження Windows атестатор або модуль, що перевіряється, запитує у довіреного платформного модуля отримання вимірювань, що зберігаються в регістрі конфігурації платформи (PCR) разом з журналом TCG. Вимірювання в обох компонентах формують свідчення атестації, яке потім відправляється в службу атестації.

3. Довірений платформний модуль перевіряється за допомогою ключів або криптографічних матеріалів, доступних у наборі мікросхем із службою сертифікатів Azure.

4. Потім ці відомості надсилаються до служби атестації у хмарі, щоб переконатися, що пристрій є безпечним. Microsoft Endpoint Manger інтегрується з Microsoft Атестація Azure для комплексного аналізу працездатності пристрою та підключення цієї інформації до умовного доступу до Azure Active Directory.

Ця інтеграція є ключем до рішень «Нікому не довіряй", які допомагають прив'язати довіру до ненадійних пристроїв.

5. Служба атестації виконує такі завдання:

– Перевірте цілісність свідчення. Ця перевірка виконується шляхом перевірки PRS, які відповідають значенням, які перераховуються шляхом відтворення журналу TCG.

– Переконайтеся, що TPM має дійсний ключ посвідчення атестації, виданий перевіркою TPM.

– Переконайтеся, що функції безпеки знаходяться в очікуваному стані.

– Служба атестації повертає звіт про атестацію, що містить відомості про функції безпеки на основі політики, налаштованої у службі атестації.

– Потім пристрій надсилає звіт у хмару Microsoft Endpoint Manager для оцінки надійності платформи відповідно до правил відповідності пристроїв, налаштованих адміністратором.

– Умовний доступ разом зі станом відповідності пристроїв вирішує дозволити або заборонити доступ.

Апаратна безпека Windows

Сучасні загрози вимагають сучасної безпеки з надійним узгодженням між апаратною безпекою та методами безпеки програмного забезпечення для захисту користувачів, даних та пристроїв. Тільки операційна система не може захиститися від широкого спектру засобів та методів, які зловмисники використовують для компрометації комп'ютера у його кремнієвих системах. Всередині зловмисників може бути важко виявити зловмисників, які можуть бути залучені до декількох шкідливих дій, від крадіжки важливих даних до запису адрес електронної пошти та інших конфіденційних відомостей. Ці нові загрози спричинять обчислювальні апаратні засоби, які захищені до самого ядра, включаючи апаратні мікросхеми та процесори. Корпорація Майкрософт та наші партнери, у тому числі виробники мікросхем та пристроїв.

Заходи безпеки	Функції & можливості
Довірений платформний модуль (TPM)	Довірений платформний модуль (TPM) призначений для надання апаратних функцій безпеки та запобігання небажаним незаконним змінам. TPM надають переваги безпеці та конфіденційності для системного обладнання, власників платформ та користувачів. Мікросхема довіреного платформного модуля – це захищений криптографічний процесор, який допомагає виконувати такі дії, як створення, зберігання та обмеження використання криптографічних ключів. Багато TPM включають кілька фізичних механізмів безпеки, щоб запобігти незаконній зміні та запобіганню незаконної зміни шкідливим програмним забезпеченням функцій безпеки довіреного платформного модуля.

Кореневий каталог довіри на основі обладнання з System Guard у Захиснику Windows	Для захисту критично важливих ресурсів, таких як автентифікація Windows, маркери єдиного входу, Windows Hello і модуль віртуальної довіреної платформи, вбудоване ПЗ та обладнання системи повинні бути надійними. System Guard у Windows Defender допомагає захистити та підтримувати цілісність системи в міру її запуску та перевірки того, чи дійсно цілісність системи була збережена за допомогою локальної та віддаленої атестації.
Увімкнення функції захисту цілісності коду на основі віртуалізації	HVCI – це функція безпеки на основі віртуалізації (VBS), доступна у Windows. У Windows безпеки пристроїв HVCI називається цілісністю пам'яті. HVCI і VBS покращують модель загроз Windows забезпечують надійніший захист від шкідливих програм, які намагаються використовувати Windows ядра. VBS використовує гіпервізор Windows для створення ізольованого віртуального середовища, яке стає коренем довіри операційної системи, яка передбачає, що ядро може бути скомпрометоване. HVCI – це критично важливий компонент, який захищає та захищає це віртуальне середовище, запускаючи в ньому цілісність коду в режимі ядра та обмежуючи виділення пам'яті ядра, яке може використовуватися для компрометації системи.
Захист прямого доступу до пам'яті ядра (DMA)	Пристрої гарячого модуля PCIe, такі як Thunderbolt, USB4 і CFexpress, дозволяють користувачам підключати нові класи зовнішніх периферійних пристроїв, включаючи графічні карти або інші пристрої PCI, до своїх комп'ютерів з інтерфейсом, ідентичним USB. Так як порти гарячого модуля PCI, що підключається, є зовнішніми і легко доступні, комп'ютери піддаються атакам прямого доступу до пам'яті (DMA). Захист доступу до пам'яті (також відомий як захист DMA ядра) захищає комп'ютери від атак DMA на диску, що використовують пристрої гарячого модуля PCIe, що підключається, обмеживши ці зовнішні периферійні пристрої можливістю безпосередньо копіювати пам'ять, коли користувач заблокує свій комп'ютер.

Комп'ютери із захищеними ядрами	Корпорація Майкрософт тісно співпрацює з партнерами OEM та постачальниками кремнієвого обладнання для створення захищених ядер комп'ютерів з глибоко інтегрованим обладнанням, вбудованим програмним забезпеченням та програмним забезпеченням для забезпечення підвищеної безпеки пристроїв, посвідчень та даних. Захищені основні комп'ютери забезпечують захист від складних атак і забезпечують підвищену впевненість при обробці критично важливих даних у деяких найбільш чутливих до цих галузях, таких як медичні працівники, які обробляють медичні записи та інші персональні дані (PII), комерційні ролі, які обробляють високий рівень впливу на бізнес та високо конфіденційні дані, такі як фінансовий контролер з даними про прибуток. Додаткові відомості прозахищені комп'ютери з ядрами.

Довірений платформний модуль

Технологія довірених платформних модулів (TPM) призначена для надання апаратних функцій, пов'язаних із безпекою. Мікросхема TPM – це надійний криптографічний процесор, який дозволяє створювати, зберігати та обмежувати використання криптографічних ключів. Детальний опис див. у наступних розділах.

Розділ	Опис
Огляд довіреного платформного модуля	Огляд довіреного платформного модуля (TPM) та його використання у Windows для керування доступом та автентифікації.
Основи TPM	Загальні відомості про роботу довіреного платформного модуля із ключами шифрування. Тут також описуються технології, які працюють з TPM, наприклад, віртуальні смарт-карти на основі TPM.
Параметри групової політики довіреного платформного модуля	Тут розглядаються служби TPM, якими централізовано можна керувати за допомогою параметрів групової політики:
Резервне копіювання даних відновлення TPM в AD DS	Опис резервного копіювання даних довіреного платформного модуля комп'ютера в доменних службах Active Directory (лише для Windows 10, версія 1511 та 1507).

Виправлення неполадок довіреного платформного модуля (TPM)	Опис дій, які можна виконати в оснастці TPM, TPM.msc: перегляд стану TPM, усунення проблем ініціалізації TPM та видалення ключів з TPM. Крім того, для TPM 1.2 та Windows 10 версії 1507 або 1511 або Windows 11 описується, як увімкнути або вимкнути TPM.
Загальні відомості про банки PCR на пристроях TPM 2.0	Загальні відомості про те, що відбувається під час перемикання банків PCR на пристроях TPM 2.0.
Рекомендації щодо довіреного платформного модуля	Розглядаються аспекти TPM, такі як різниця між TPM 1.2 та 2.0, та функції Windows, для яких потрібно або рекомендується використовувати TPM.

Захисник Windows System Guard: як апаратний корінь довіри допомагає захистити Windows 10

Щоб захистити критично важливі ресурси, такі як Windows стек автентифікації, однотонні маркери, біометричний стек Windows Hello і модуль віртуальної надійної платформи, необхідно довіряти прошивці та обладнанню системи.

Захисник Windows System Guard реорганізує існуючі Windows 10 функції цілісності системи під одним дахом і визначає наступний набір інвестицій у Windows безпеки. Він призначений для забезпечення цих гарантій безпеки:

– Захист та збереження цілісності системи у міру її початку.

– Перевірка того, що цілісність системи дійсно підтримується за допомогою локальної та віддаленої перевірки.

Підтримка цілісності системи у міру її початку

Статичний корінь довіри для вимірювання (SRTM)

З Windows 7 одним із засобів, які зловмисники будуть використовувати для виявлення і ухилятися від виявлення, є установка в системі так часто іменованого як bootkit або rootkit. Це шкідливе програмне забезпечення почнеться Windows запуску або під час процесу завантаження, що дозволить йому почати з найвищого рівня привілеїв.

З Windows 10 на сучасному обладнанні (тобто Windows 8 сертифіковано або більше) корінь довіри на основі обладнання допомагає переконатися, що несанкціоноване прошивка або програмне забезпечення (наприклад, bootkit) може розпочатися до завантаження Windows завантажувача. Ця коренева довіра на основі обладнання походить від функції Безпечного завантаження пристрою, яка є частиною єдиного extensible інтерфейсу прошивки (UEFI). Цей метод вимірювання статичних ранніх компонентів завантаження UEFI називається статичним коренем довіри вимірювання (SRTM).

Так як існують тисячі постачальників ПК, які виробляють багато моделей з різними версіями UEFI BIOS, при завантаженні стає неймовірно велика кількість вимірів SRTM. Для встановлення довіри тут існують два методи: або підтримувати список відомих «поганих» вимірів SRTM (також відомих як блок-

лист), або список відомих «хороших» вимірів SRTM (також відомий як список дозвільних даних).

Кожен варіант має недолік:

– Список відомих «поганих» вимірювань SRTM дозволяє хакеру змінити лише 1 біт у компоненті, щоб створити новий ґеш SRTM, який необхідно перерахувати. Це означає, що потік SRTM за своєю суттю є крихким – незначна зміна може призвести до недійсних для всього ланцюжка довіри.

– Список відомих «хороших» вимірювань SRTM вимагає, щоб кожен новий вимір комбінації BIOS/PC був ретельно доданий, що є повільним. Крім того, виправлення помилки для коду UEFI може зайняти багато часу для розробки, складання, повторної перевірки, перевірки та переробки.

Безпечний запуск – динамічний корінь довіри для вимірювання (DRTM)

Захисник Windows System Guard Secure Launch, вперше представлений у Windows 10 версії 1809, спрямований на усунення цих проблем за допомогою технології, відомої як динамічний корінь довіри для вимірювання (DRTM). DRTM дозволяє системі вільно завантажитися в ненаглядовий код спочатку, але незабаром після запуску системи в надійний стан, взявши під контроль всі процесори і змусивши їх вниз по відомому та виміряному шляху коду. Це дозволяє ненадійним раннім кодом UEFI завантажити систему, але потім безпечно перейти в надійний та виміряний стан.

Secure Launch спрощує управління вимірами SRTM, оскільки код запуску тепер не пов'язаний із певною конфігурацією обладнання. Це означає, що кількість допустимих вимірювань коду невелика, а майбутні оновлення можна розгорнути ширше та швидше.

Захист режиму керування системою (SMM)

Режим управління системою (SMM) – це режим ЦП спеціального призначення в мікроконтролерах x86, який обробляє управління живленням, конфігурацію обладнання, моніторинг теплового середовища та все інше, що виробник вважає за корисне. Щоразу, коли запитується одна з цих системних операцій, під час виконання викликається не переривання, що маскується (SMI), який виконує SMM-код, встановлений BIOS. SMM-код виконується на найвищому рівні привілеїв та невидимий для ОС, що робить його привабливою метою для шкідливих дій. Навіть якщо для пізнього запуску використовується system Guard Secure Launch, SMM-код потенційно може отримати доступ до пам'яті гіпервізора та змінити гіпервізор.

Для захисту від цього використовуються два методи:

– Захист підкачки для запобігання неналежного доступу до коду та даних.

– Спостереження та аттестація обладнання SMM.

Захист від пагінгу може бути реалізований для блокування певних таблиць коду для читання тільки для запобігання фальсифікації. Це запобігає доступу до пам'яті, яка не була призначена.

Функція обробника SMI з апаратним забезпеченням, відома як обробник SMI, може відстежувати SMM і не отримувати доступу до будь-якої частини адресного простору, на яку вона не повинна.

Захист SMM побудований на основі технології Secure Launch і потребує її функціонування. У майбутньому Windows 10 також буде вимірювати поведінку обробника SMI і засвідчити, що жодна пам'ять, що належить ОС, не була підроблена.

Перевірка цілісності платформи після Windows (час запуску)

Хоча Захисник Windows System Guard надає розширені засоби захисту, які допоможуть захистити та зберегти цілісність платформи під час завантаження та під час запуску, реальність така, що ми повинні застосувати ментальність «припустити порушення» навіть для наших найскладніших технологій безпеки. Ми можемо довіряти, що технології успішно роблять свою роботу, але нам також потрібна можливість переконатися, що вони успішно досягають своєї мети. Для цілісності платформи ми можемо просто довіряти платформі, яка потенційно може бути скомпрометована, щоб самостійно підтвердити її стан безпеки. Так Захисник Windows System Guard включає низку технологій, які дозволяють віддалено аналізувати цілісність пристрою.

Як Windows 10 чоботи, ряд вимірів цілісності Захисник Windows System Guard за допомогою довіреного модуля платформи 2.0 (TPM 2.0). System Guard Secure Launch не підтримує попередні версії TPM, наприклад TPM 1.2. Цей процес та дані ізольовані від Windows, щоб гарантувати, що дані вимірювань не схильні до типу фальсифікації, які можуть статися, якщо платформа була скомпрометована. Тут вимірювання можна використовувати для визначення цілісності прошивки пристрою, стану конфігурації обладнання та компонентів Windows, пов'язаних із завантаженням.

Після роботи системи Захисник Windows system Guard підписує та запечатує ці вимірювання за допомогою TPM. За запитом, система керування, наприклад Intune або Microsoft Endpoint Configuration Manager, може придбати їх для віддаленого аналізу. Якщо Windows Defender system Guard вказує, що пристрій не вистачає цілісності, система керування може прийняти ряд дій, наприклад заборонити пристрою доступ до ресурсів.

Безпечний запуск System Guard та захист SMM

У цьому розділі пояснюється, як налаштувати захист системного безпечного запуску та режиму керування системою (SMM) для підвищення безпеки під час запуску Windows 10 та Windows 11 пристроїв. Наведені нижче відомості представлені з погляду клієнта.

Увімкнення безпечного запуску System Guard

Ви можете увімкнути безпечний запуск System Guard за допомогою будь-якого з наступних параметрів:

- Управління мобільними пристроями (MDM).
- Групова політика.
- Безпека Windows програми.
- Реєстр.

Управління мобільними пристроями

Безпечний запуск System Guard можна налаштувати для мобільних Керування пристроями (MDM) за допомогою DeviceGuard у постачальника служб конфігурації політики DeviceGuard/ConfigureSystemGuardLaunch.

Групова політика

1. Натисніть кнопку « >« і виберіть «Змінити групову політику".

2. Натисніть кнопку «Адміністративні > шаблони конфігурації комп'ютера > «. Система > Device Guard > увімкне > конфігурацію безпечного запуску на основі віртуалізації.

Безпека Windows програми

Натисніть кнопку start > Установки > Update & Security > Безпека Windows > Open Безпека Windows > Device security > Core isolation > Firmware protection.

Реєстр

1. Відкрийте редактор реєстру.

2. Клацніть HKEY_LOCAL_MACHINE > system > CurrentControlSet > Control > DeviceGuard > Scenarios.

3. Клацніть правою кнопкою миші «Сценарії створення > ключа > « і наведіть ім'я нового ключа SystemGuard.****

4. Клацніть правою кнопкою миші systemGuard > New > DWORD (32-розрядне) значення та наведіть ім'я нового параметра DWORD Enabled.

5. Двічі клацніть «Увімкнено «, змініть значення на 1 і натисніть кнопку «ОК".

Перевірка налаштування та виконання безпечного запуску System Guard

Щоб переконатися, що безпечний запуск запущено, використовуйте інформацію про систему (MSInfo32). Натисніть **кнопку «** Пуск «**, знайдіть** Відомості про систему та перегляньте **розділ «** Запущені служби безпеки на основі віртуалізації» та «Настроєні служби безпеки на **основі віртуалізації"**.

Увімкнення функції захисту цілісності коду на основі віртуалізації (HVCI)

У цьому розділі описано різні способи увімкнення цілісності коду із захистом гіпервізора (HVCI) Windows 10 і Windows 11. Деякі програми, включаючи драйвери пристроїв, можуть бути несумісні з HVCI. Така несумісність може призвести до збою пристроїв або програмного забезпечення, а в окремих випадках може призвести до синього екрана. Такі проблеми можуть виникати після активації служби HVCI або безпосередньо під час активації служби. Якщо ці проблеми виникають, див. інструкції з усунення несправностей.

Так як у ньому використовується управління виконанням на основі *режиму,* HVCI краще працює з процесорами Intel Kaby Lake або AMD Zen 2 та пізнішими версіями. Процесори без MBEC покладатимуться на емуляцію цієї функції, звану обмеженим користувальницьким режимом, *яка* більш впливає на продуктивність.

Функції HVCI

– HVCI захищає зміну растрового зображення Control Flow Guard (CFG).

– HVCI також гарантує, що інші довірені процеси, такі як Credential Guard отримали дійсний сертифікат.

– Сучасні драйвери пристроїв повинні мати сертифікат EV (розширена перевірка) і підтримувати HVCI.

Увімкнення HVCI у Windows 10 та Windows 11

Щоб увімкнути HVCI на Windows 10 та Windows 11 із допоміжним обладнанням на підприємстві, використовуйте будь-який з наступних варіантів:

– Безпека Windows програми.

– Microsoft Intune (або іншого постачальника MDM).

– Групова політика.

– Microsoft Endpoint Configuration Manager.

– Реєстр.

Безпека Windows програми

HVCI **** > позначена як **** цілісність пам'яті в програмі Безпека Windows, і доступ до неї можна отримати за допомогою оновлення параметрів & Security > Безпека Windows > Device security > Core isolation details > Memory integrity.

Увімкнення HVCI за допомогою Intune

Щоб увімкнути Intune, необхідно використовувати вузол цілісності коду в постачальнику служб конфігурації AppLocker.

Включення HVCI за допомогою групової політики

1. Щоб змінити існуючий об'єкт групової політики або створити новий об'єкт групової політики, використовуйте групову політику редактора (gpedit.msc).

2. Перейдіть до адміністративних > шаблонів конфігурації комп'ютера > System > Device Guard.

3. Двічі клацніть «Включити безпеку на основі віртуалізації".

4. Клацніть « Увімкнено» і в розділі «Захист цілісності коду на основі віртуалізації» виберіть «Увімкнено з блокуванням UEFI **", щоб переконатися, що HVCI не можна відключити віддалено, або виберіть «Увімкнено без блокування UEFI".

5. Натисніть кнопку « ОК", щоб закрити редактор.

Щоб застосувати нову політику на комп'ютері, приєднаному до домену, перезапустіть або запустіть gpupdate /forceкомандний рядок з підвищеними привілеями.

Використання розділів реєстру для увімкнення захисту цілісності коду на основі віртуалізації

Встановіть наступні значення розділів реєстру, щоб увімкнути HVCI. Ці ключі надають такий самий набір параметрів конфігурації, що і групова політика.

Захист DMA для ядра

У Windows 10 версії 1803 корпорація Майкрософт представила нову функцію під назвою «Захист DMA ядра» для захисту комп'ютерів від атак прямого доступу до пам'яті (DMA) за допомогою пристроїв гарячого модуля PCI, що підключається до зовнішніх портів PCIe (наприклад, портів Thunderbolt™ CFexpress). У Windows 10 версії 1903 корпорація Майкрософт розширює підтримку захисту DMA ядра, щоб охопити внутрішні порти PCIe (наприклад, слоти M.2).

Атаки DMA на диску можуть призвести до розкриття конфіденційної інформації на комп'ютері або навіть впровадження шкідливих програм, які дозволяють зловмисникам обійти екран блокування або керувати комп'ютерами віддалено.

Ця функція не захищає від атак DMA за допомогою 1394/FireWire, PCMCIA, CardBus, ExpressCard тощо.

Фон

Пристрої PCI підтримують DMA, що дозволяє їм зчитувати та записувати системну пам'ять у міру потреби, не залучаючи системний процесор до цих операцій. Можливість DMA – це те, що робить пристрої PCI найбільш високовиробними пристроями, доступними на сьогоднішній день. Ці пристрої історично існували лише у корпусі ПК, підключених як картка чи припайних до плати. Для доступу до цих пристроїв користувачеві потрібно було вимкнути живлення системи та дизассемблювати корпус.

В даний час це більше не працює з портами PCIe гарячого модуля (наприклад, Thunderbolt™ і CFexpress).

Порти pcIe з гарячим модулем, що підключається, такі як технологія Thunderbolt™, надали сучасні комп'ютери з розширюваністю, яка раніше була недоступна для комп'ютерів. Він дозволяє користувачам підключати нові класи зовнішніх периферійних пристроїв, таких як графічні карти або інші пристрої PCI, до своїх комп'ютерів за допомогою гарячого модуля, що підключається, ідентичного USB. Наявність зовнішніх і легко доступних портів гарячого модуля PCI, що підключається, робить комп'ютери вразливими до атак DMA на дисках.

Атаки DMA на диску – це атаки, які відбуваються, коли власник системи відсутній і зазвичай займає менше 10 хвилин з простими і модеративними засобами атак (доступним, готовим обладнанням та програмним забезпеченням), які не потребують дизассемблювання комп'ютера. Простим прикладом може бути те, що власник комп'ютера залишає комп'ютер для швидкої кавоварки, а в перерві зловмисник підключається до USB-пристрою та покрокову передачу всіх секретів на комп'ютері або впроваджує шкідливу програму, яка дозволяє йому віддалено керувати комп'ютером.

Захист Windows від атак на диски DMA

Windows використовує системну одиницю керування пам’яттю вводу-виводу (IOMMU) для блокування запуску та виконання DMA зовнішніми периферійними пристроями, якщо драйвери цих периферійних пристроїв не підтримують ізоляцію пам'яті (наприклад, DMA-remapping). Периферійні пристрої із сумісними драйверами DMA Remapping автоматично

перераховуються, запускаються і можуть виконувати DMA у призначених ним областях пам'яті.

За замовчуванням периферійні пристрої з несумісними драйверами DMA remapping блокуватимуть запуск та виконання DMA доти, доки авторизований користувач не увійде до системи або не розблокує екран. IT-адміністратори можуть змінювати стандартну поведінку, яка застосовується до пристроїв з несумісними драйверами DMA RemaPping, за допомогою політик MDM DmaGuard.

Взаємодія з користувачем

За замовчуванням периферійні пристрої з драйверами пристроїв, сумісними з DMA, автоматично перераховуватимуться та запускатимуться. Периферійні пристрої з несумісними драйверами перенаправлення DMA будуть заблоковані, якщо периферійний пристрій був підключений до входу авторизованого користувача або під час блокування екрана. Після розблокування системи ос запускає периферійний драйвер, і периферійний пристрій працюватиме у звичайному режимі до перезавантаження системи або вимкнення периферійного пристрою. Периферійний пристрій продовжить працювати у звичайному режимі, якщо користувач заблокує екран або вийдіть із системи.

Сумісність системи

Для захисту від Ядра DMA потрібна нова підтримка вбудованого UEFI. Ця підтримка очікується тільки в системах, що недавно з'явилися, на базі Intel з Windows 10 версії 1803 (не для всіх систем). Безпека на основі віртуалізації (VBS) не потрібна.

Щоб дізнатися, чи підтримує система захисту DMA ядра, перевірте настільний додаток System Information (MSINFO32). Системи, випущені до Windows 10 версії 1803, не підтримують захист DMA ядра, але можуть використовувати інші заходи щодо усунення атак DMA, як описано у статті про лічильники BitLocker.

Безпека операційної системи Windows

Безпека та конфіденційність залежать від операційної системи, яка захищає систему та інформацію з моменту її запуску, забезпечуючи основний захист від мікросхеми у хмару. Windows 11 є найбільш безпечним Windows з великими заходами безпеки, призначеними для забезпечення безпеки. До цих заходів відносяться вбудоване розширене шифрування і захист даних, надійна безпека мережі та системи, а також інтелектуальні заходи захисту від загрози, що постійно змінюється.

Заходи безпеки	Функції та можливості
Безпечне завантаження та довірене завантаження	Безпечне завантаження та довірене завантаження допомагають запобігти завантаженню шкідливих програм та пошкоджених компонентів у Windows пристрою. Безпечне завантаження починається з початкового захисту під час завантаження, а потім довірене завантаження вибирає процес. Водночас безпечне завантаження та довірене завантаження допомагають забезпечити безпечне завантаження системи Windows.
Управління криптографією та сертифікатами	Шифрування використовує код для перетворення даних, щоб конкретний одержувач зчитую їх за допомогою ключа. Шифрування забезпечує конфіденційність, щоб ніхто, крім передбачуваного одержувача, не зчитування даних, цілісність, щоб забезпечити захист даних від незаконної зміни, та автентифікацію, яка перевіряє посвідчення для забезпечення безпеки обміну даними.
Безпека Windows програми	Вбудований Windows безпеки, знайдений у параметрах, дозволяє швидко переглянути стан безпеки та працездатність пристрою. Ці аналітичні відомості допомагають виявити проблеми та вжити заходів для захисту.
Шифрування та захист даних	Де конфіденційні дані не зберігаються, вони повинні бути захищені від несанкціонованого доступу, як шляхом крадіжки фізичного пристрою, так і з шкідливих додатків. Windows надійні рішення захисту неактивних даних, які забезпечують захист від зловмисників.
BitLocker	Шифрування диска BitLocker – це функція захисту даних, яка інтегрується в операційну систему та запобігає загрозі розкрадання даних або розкриття інформації на втрачених, вкрадених або неправильно виведених з експлуатації комп'ютерах. BitLocker забезпечує максимальний захист при використанні довіреного платформного модуля (TPM) версії 1.2 або вище.

Зашифрований жорсткий диск	Зашифрований жорсткий диск використовує швидке шифрування, що надається шифруванням диска BitLocker, для підвищення безпеки даних та управління ними. Шляхом передачі криптографічних операцій на обладнання функція «Зашифрований жорсткий диск» підвищує продуктивність BitLocker та знижує споживання ресурсів ЦП та електроенергії. Завдяки тому, що функція зашифрованих жорстких дисків швидко шифрує дані, пристрої організації можуть розширювати розгортання BitLocker з мінімальним впливом на продуктивність.
Базові показники безпеки	Базові параметри безпеки – це група рекомендованих корпорацією Майкрософт параметрів конфігурації, щоб пояснити їх вплив на безпеку. Ці параметри ґрунтуються на відгуках фахівців із забезпечення безпеки Microsoft, груп розвитку продуктів, партнерів та клієнтів. Базові показники безпеки включені до набору засобів забезпечення відповідності вимогам безпеки, який можна завантажити з Центру завантаження Майкрософт.
Віртуальна приватна мережа	Віртуальні приватні мережі (VPN) – це з'єднання точки в приватній або загальнодоступній мережі, наприклад, в Інтернеті. VPN-клієнт використовує спеціальні протоколи на основі TCP/IP або UDP, які називають протоколами тунелювання для віртуального виклику віртуального порту VPN-сервера.
Брандмауер Windows Defender	Брандмауер Захисника Windows – це брандмауер вузла з відстеженням стану, який допомагає захистити пристрій, дозволяючи створювати правила, які визначають, який мережевий трафік може входити на пристрій з мережі та який мережевий трафік пристрій може надсилати до мережі. брандмауер Windows Defender також підтримує протокол IPsec, який можна використовувати для запиту автентифікації з будь-якого пристрою, який намагається зв'язатися з пристроєм.

Антивірусна програма & захист від шкідливих програм	Антивірусна програма в Microsoft Defender включена у всі версії Windows 10, Windows Server 2016 і пізніших версій, а також Windows 11. Якщо у вас встановлена та включена інша антивірусна програма, антивірусна програма в Microsoft Defender автоматично відключається. Якщо видалити іншу програму, антивірусна програма в Microsoft Defender знову буде увімкнено. З моменту завантаження Windows антивірусна програма в Microsoft Defender постійно відстежує шкідливі програми, віруси та загрози безпеці. Оновлення завантажуються автоматично, щоб захистити пристрій від загроз. антивірусна програма в Microsoft Defender постійно перевіряє наявність шкідливих програм та загроз, а також виявляє та блокує потенційно небажані програми (додатки, які можуть негативно вплинути на пристрій, навіть якщо вони не вважаються шкідливими). Антивірусна програма в Microsoft Defender інтегрується з хмарним захистом, який забезпечує практично миттєве виявлення та блокування нових та нових загроз.
Правила скорочення напрямів атак	Ваші області атаки – це місця та способи, якими ви схильні до кібератаків. Правила зменшення вразливої зони вбудовані в Windows та Windows Server для запобігання та блокування певних дій, які часто використовуються для компрометації пристрою або мережі. Така поведінка може включати запуск скриптів або виконуваних файлів, які намагаються завантажити або запустити інші файли, запускати підозрілі скрипти або виконувати інші дії, які програми зазвичай не ініціюють під час звичайної роботи. Ви можете налаштувати правила зменшення вразливої зони для захисту від ризикованих дій.

Захист від незаконної зміни	Під час кібер атак (наприклад, спроб програм-шантажистів) зловмисники намагаються відключити функції безпеки, такі як антивірусний захист на цільових пристроях. Зловмисники хотіли б вимкнути функції безпеки, щоб спростити доступ до даних користувача, встановити шкідливі програми або іншим чином скористатися даними, посвідченнями та пристроями користувача, не побоюючись блокування. Захист від незаконної зміни допомагає запобігти таким діям. При захисті від незаконної зміни шкідливі програми не можуть виконувати такі дії, як: – відключення захисту від вірусів і загроз – відключення захисту в режимі реального часу – відключення моніторингу поведінки – відключення антивірусної програми (наприклад, IOffice Antivirus (IOAV)) – відключення хмарного захисту; – видалення оновлень аналітики безпеки.
Захист мережі	Захист мережі у Windows допомагає запобігти доступу користувачів до небезпечних IP-адрес і доменів, на яких можуть бути розміщені атаки фішингу, експлойти та інший шкідливий вміст в Інтернеті. Захист мережі є частиною скорочення напрямків атак та допомагає забезпечити додатковий рівень захисту для користувача. За допомогою служб на основі репутації захист мережі блокує доступ до потенційно шкідливих доменів та IP-адрес на основі низької репутації. У корпоративних середовищах захист мережі найкраще працює з Microsoft Defender для кінцевої точки, яка надає докладні звіти про події захисту в рамках більших сценаріїв дослідження.
Контрольований доступ до папок	За допомогою керованого доступу до папок можна захистити цінну інформацію у певних папках, керуючи доступом додатків до певних папок. Тільки довірені програми можуть отримати доступ до захищених папок, заданих при налаштуванні керованого доступу до папок. Як правило, до списку керованих папок включаються папки, що часто використовуються, наприклад для документів, зображень, файлів, що завантажуються. Керований доступ до папок допомагає захистити цінні дані від шкідливих програм та загроз, таких як програми-шантажисти.

Захист від експлойтів	Захист від експлойтів, доступний у Windows 10 версії 1709 і пізніших, автоматично застосовує кілька методів усунення експлойтів до процесів та додатків операційної системи. Захист від експлойтів найкраще працює з Microsoft Defender для кінцевої точки, яка надає організаціям докладні звіти про події та блоки захисту від експлойтів у рамках типових сценаріїв дослідження оповіщень. Ви можете увімкнути захист від експлойтів на окремому пристрої, а потім використовувати групова політика для поширення файлу XML на кілька пристроїв одночасно. Якщо ви знайдете захист на пристрої, з'явиться повідомлення із центру сповіщень. Ви можете налаштувати повідомлення, вказавши відомості про компанію та контактні дані. Ви також можете включити правила окремо, щоб налаштувати методи, які відстежуються компонентами.
Microsoft Defender для кінцевої точки	Windows E5 отримують переваги від Microsoft Defender для кінцевої точки, корпоративної виявлення та нейтралізація атак на кінцеві точки, яка допомагає корпоративним командам безпеки виявляти, досліджувати та реагувати на складні загрози. Завдяки докладним даними про події та аналітичні відомості про атаки Defender для кінцевої точки дозволяє групі безпеки дослідити інциденти та ефективно та ефективно виконувати дії з виправлення. Defender для кінцевої точки також є частиною Microsoft 365 Defender, єдиного корпоративного набору засобів захисту до та після порушення безпеки, що спочатку координує виявлення, запобігання, дослідження та реагування на них між кінцевими точками, посвідченнями, електронною поштою та додатками для забезпечення інтегрованого захисту від складних атак.

Безпечне завантаження та довірене завантаження

Безпечне завантаження та довірене завантаження допомагають запобігти завантаженню шкідливих програм та пошкоджених компонентів при Windows 11 пристрою. Безпечне завантаження починається з початкового захисту під час завантаження, а потім довірене завантаження вибирає процес. Водночас безпечне завантаження та довірене завантаження допомагають забезпечити безпечне завантаження Windows 11 системи.

Безпечне завантаження

Першим кроком у захисті операційної системи є забезпечення безпечного завантаження після безпечного завершення початкових послідовностей завантаження обладнання та вбудованого програмного забезпечення. Безпечне завантаження забезпечує безпечний та надійний шлях із UEFI через послідовність надійного завантаження ядра Windows. Атаки шкідливих програм на послідовність завантаження Windows блокуються підтвердженнями застосування підписів у всій послідовності завантаження між середовищами UEFI, завантажувачем, ядром та додатками.

Коли комп'ютер починає процес завантаження, він спочатку перевіряє, чи підписано вбудоване програмне забезпечення цифровим підписом, що знижує ризик використання кореневих наборів вбудованого програмного забезпечення. Потім безпечне завантаження перевіряє весь код, що виконується до операційної системи, і перевіряє цифровий підпис завантажувача ОС, щоб переконатися, що вона є довіреною політикою безпечного завантаження і не була змінена.

Надійне завантаження

Довірене завантаження вибирає процес, який розпочався із безпечного завантаження. Завантажувач Windows перевіряє цифровий підпис ядра Windows перед завантаженням. Ядро Windows, у свою чергу, перевіряє всі інші компоненти процесу запуску Windows, у тому числі драйвери завантаження, файли запуску та драйвер антишкідливих програм для раннього запуску антишкідливих програм (ELAM). Якщо якийсь із цих файлів було змінено, завантажувач виявляє проблему та відхиляє завантаження пошкодженого компонента. Незаконна зміна або шкідливі програми в послідовності завантаження Windows блокуються підтвердженням застосування сигнатур між середовищами UEFI, завантажувачем, ядром та програмами.

Часто Windows може автоматично відновити пошкоджений компонент, відновлюючи цілісність Windows і дозволяючи Windows 11 нормально запускатися.

Шифрування та захист даних у Windows клієнті

Коли люди переміщуються разом зі своїми комп'ютерами та пристроями, їхня конфіденційна інформація передається разом з ними. Де конфіденційні дані не зберігаються, вони повинні бути захищені від несанкціонованого доступу, як шляхом крадіжки фізичного пристрою, так і з шкідливих додатків. Функції шифрування та захисту даних включають:

– Зашифрований жорсткий диск.
– BitLocker.

Зашифрований жорсткий диск

Зашифрований жорсткий диск використовує швидке шифрування, що надається шифруванням диска BitLocker, для підвищення безпеки даних та управління ними. Розвантаживши криптографічні операції на обладнання, зашифровані жорсткі диски збільшують продуктивність BitLocker та знижують завантаження ЦП та енергоспоживання. Оскільки зашифровані жорсткі диски

швидко шифрують дані, корпоративні пристрої можуть розширювати розгортання BitLocker із мінімальним впливом на продуктивність.

Зашифровані жорсткі диски надають такі можливості:

– Підвищена продуктивність: обладнання шифрування, інтегроване в контролер диска, дозволяє працювати з повною швидкістю передачі даних без зниження продуктивності.

– Надійна безпека на основі обладнання: шифрування завжди увімкнено, а ключі шифрування ніколи не залишають жорсткий диск. Перевірка автентифікації користувача виконується диском до його розблокування незалежно від операційної системи.

– Простота використання: шифрування є прозорим для користувача, і користувачеві не потрібно його увімкнути. Зашифровані жорсткі диски легко видаляються за допомогою локального ключа шифрування. не потрібно повторно шифрувати дані на диску.

– Низька вартість володіння: нова інфраструктура не потрібна для керування ключами шифрування, оскільки BitLocker використовує існуючу інфраструктуру для збереження відомостей про відновлення. Пристрій працює ефективніше, оскільки цикли процесора не потрібно використовувати для процесу шифрування.

Зашифровані жорсткі диски – це новий клас жорстких дисків, які самозашифруються на апаратному рівні та дозволяють повністю шифрувати обладнання на диску.

BitLocker

Шифрування диска BitLocker – це функція захисту даних, яка інтегрується в операційну систему та запобігає загрозі розкрадання даних або розкриття інформації на втрачених, вкрадених або неправильно виведених з експлуатації комп'ютерах.

BitLocker забезпечує шифрування операційної системи, фіксованих даних та знімних дисків даних за допомогою таких технологій, як апаратний інтерфейс тестування безпеки (HSTI), сучасний резервний сервер, безпечне завантаження UEFI та TPM.

Windows постійно покращує захист даних, покращуючи наявні параметри та надаючи нові стратегії.

Базові показники безпеки

Використання базових параметрів безпеки у вашій організації

Корпорація Майкрософт призначена для надання клієнтам безпечних операційних систем, таких як Windows та Windows Server, та безпечних програм, таких як програми Microsoft 365 для підприємств та Microsoft Edge. Крім гарантії безпеки своїх продуктів, Microsoft також дозволяє точно керувати середовищем за допомогою різних можливостей конфігурації.

Незважаючи на те, що в Windows і Windows Server реалізовані вбудовані засоби безпеки, багатьом організаціям все ж таки потрібен ретельніший контроль над конфігураціями безпеки. Для орієнтації в різних елементах управління

організаціям потрібні рекомендації щодо налаштування різних функцій безпеки. Microsoft надає такі рекомендації як базові параметри безпеки.

Рекомендується відмовитися від самостійного створення конфігурацій на користь розгортання поширених і ретельно протестованих стандартних конфігурацій, наприклад, базових параметрів безпеки Microsoft. Ця стандартна у галузі конфігурація допомагає підвищити гнучкість та знизити витрати.

Для отримання додаткових відомостей див. наступний запис блогу: «Використання добре відомих і перевірених рішень".

Що таке базові параметри безпеки?

Кожна організація стикається з загрозами безпеці. Однак типи загроз безпеці, які є найважливішими для однієї організації, можуть відрізнятися від інших. Наприклад, компанія електронної комерції може зосередитись на захисті своїх веб-додатків з виходом в Інтернет, а госпітал може зосередитися на захисті конфіденційної інформації про пацієнтів. Всі ці організації об'єднує одне: їм необхідно забезпечити безпеку своїх програм та пристроїв. Пристрої повинні відповідати стандартам (або базовим параметрам) безпеки, які визначаються організацією.

Базові показники безпеки – це група рекомендованих корпорацією Майкрософт параметрів конфігурації, яка пояснює їх вплив на безпеку. Ці параметри ґрунтуються на відгуках фахівців із забезпечення безпеки Microsoft, груп розвитку продуктів, партнерів та клієнтів.

Навіщо потрібні базові параметри безпеки?

Базові параметри безпеки надають користувачам важливі переваги, оскільки поєднують глибокі знання фахівців Microsoft, її партнерів і клієнтів.

Наприклад, існує більше 3000 параметрів групової політики для Windows 10, які не включають більше 1800 параметрів Internet Explorer 11. З цих 4800 параметрів лише деякі пов'язані з безпекою. Хоча Microsoft надає комплексні рекомендації щодо різних функцій безпеки, вивчення кожної з них може тривати багато часу. Вам доведеться самостійно визначити вплив кожного параметра на безпеку. Потім, як і раніше, необхідно визначити відповідне значення для кожного параметра.

У сучасних організаціях середовище загроз безпеки постійно розвивається, і IT-фахівці та розробники політик повинні стежити за загрозами безпеки та вносити необхідні зміни до параметрів безпеки для усунення цих загроз. Щоб прискорити розгортання та спростити керування продуктами Майкрософт, корпорація Майкрософт надає клієнтам базові показники безпеки, доступні в форматах, що споживаються, таких як резервне копіювання об'єктів групової політики.

Базові принципи

Наші рекомендації відповідають спрощеному та ефективному підходу до базових визначень. В основі цього підходу, за суттю, є:

– Базові показники призначені для добре керованих організацій з підтримкою безпеки, в яких стандартні кінцеві користувачі не мають прав адміністратора.

– Базовий план застосовує параметр лише в тому випадку, якщо він усуває загрозу безпеці та не викликає операційних проблем, які гірші, ніж ризики, які вони усувають.

– Базовий план застосовує значення за замовчуванням тільки в тому випадку, якщо авторизований користувач може задати небезпечний стан:

- Якщо користувач без права адміністратора може встановити небезпечний стан, встановіть значення за замовчуванням.
- Якщо для налаштування небезпечного стану потрібні права адміністратора, примусіть значення за замовчуванням лише в тому випадку, якщо неправильно сформований адміністратор в іншому випадку вибере неправильний вибір.

Як використовувати базові параметри безпеки?

Базові параметри безпеки можна використовувати таким чином:

– для забезпечення відповідності параметрам конфігурації користувачів та пристроїв;

– для налаштування параметрів конфігурації. Наприклад, можна використовувати групову політику, Microsoft Endpoint Configuration Manager або Microsoft Intune для налаштування пристрою з параметрами, вказаними в базовому плані.

Де можна отримати базові параметри безпеки?

Існує кілька способів отримання та використання базових показників безпеки:

1. Ви можете завантажити базові параметри безпеки з Центру завантаження Майкрософт. Ця сторінка завантаження призначена для набору засобів забезпечення відповідності вимогам безпеки (SCT), який включає засоби, які можуть допомогти адміністраторам управляти базовими показниками на додаток до базових показників безпеки. SCT також включає засоби управління базовими показниками безпеки. Ви також можете одержати підтримку базових показників безпеки.

2. Базові показники безпеки управління мобільними пристроями (MDM) функції, такі як базові показники безпеки на основі групової політики Майкрософт, можуть легко інтегрувати ці базові показники в існуючий засіб управління MDM.

3. Базові показники безпеки MDM можна легко налаштувати в Microsoft Endpoint Manager на пристроях під керуванням Windows 10 та Windows 11. Додаткові відомості див. у списку параметрів у базовому плані безпеки MDM Windows 10/11 у Intune.

Технічний посібник з VPN Для Windows

У цьому посібнику наведено покрокові інструкції щодо прийняття рішень для Windows 10 або Windows 11 клієнтів у корпоративному рішенні VPN та налаштуванні розгортання. Цей посібник посилається на постачальника служб конфігурації (CSP) VPNv2 і містить інструкції з налаштування керування мобільними пристроями (MDM) за допомогою Microsoft Intune та шаблону профілю VPN для Windows 10 та Windows 11.

Розділ	Опис
Типи підключень VPN	Виберіть VPN-клієнт та протокол тунелювання.
Рішення про маршрутизацію для VPN	Виберіть конфігурацію з розділенням тунелю або примусовим використанням тунелю.
Параметри автентифікації для VPN	Виберіть метод автентифікації EAP.
VPN та умовний доступ	Використовуйте оцінку політики Azure Active Directory для налаштування політик доступу для підключення VPN.
Дозвіл імен VPN	Визначте, як працюватиме роздільна здатність імен.
Параметри профілю VPN, що автоматично ініціюються.	Налаштуйте профіль VPN, щоб автоматично встановлювати підключення залежно від програми або імені, включати режим «Завжди увімкнено» та не активувати VPN у довірених мережах.
Функції безпеки VPN	Налаштування фільтрації трафіку, підключення профілю VPN до Windows Information Protection (WIP) тощо.
Параметри профілю VPN	Об'єднайте параметри в один профіль VPN за допомогою XML.

Брандмауер Windows Defender з розширеною безпекою

У цьому розділі наведено огляд функцій брандмауера Windows Defender (WFS) та протоколу IPsec.

Загальні відомості про брандмауер Windows Defender з розширеною безпекою

Брандмауер Захисника Windows у Windows 8, Windows 7, Windows Vista, Windows Server 2012, Windows Server 2008 та Windows Server 2008 R2 – це брандмауер вузла з відстеженням стану, який допомагає захистити пристрій, дозволяючи створювати правила, що визначають, який мережевий трафік може входити на пристрій із мережі та який мережевий трафік. пристрій може надсилатися до мережі. брандмауер Windows Defender також підтримує протокол IPsec, який можна використовувати для запиту автентифікації з будь-якого пристрою, який намагається зв'язатися з пристроєм. Якщо потрібна автентифікація, пристрої, які не можуть бути автентифіковані як довірені пристрої, не можуть взаємодіяти з пристроєм. За допомогою IPsec можна також вимагати шифрування певного мережевого трафіку,

Оснащення брандмауера Windows Defender MMC розширеної безпеки є більш гнучким і надає набагато більше функціональних можливостей, ніж користувальницький інтерфейс брандмауера Windows Defender на панелі керування. Обидва інтерфейси взаємодіють із однаковими базовими службами, але забезпечують різні рівні контролю над цими службами. Хоча програма брандмауер Windows Defender панель керування може захистити один пристрій у домашній середовищі, вона не надає достатньо централізованих функцій

управління або безпеки для захисту більш складного мережевого трафіку в типовому корпоративному середовищі.

Опис компонента

брандмауер Windows Update з розширеною безпекою є важливою частиною багаторівневої моделі безпеки. Забезпечуючи двонаправлену фільтрацію мережевого трафіку на основі вузла для пристрою, брандмауер Windows Defender блокує несанкціонований мережевий трафік, що входить до локального пристрою або виходить з нього. брандмауер Windows Defender також працює зі службою «Повідомлення про мережу", щоб вона використовувала параметри безпеки, які відповідають типам мереж, до яких підключено пристрій. брандмауер Windows Defender конфігурації IPsec інтегровані в одну консоль керування (MMC) з іменем брандмауер Windows Defender, тому брандмауер Windows Defender також є важливою частиною мережі. стратегії ізоляції.

Практичне застосування

Щоб вирішити проблеми з безпекою мережі, брандмауер Windows Defender надає такі переваги:

– **Знижує ризик погроз безпеки мережі.** брандмауер Windows Defender зменшує поверхню атаки пристрою, надаючи додатковий рівень для моделі глибинного захисту. Зменшення поверхні атаки пристрою підвищує керованість та знижує ймовірність успішної атаки.

– **Захищає конфіденційні дані та інтелектуальну власність.** Завдяки інтеграції з IPsec брандмауер Windows Defender надає простий спосіб примусового забезпечення наскрізного мережного зв'язку з автентифікацією. Він надає масштабований багаторівневий доступ до довірених мережних ресурсів, допомагаючи забезпечити цілісність даних та за бажанням допомагаючи захистити конфіденційність даних.

– **Розширює цінність наявних інвестицій.** Так брандмауер Windows Defender є брандмауером на основі вузла, який входить в операційну систему, іншого обладнання або програмного забезпечення не потрібно. Брандмауер Windows Defender також призначений для доповнення існуючих рішень для безпеки мережі, що не стосуються Майкрософт, за допомогою задокументованих програмних інтерфейсів (API).

Захист від вірусів та погроз

Захист від вірусів та погроз призначений для виявлення та блокування нових і виникаючих загроз. Завдяки хмарному та машинному навчанню антивірусна програма Microsoft Defender допоможе зупинити атаки в режимі реального часу.

– Автоматична служба пісочниці.
– Моніторинг поведінки.
– Захист на основі хмари.
– Машинне навчання.
– Захист URL-адрес.

Безпека додатків Windows

Кіберзлочинні регулярно отримують доступ до цінних даних шляхом злому додатків. Це може бути атака шляхом впровадження коду, коли зловмисники вставляють шкідливий код, який може змінювати дані або навіть знищувати його. Можливо, у програмі налаштована неправильна конфігурація безпеки, тому зловмисники можуть відчинити двері. Крім того, важливі відомості про клієнтів та корпоративні дані можуть залишити конфіденційні дані недоступними. Windows захищає цінні дані за допомогою рівнів безпеки програм.

Заходи безпеки	Функції та можливості
Керування програмами у програмі Windows Defender	Керування програмами – це один з найбільш ефективних елементів керування безпекою, які запобігають запуску небажаного або шкідливого коду. Він переходить від моделі довіри додатків, де передбачається, що весь код є надійним, модель, в якій програми повинні отримати довіру для виконання.
Application Guard в Microsoft Defender	Application Guard використовує апаратну ізоляцію на основі мікросхем для ізоляції недовірених веб-сайтів та ненадійних Office-файлів, безперешкодного запуску ненадійних веб-сайтів та файлів в ізольованому контейнері на основі Hyper-V, окремо від операційної системи робочого столу, та гарантує, що все, що відбувається у контейнері, залишається ізольованим від робочого столу.
Пісочниця Windows	Пісочниця Windows надає компактне середовище робочих столів для безпечного запуску програм в ізоляції. Програмне забезпечення, встановлене всередині середовища Пісочниці Windows, ізольовано від решти системи і працює незалежно від головного комп'ютера. Пісочниця є тимчасовою. При її закритті все програмне забезпечення, що знаходиться в ній, всі файли і дані про стан видаляються. При кожному відкритті програми ви отримуєте новий екземпляр пісочниці.
Безпека електронної пошти	Завдяки Windows безпеки електронної пошти S/MIME користувачі можуть шифрувати вихідні повідомлення та вкладення, щоб їх могли читати лише отримувачі з цифровою ідентифікацією (ідентифікатором), також званим сертифікатом. Користувачі можуть цифрово підписати повідомлення, яке перевіряє посвідчення відправника та гарантує, що повідомлення не було змінено.

Фільтр SmartScreen у Microsoft Defender	Фільтр SmartScreen у Microsoft Defender захищає від фішингових та шкідливих веб-сайтів та програм, а також від скачування потенційно небезпечних файлів.

Управління програмами у Windows Defender та захист цілісності коду на основі віртуалізації

Windows 10 включає набір технологій обладнання та ОС, які при спільному налаштуванні дозволяють підприємствам «блокувати» Windows 10 системи, щоб вони більшою мірою поводяться як мобільні пристрої. У цій конфігурації Захисник Windows application Control (WDAC) використовується для обмеження пристроїв на запуск лише затверджених програм, в той час як операційна система захищена від атак на пам'ять ядра за допомогою цілісності коду, захищеного гіпервізором (HVCI).

Політики WDAC та HVCI – це потужні засоби захисту, які можна використовувати окремо. Однак, якщо ці дві технології налаштовані для спільної роботи, вони мають надійний захист для Windows 10 пристроїв.

Використання Захисник Windows керування програмами для обмеження пристроїв лише авторизованими програмами має такі переваги в порівнянні з іншими рішеннями:

1. Політика WDAC застосовується до самого ядру Windows, і вона набирає чинності на ранніх етапах послідовності завантаження перед виконанням багатьох інших кодів ОС і до запуску традиційних антивірусних рішень.

2. WDAC дозволяє задати політику керування додатками для коду, який виконується в режимі користувача, драйверів обладнання та програмного забезпечення в режимі ядра, а також навіть коду, який виконується як частина Windows.

3. Клієнти можуть захистити політику WDAC навіть від незаконної зміни локального адміністратора, підписавши політику цифровим підписом. Для зміни підписаної політики потрібні права адміністратора та доступ до процесу цифрового підписування організації. Через це зловмиснику, зокрема користувачеві, якому вдалося отримати права адміністратора, важко змінити політику WDAC.

4. Ви можете захистити весь механізм примусового застосування WDAC за допомогою HVCI. Навіть якщо вразливість існує у коді режиму ядра, HVCI значно знижує ймовірність того, що зловмисник може успішно використовувати її. Це важливо, тому що зловмисник, який скомпрометує ядро, зазвичай може відключити більшість системних захисту, включаючи ті, які застосовуються WDAC або будь-яким іншим рішенням для керування програмами.

Керування програмами для Windows

Щодня створюються тисячі нових шкідливих файлів, тому використання традиційних методів, таких як антивірусні програми-визначення шкідливого коду на основі сигнатур з його подальшим усуненням-не забезпечує достатнього захисту від нових атак.

У більшості організацій інформація є найбільш цінним ресурсом, і дуже важливо переконатися, що доступом до цієї інформації мають лише затверджені користувачі. Однак, якщо користувач запускає процес, цей процес має той самий рівень доступу до даних, що й у користувача. В результаті конфіденційні відомості можуть бути легко видалені або передані за межі організації, якщо користувач навмисно або випадково запускає шкідливе ПЗ.

Керування програмами може допомогти усунути такі загрози безпеці, обмеживши програми, які можуть запускати користувачі, і код, що виконується в System Core (ядро). Політики керування програмами також можуть блокувати непідписані скрипти та msis та обмежувати Windows PowerShell для виконання в обмеженому мовному режимі.

Управління додатками – це ключова лінія захисту для захисту підприємств з урахуванням сучасних загроз, яка має перевагу в порівнянні з традиційними антивірусними рішеннями. Зокрема, керування додатками переходить від моделі довіри додатків, де всі додатки вважаються надійними, тоді як додатки повинні отримати довіру для запуску. Багато організацій, такі як Australian Signals Directorate, розуміють важливість управління програмами і часто називають управління програмами одним з найбільш ефективних способів усунення загрози виконуваних файлових шкідливих програм (.exe,.dll і т.д.).

Windows 10 і Windows 11 включають дві технології, які можна використовувати для керування програмами в залежності від конкретних сценаріїв та вимог вашої організації:

– Захисник Windows керування програмами (WDAC).
– AppLocker.

Огляд Application Guard у Microsoft Defender

Application Guard у Microsoft Defender (Application Guard) призначена для запобігання старим і новим атакам, щоб підтримувати продуктивність співробітників. За допомогою нашого унікального підходу до ізоляції обладнання наша мета полягає в тому, щоб знищити книгу відтворення, що використовується зловмисниками через те, що сучасні методи атаки застаріли.

Для Microsoft Edge application Guard допомагає ізолювати сайти, які не захищені корпоративними даними, захищаючи вашу компанію під час перегляду співробітниками Інтернету. Як адміністратор підприємства, ви визначаєте, які веб-сайти, хмарні ресурси та внутрішні мережі можна вважати довіреними. Усі елементи, які відсутні у списку, розцінюються як ненадійні. Якщо працівник відправляється на непорушний сайт через Microsoft Edge або Internet Explorer, Microsoft Edge відкриває сайт в ізольованому контейнері з Hyper-V увімкненою підтримкою.

Для Microsoft Office application Guard допомагає запобігти доступу до довірених ресурсів файлів Word, PowerPoint Excel і Excel. Application Guard відкриває ненав'язані файли в ізольованому Hyper-V із включеною підтримкою. Ізольований контейнер Hyper-V окремо від хост-операційної системи. Це ізолювання контейнера означає, що якщо непорушений сайт чи файл виявиться шкідливим, хост-пристрій захищений, а зловмисник не може отримати дані

підприємства. Ця концепція передбачає роботу ізольованого контейнера в анонімному режимі, тому зловмисник зможе отримати корпоративні облікові дані вашого співробітника.

Пісочниця Windows

Пісочниця Windows надає компактне середовище робочих столів для безпечного запуску програм в ізоляції. Програмне забезпечення, встановлене всередині Пісочниці Windows, ізольовано від решти системи і працює незалежно від головного комп'ютера.

Пісочниця є тимчасовою. При її закритті все програмне забезпечення, що знаходиться в ній, всі файли і дані про стан видаляються. При кожному відкритті програми ви отримуєте новий екземпляр пісочниці. Зверніть увагу, що починаючи з Windows 11 (складання 22509) ваші дані будуть зберігатися під час перезапуску, ініційованого з віртуалізованого середовища. Це зручно для встановлення програм, яким потрібне перезавантаження ОС.

Програмне забезпечення та програми, встановлені на головному комп'ютері, не є безпосередньо доступними у пісочниці. Якщо в середовищі Пісочниці Windows потрібні певні програми, їх необхідно явно встановити в цьому середовищі.

Пісочниця Windows має такі властивості:

– Це частина Windows: все, що потрібно для цієї функції, входить до операційних систем Windows 10 Pro та Windows 10 Корпоративна. Немає необхідності завантажувати VHD.

– Чиста система: під час кожного запуску Пісочниці Windows створюється новий екземпляр Windows.

– Одноразовість: на пристрої не зберігаються жодні дані. Коли користувач закриває цю програму, всі дані видаляються.

– Безпека: для ізоляції ядра використовується апаратна віртуалізація. Гіпервізор Майкрософт виконує окреме ядро, яке відокремлює Пісочницю Windows від комп'ютера.

– Ефективність: використовується інтегрований планувальник ядра, інтелектуальне керування пам'яттю та віртуальний ГП.

Налаштування S/MIME для Windows

S/MIME забезпечує додатковий рівень безпеки для пошти, що надсилається та отримує обліковий запис Exchange ActiveSync (EAS). S/MIME дозволяє користувачам шифрувати вихідні повідомлення та вкладення, щоб тільки передбачувані одержувачі, які мають цифрову ідентифікацію (ID), також відому як сертифікат, могли їх читати. Користувачі можуть створювати цифрові підписи для повідомлень, що забезпечує одержувачам можливість перевірити посвідчення відправника та переконатися в тому, що повідомлення не було несанкціоновано змінено.

Шифрування повідомлень

Користувачі можуть надсилати зашифровані повідомлення контактам у своїй організації та за її межами за наявності сертифікатів шифрування. Однак

користувачі, які використовують програму Mail for Windows, можуть зчитувати зашифровані повідомлення лише в тому випадку, якщо повідомлення отримано в обліковому записі Exchange і у них є відповідні ключі розшифровки.

Зашифровані повідомлення можуть прочитати лише отримувачі, які мають сертифікат. При спробі надіслати зашифроване повідомлення одержувачам, чий сертифікат шифрування недоступний, програма перед відправкою запропонує видалити одержувачам.

Цифрові підписи

Цифровий підпис повідомлення показує одержувачу, що повідомлення не було піддано несанкціонованій зміні та перевіряє посвідчення відправника. Отримувачі можуть перевірити цифровий підпис лише за умови використання клієнта електронної пошти з підтримкою S/MIME.

Шифрування та підписання окремих повідомлень

1. Під час створення повідомлення виберіть вкладку стрічки Параметри. На телефоні можна отримати доступ до параметрів, натиснувши багатокрапку (...).

2. Щоб підписати це повідомлення за допомогою цифрового підпису або зашифрувати його, використовуйте піктограми Підписати та Шифрувати відповідно.

Читання підписаних або зашифрованих повідомлень

Коли ви отримуєте зашифроване повідомлення, поштова програма перевіряє, чи є на вашому комп'ютері сертифікат. Якщо сертифікат доступний, під час відкриття повідомлення буде розшифровано. Якщо сертифікат зберігається на смарт-карті, вам буде запропоновано вставити смарт-картку, щоб прочитати повідомлення. Для доступу до сертифіката на смарт-картці також може знадобитися ПІН-код.

Встановлення сертифікатів із отриманого повідомлення

При отриманні підписаного повідомлення ел. пошти програма надає можливість встановлення на пристрій відповідного сертифіката шифрування, якщо такий сертифікат доступний. Цей сертифікат надалі можна використовувати для надсилання зашифрованої електронної пошти цій людині.

1. Відкрийте підписане повідомлення.

2. Торкніться піктограми цифрового підпису в області читання або натисніть.

3. Торкніться Встановити.

Windows посвідчення та конфіденційності

Зловмисники щодня запускають мільйони атак із паролями. Слабкі паролі, розпилення паролів та фішинг є точкою входу для багатьох атак. Знаючи, що потрібний користувач має доступ до правильного пристрою та потрібні дані, дуже важливо забезпечити безпеку та безпеку вашого бізнесу, сім'ї та себе. Windows Hello, Windows Hello для бізнесу та Credential Guard дозволяють клієнтам перейти на багатофакторну автентифікацію без пароля (MFA). MFA може знизити ризик компрометації в організаціях.

Можливості безпеки	Опис
Захист посвідчення користувача за допомогою Windows Hello	Windows Hello та Windows Hello для бізнесу замінити автентифікацію на основі пароля більш надійною моделлю автентифікації для входу на пристрій за допомогою секретного коду (ПІН-коду) або іншої біометричної автентифікації. Ця автентифікація на основі PIN-коду або біометричних даних дійсна лише на пристрої, на якому вона зареєстрована, і не може використовуватися на іншому пристрої. Додаткові відомості: Windows Hello для бізнесу
Credential Guard у Windows Defender та Remote Credential Guard	Credential Guard у Windows Defender допомагає захистити системи від методів крадіжки облікових даних (pass-the-hash або pass-the-ticket), а також допомагає запобігти доступу шкідливих програм до секретів системи, навіть якщо процес виконується з правами адміністратора. Захисник Windows Remote Credential Guard допомагає захистити облікові дані через підключення до віддаленого робочого стола шляхом перенаправлення запитів Kerberos назад на пристрій, що запитує підключення. Він також дає можливість єдиного входу для сеансів віддаленого робочого столу. Додаткові відомості: захист похідних облікових даних домену за допомогою програми Credential Guard у Захиснику Windows та захист облікових даних віддаленого робочого стола за допомогою Windows Remote Credential Guard
Альянс FIDO	Протоколи, визначені в Fast Identity Online (FIDO), стають відкритим стандартом для забезпечення надійної автентифікації, яка допомагає запобігти фішингу, а також зрозумілі і з урахуванням конфіденційності. Windows 11 підтримує вхід пристрою за допомогою ключів безпеки FIDO 2, а також Microsoft Edge або іншими сучасними браузерами підтримує використання захищених облікових даних на основі FIDO для захисту облікових записів користувачів. Докладніше про FIDO Alliance.

Microsoft Authenticator	Microsoft Authenticator є ідеальним компаньйоном для забезпечення безпеки за допомогою Windows 11. Це дозволяє легко і безпечно виконувати входи для всіх облікових записів в Інтернеті за допомогою багатофакторної автентифікації, входу на телефон без пароля або автозаповнення паролів. Крім того, у вас є додаткові параметри керування обліковими записами корпорації Майкрософт для особистих, робочих або навчальних облікових записів. Microsoft Authenticator можна використовувати для налаштування багатофакторної автентифікації для користувачів. Додаткові відомості: увімкнення входу без пароля за допомогою програми Microsoft Authenticator.
Смарт-картки	Смарт-картки – це стійкі до незаконного злому переносні пристрої зберігання, які можуть підвищити безпеку завдань у Windows, таких як автентифікація клієнтів, код підписування, захист електронної пошти та вхід за допомогою облікових записів Windows домену. Додаткові відомості про смарт-картки.
Контроль доступу	Керування доступом – це процес авторизації користувачів, груп та комп'ютерів для доступу до об'єктів та ресурсів у мережі або комп'ютері. Комп'ютери можуть керувати використанням системних та мережевих ресурсів за допомогою взаємопов'язаних механізмів автентифікації та авторизації. Додаткова інформація: контроль доступу.

Windows Hello для бізнесу

У Windows 10 Windows Hello для бізнесу замінює паролі суворою двофакторною автентифікацією на пристроях. У процесі автентифікації використовується новий тип облікових даних користувача, прив'язаних до пристрою, включаючи біометричні дані або ПІН-код.

Вхід із використанням біометричних даних

Windows Hello забезпечує надійну комплексну біометричну автентифікацію на основі розпізнавання облич або відбитків пальців. У Windows Hello використовується поєднання з особливих інфрачервоних (ІЧ)-камер та програмного забезпечення, що підвищує точність та захищає від спуфінгу. Провідні виробники обладнання постачають пристрої із вбудованими камерами, сумісними із Windows Hello. Обладнання для читання відбитків пальців можна використовувати або додавати на пристрої, на яких його немає. На пристроях, які підтримують Windows Hello, простий біометричний жест розблокує облікові дані користувачів.

– **Розпізнавання особи**. Це тип біометричної автентифікації, коли використовуються спеціальні камери, що зчитують дані в ІЧ-діапазоні, що дозволяє надійно відрізнити фотографію або відскановане зображення від живої

людини. Деякі виробники постачають зовнішні камери, в які вбудована така можливість, і більшість виробників ноутбуків також вбудовують цю функцію у свої пристрої.

– **Розпізнавання відбитків пальців**. Це тип біометричної автентифікації, коли використовується ємнісний датчик, скануючий відбитки пальців. Сканери відбитків пальців були доступні для комп'ютерів Windows протягом багатьох років, але поточне покоління датчиків є більш надійним і менш схильні до помилок. Більшість існуючих засобів читання відбитків пальців працюють Windows 10 і Windows 11, незалежно від того, чи вони зовнішні або інтегровані в ноутбуки або USB-клавіатури.

Біометричні дані, що використовуються для реалізації Windows Hello, надійно зберігаються у Windows лише на локальному пристрої. Біометричні дані не переміщуються та ніколи не відправляються на зовнішні пристрої або сервери. Так, Windows Hello дані біометричної ідентифікації зберігаються тільки на пристрої, немає єдиної точки збору, яку зловмисник може скомпрометувати для крадіжки біометричних даних. Для отримання додаткових відомостей про біометричну автентифікацію з Windows Hello для бізнесу див. Windows Hello біометричних даних на підприємстві.

Захист від крадіжки облікових даних у Windows

У цьому розділі пояснюється, як відбуваються атаки з крадіжкою облікових даних, а також стратегії та засоби протидії, які можна реалізувати для їх усунення на наступних етапах безпеки:

– Визначення ресурсомістких ресурсів із високою цінністю.
– Захист від відомих та невідомих погроз.
– Виявлення атак pass-the-hash та пов'язаних з ними атак.
– Реагування на підозрілі дії.
– Відновлення після пролому.

Атаки, які викрадають облікові дані

Дізнайтеся про різні типи атак, які використовуються для крадіжки облікових даних, і про фактори, які можуть призвести до ризику вашої організації. До типів атак належать:

– Передача ґешу.
– Kerberos передає квиток.
– Квиток Kerberos Golden Ticket та silver.
– Клавіатурні шпигуни.
– Сучасна дошка.

Стратегії захисту облікових даних

Ця частина посібника допоможе вам зрозуміти налаштування зловмисника з вказівкою того, як розставити пріоритети для високопріоритетних облікових записів та комп'ютерів. Ви дізнаєтесь, як створити архітектуру захисту від крадіжки облікових даних:

– Створення моделі зберігання для привілеїв облікового запису.
– Посилення захисту та обмеження адміністративних вузлів.
– Переконайтеся, що реалізовані конфігурації безпеки та рекомендації.

Технічні контрзаходи для крадіжки облікових даних

Цілі та очікувані результати розглядаються для кожного з цих лічильників:

– Використання Windows 10 Credential Guard.

– Обмеження та захист облікових записів домену з високим рівнем привілеїв.

– Обмеження та захист локальних облікових записів із правами адміністратора.

– Обмеження вхідного мережевого трафіку.

Також розглядаються багато інших контрзаходів, такі як використання Microsoft Passport та Windows Hello або багатофакторна автентифікація.

Виявлення атак з обліковими даними

У цих розділах описано, як виявити використання вкрадених облікових даних і як збирати події комп'ютера для виявлення крадіжки облікових даних.

Реагування на підозрілі дії

Ознайомтеся з рекомендаціями корпорації Майкрософт щодо реагування на інциденти, включаючи відновлення контролю скомпрометованих облікових записів, вивчення атак та відновлення пролому.

Захист витягнутих облікових даних домену за допомогою Credential Guard у Захиснику Windows

Вперше компонент Credential Guard у Windows Defender з'явився в Windows 10 Корпоративна та Windows Server 2016. Для захисту секретів він використовує засіб забезпечення безпеки на основі віртуалізації, щоб тільки привілейоване системне ПЗ могло отримувати доступ до цих даних. Несанкціонований доступ до секретів може призвести до атак, спрямованих на крадіжку облікових даних, наприклад Pass-the-Hash або Pass-The-Ticket. Credential Guard у Захиснику Windows запобігає цим атакам, захищаючи ґеш-коди паролів NTLM, квитки Kerberos Ticket Granting та облікові дані, що зберігаються в додатках як облікові дані домену.

Credential Guard у Windows Defender забезпечує перелічені нижче функції та рішення:

– **Апаратний захист** У NTLM, Kerberos та диспетчері облікових даних для захисту облікових даних використовуються функції забезпечення безпеки платформи, включаючи безпечне завантаження та віртуалізацію.

– **Засіб забезпечення безпеки на основі віртуалізації**. Облікові дані, витягнуті з Windows NTLM і Kerberos, та інші секрети виконуються в захищеному середовищі, яке ізольовано від операційної системи, що використовується.

– **Покращений захист від цілеспрямованих стійких загроз** Якщо для захисту облікових даних домену диспетчера облікових даних, а також облікових даних, вилучених з NTLM і Kerberos, використовується за допомогою засобу безпеки на основі віртуалізації, блокуються методи та засоби крадіжок облікових даних, які використовуються в багатьох цілеспрямованих атаках. Шкідливі програми, що працюють в операційній системі з правами адміністратора, не можуть отримати доступ до секретів, захищених за допомогою засобу безпеки

на основі віртуалізації. Хоча Credential Guard у Windows Defender є потужним засобом усунення загроз, постійні атаки збереженої загрози, швидше за все, будуть перемикання на нові методи атак, і вам також слід впровадити інші стратегії безпеки та архітектури.

Політика технічної підтримки для втрачених або забутих паролів

Облікові записи Майкрософт, операційна система Windows та інші продукти Microsoft містять паролі для захисту інформації. У цій статті наведено деякі параметри, які можна використовувати для скидання або відновлення пароля, якщо ви забули його. Якщо ці параметри не працюють, інженери служби підтримки Майкрософт не можуть допомогти вам отримати або обійти втрачений або забутий пароль.

Скидання пароля для облікового запису домену

Якщо ви втратите або забудете пароль для облікового запису домену, зверніться до IT-адміністратора або служби технічної підтримки. Щоб отримати додаткові відомості, див. Зміна або скидання пароля Windows.

Скидання пароля для облікового запису Майкрософт

Якщо ви втратите або забудете пароль для облікового запису Майкрософт, використовуйте майстер відновлення облікового запису.

Цей майстер просить ваші перевірки безпеки. Якщо ви забули свої перевірки безпеки або більше не маєте до них доступу, виберіть, що я **їх більше не має**. Після вибору цього параметра заповніть форму команди облікового запису Майкрософт. Вкажіть якнайбільше відомостей у цій формі. Команда облікових записів Майкрософт перевіряє відомості, які ви надаєте, щоб визначити, чи є власником облікового запису. Це остаточне рішення. Корпорація Майкрософт не впливає на вибір команди.

Скидання пароля для локального облікового запису на пристрої Windows

Локальні облікові записи на пристрої включають обліковий запис адміністратора пристрою.

Скидання пароля BIOS обладнання

Якщо ви втратите або забудете пароль для BIOS обладнання пристрою, зверніться за допомогою та підтримкою до виробника пристрою. Якщо ви дійсно зверталися до виробника через Інтернет, обов'язково відвідайте веб-сайт виробника, а не веб-сайт стороннього виробника.

Скидання пароля для окремого файлу

Деякі програми дозволяють захистити окремі файли паролем. Якщо ви втратите або забудете такий пароль, ви можете використовувати цю програму тільки для скидання або відновлення. Інженери служби підтримки Майкрософт не можуть допомогти вам скинути, вийняти або обійти такі паролі.

Використання сторонніх засобів введення паролів

Деякі сторонні компанії мають можливість обійти паролі, які були застосовані до файлів та функцій, які використовуються програмами Майкрософт. З юридичних причин ми не можемо рекомендувати чи

підтримувати будь-яку з цих компаній. Якщо вам потрібна допомога в обході або скиданні пароля, ви можете знайти та звернутися за допомогою до третьої сторони. Однак ви використовуєте такі сторонні продукти та служби на свій ризик.

Огляд керування доступом

У цьому розділі для IT-фахівців описується керування доступом у Windows, яке є процесом авторизації користувачів, груп та комп'ютерів для доступу до об'єктів у мережі або на комп'ютері. Основними поняттями, які є управління доступом, є дозволи, володіння об'єктами, наслідування дозволів, права користувача та аудит об'єктів.

Опис компонента

Комп'ютери з підтримуваною версією Windows можуть керувати використанням системних та мережевих ресурсів за допомогою взаємопов'язаних механізмів автентифікації та авторизації. Після автентифікації користувача операційна система Windows використовує вбудовані технології авторизації та контролю доступу для реалізації другого етапу захисту ресурсів: визначення того, чи користувач, що пройшов перевірку автентичності, правильні дозволи на доступ до ресурсу.

Загальні ресурси доступні користувачам та групам, крім власника ресурсу, та їх необхідно захистити від несанкціонованого використання. У моделі керування доступом користувачі та групи (також звані суб'єктами безпеки) представлені унікальними ідентифікаторами безпеки (SID). Їм призначаються права та дозволи, які повідомляють операційній системі, що може робити кожен користувач та група. Кожен ресурс має власника, який надає дозволи суб'єктам безпеки. Під час перевірки контролю доступу ці дозволи перевіряються, щоб визначити, які суб'єкти безпеки можуть отримати доступ до ресурсу та як вони можуть отримати доступ до нього.

Суб'єкти безпеки виконують дії (включаючи читання, запис, зміну або повний контроль) з об'єктами. До об'єктів належать файли, папки, принтери, розділи реєстру та доменні служби Active Directory (AD DS). Загальні ресурси використовують списки керування доступом (ACL) для призначення дозволів. Це дозволяє диспетчерам ресурсів застосовувати керування доступом такими способами:

– Заборона доступу неавторизованих користувачів та груп.

– Встановлення чітко визначених обмежень на доступ, наданий авторизованим користувачам та групам.

Власники об'єктів зазвичай надають дозволи групам безпеки, а не окремим користувачам. Користувачі та комп'ютери, додані до існуючих груп, передбачають дозволи цієї групи. Якщо об'єкт (наприклад, папка) може містити інші об'єкти (наприклад, вкладені папки та файли), він називається контейнером. В ієрархії об'єктів зв'язок між контейнером та його вмістом виражається посиланням на контейнер як батьківський. Об'єкт у контейнері називається дочірнім, і дочірній елемент успадковує параметри керування доступом

батьківського елемента. Власники об'єктів часто визначають дозвіл для об'єктів контейнерів, а не окремих дочірніх об'єктів, щоб спростити керування доступом.

Цей набір містить:

- Огляд динамічного контролю доступу.
- Ідентифікатори безпеки.
- Суб'єкти безпеки:
  - Локальні облікові записи.
  - Облікові записи Active Directory.
  - Облікові записи Майкрософт.
  - Облікові записи служби.
  - Групи безпеки Active Directory.

Практичне застосування

Адміністратори, які використовують підтримувану версію Windows, можуть уточнити програму та керування доступом до об'єктів та суб'єктів, щоб забезпечити наступну безпеку:

– Захистіть більшу кількість та різноманітність мережних ресурсів від неправильного використання.

– Підготовка користувачів до доступу до ресурсів відповідно до політик організації та вимог їх завдань.

– Надання користувачам доступу до ресурсів із різних пристроїв у різних розташуваннях.

– Регулярно оновлюйте доступ користувачів до ресурсів у міру зміни політик організації чи зміни завдань користувачів.

– З урахуванням зростаючого числа сценаріїв використання (таких як доступ з віддалених розташування або швидко розширюється безліч пристроїв, таких як планшетні комп'ютери і мобільні телефони).

– Виявляйте та усувайте проблеми з доступом, коли допустимі користувачі не можуть отримати доступ до ресурсів, необхідних для виконання своїх завдань.

Дозволи

Дозволи визначають тип доступу, який надається користувачеві або групі для об'єкта або властивості об'єкта. Наприклад, групі Finance можна надати дозволи на читання та запис файлу з ім'ям Payroll.dat.

За допомогою інтерфейсу керування доступом можна встановити дозволи NTFS для таких об'єктів, як файли, об'єкти Active Directory, об'єкти реєстру або системні об'єкти, такі як процеси. Дозволи можуть бути надані будь-якому користувачеві, групі чи комп'ютеру. Рекомендується призначати дозволи групам, оскільки це підвищує продуктивність системи під час перевірки доступу до об'єкта.

Для будь-якого об'єкта можна надати дозволи на:

– Групи, користувачі та інші об'єкти з ідентифікаторами безпеки у домені.

– Групи та користувачі в цьому домені та всі довірені домени.

– Локальні групи та користувачі на комп'ютері, де знаходиться об'єкт.

Дозволи, підключені до об'єкта, залежать від типу об'єкта. Наприклад, дозволи, які можна вкласти у файл, відрізняються від дозволів, які можна вкласти

до розділу реєстру. Однак, деякі дозволи є спільними для більшості типів об'єктів. Нижче наведено поширені дозволи.

– Прочитайте.
– Змінити.
– Зміна власника.
– Видалити.

Під час встановлення дозволів вказується рівень доступу для груп та користувачів. Наприклад, можна дозволити одному користувачу зчитувати вміст файлу, дозволити іншому користувачеві вносити зміни до файлу та заборонити іншим користувачам доступ до файлу. Ви можете задати аналогічні дозволи на принтерах, щоб певні користувачі могли налаштовувати принтер, а інші користувачі могли лише друкувати.

Якщо потрібно змінити дозволи для файлу, можна запустити провідник Windows, клацнути правою кнопкою миші ім'я файлу та натиснути кнопку «**Властивості"**. На **вкладці «** Безпека» можна змінити дозволи для файлу. Щоб отримати додаткові відомості, див. Управління роздільною здатністю.

Володіння об'єктами

Власник призначається об'єкту під час його створення. За замовчуванням власником об'єкта є власник. Незалежно від дозволу об'єкта, власник об'єкта завжди може змінити дозволи. Щоб отримати додаткові відомості, див. Управління володінням об'єктом.

Наслідування дозволів

Спадкування дозволяє адміністраторам легко призначати дозволи та керувати ними. Ця функція автоматично призводить до того, що об'єкти в контейнері успадковують всі дозволи цього контейнера. Наприклад, файли в папці успадковують роздільну здатність папки. Наслідуються лише дозволи, позначені для наслідування.

Права користувача

Права користувача надають певні привілеї та права входу користувачам та групам у обчислювальному середовищі. Адміністратори можуть призначати певні права на облікові записи груп або окремі облікові записи користувачів. Ці права дозволяють користувачам виконувати певні дії, такі як вхід до системи в інтерактивному режимі або резервне копіювання файлів та каталогів.

Права користувача відрізняються від дозволів, оскільки права користувача застосовуються до облікових записів користувачів, а дозволи пов'язані з об'єктами. Хоча права користувачів можуть застосовуватися до окремих облікових записів користувачів, права користувачів найкраще адмініструвати на основі облікового запису групи. У інтерфейсі керування доступом користувача не підтримується надання прав користувача. Однак призначення прав користувача можна адмініструвати за допомогою **локальних параметрів безпеки**.

Для отримання додаткових відомостей про права користувачів див. розділ «Призначення прав користувача".

Аудит об'єктів

З правами адміністратора можна виконувати аудит успішного чи невдалого доступу користувачів до об'єктів. Ви можете вибрати, який об'єкт має доступ до аудиту, за допомогою інтерфейсу управління доступом, але спочатку необхідно включити політику **** аудиту, вибравши «Аудит доступу до об'єкта» в розділі «Локальні політики» в локальних параметрах безпеки. Потім ці події, пов'язані з безпекою, можна переглянути в журналі безпеки Перегляд подій.

Технічний довідник смарт-карт

Що таке смарт-картки?

Смарт-картки – це стійкі до незаконного злому переносні пристрої зберігання, які можуть підвищити безпеку таких завдань, як перевірка справжності клієнтів, підписування коду, захист електронної пошти та вхід за допомогою облікового запису домену Windows.

Смарт-картки надають:

– Захищене від незаконної зміни сховище для захисту закритих ключів та інших форм персональних даних.

– Ізоляція критично важливих для безпеки обчислень, які включають автентифікацію, цифрові підписи та обмін ключами з інших частин комп'ютера. Ці обчислення виконуються на смарт-картці.

– Перенесення облікових даних та іншої конфіденційної інформації між комп'ютерами на роботі, вдома або в дорозі.

Смарт-картки можна використовувати лише для входу до облікових записів домену, а не для локальних облікових записів. При використанні пароля для інтерактивного входу в обліковий запис домену Windows використовує протокол Kerberos версії 5 (v5) для автентифікації. Якщо ви використовуєте смарт-карту, операційна система використовує автентифікацію Kerberos версії 5 з сертифікатами X.509 v3.

Віртуальні смарт-картки з'явилися у Windows Server 2012 та Windows 8, щоб усунути необхідність у фізичній смарт-картці, засобі читання смарт-карток та пов'язаному адмініструванні цього обладнання. Відомості про віртуальні смарт-карти див. у розділі «Загальні відомості про віртуальні смарт-картки".

Windows та хмарна безпека

Сучасні співробітники мають більшу свободу і мобільність, ніж будь-коли раніше. Зі збільшенням впровадження корпоративної хмари, збільшенням використання особистих додатків та збільшенням використання сторонніх додатків ризик уразливості даних є найвищим. Увімкнення Zero-Trust захисту Windows 11 працює з хмарними службами Майкрософт. Windows та хмарні служби допомагають організаціям посилити інфраструктуру безпеки в декількох хмарах, захистити гібридні хмарні робочі навантаження та захистити конфіденційну інформацію, контролюючи доступ та усуваючи загрози.

Windows 11 включає хмарні служби, перелічені в наступній таблиці:

Тип служби	Опис
Управління мобільними пристроями (MDM) та Microsoft Endpoint Manager	Windows 11 підтримує MDM, рішення для управління підприємством, допомагаючи керувати політиками безпеки та бізнес-додатками вашої організації. MDM дозволяє групі безпеки керувати пристроями, не порушуючи конфіденційність користувачів на власних пристроях. Сервери сторонніх розробників можна використовувати для керування Windows 11 за допомогою стандартних галузевих протоколів.
Обліковий запис Майкрософт	Коли користувачі додають обліковий запис Microsoft у Windows 11, вони можуть переносити Windows, Microsoft Edge, Xbox, вибрані веб-сторінки, файли, фотографії та ін. на своїх пристроях. Обліковий запис Microsoft дозволяє користувачам керувати всім в одному місці. Вони можуть зберігати вкладки у своїх підписках та журналі замовлень, впорядковувати цифрове життя сім'ї, оновлювати параметри конфіденційності та безпеки, відстежувати працездатність та безпеку своїх пристроїв та навіть отримувати винагороди.
OneDrive	OneDrive – це інтернет-сховище для файлів, фотографій та даних. OneDrive забезпечує додаткову безпеку, резервне копіювання та відновлення важливих файлів та фотографій. За допомогою особистих та бізнес-рішень користувачі можуть використовувати OneDrive для зберігання та захисту файлів у хмарі, дозволяючи користувачам працювати на ноутбуках, настільних комп'ютерах та мобільних пристроях. Якщо пристрій втрачено або викрадено, користувачі можуть швидко відновити всі важливі файли, фотографії та дані. Особистий OneDrive також забезпечує захист найбільш конфіденційних файлів без втрати зручності доступу будь-де. Файли захищені за допомогою автентифікації, але легко доступні користувачам на їхніх пристроях. Дізнайтеся, як налаштувати Особистий сейф. У разі атаки програми-шантажиста OneDrive можливість відновлення. Якщо ви налаштуєте резервне копіювання в OneDrive, у вас буде більше можливостей для усунення та відновлення після атаки програми-шантажиста.

Доступ до Azure Active Directory	Microsoft Azure Active Directory (Azure AD) – це повне хмарне рішення для керування посвідченнями та каталогами, забезпечення доступу до програм та захисту посвідчень від загроз безпеки. Використовуючи Azure AD, ви можете керувати посвідченнями та захищати посвідчення для співробітників, партнерів та клієнтів для доступу до потрібних програм та служб. Windows 11 з Azure Active Directory забезпечує безпечний доступ, керування посвідченнями та єдиний вхід до програм та служб з будь-якого місця.

Управління мобільними пристроями

Дізнайтеся, як реєструвати пристрої Windows та керувати політиками безпеки компанії та бізнес-програмами.

Azure Active Directory

Захищений адаптивний доступ

Захистіть доступ до ресурсів і даних завдяки надійній автентифікації та політиці адаптивного доступу на основі ризиків, не впливаючи на роботу користувачів.

Зручна взаємодія з користувачем

Забезпечте простий і швидкий вхід у своє багатохмарне середовище, щоб підвищити продуктивність користувачів, а також зменшити витрати часу на керування паролями.

Комплексне керування ідентичностями

Керуйте ідентичностями й забезпечуйте доступ до локальних і хмарних програм у центральному розташуванні, щоб покращити видимість та контроль.

Спрощене керування ідентичностями

Ефективно керуйте доступом до програм і даних усіх користувачів та адміністраторів за допомогою автоматичних засобів керування ідентичностями, щоб гарантувати доступ лише авторизованим користувачам.

Облікові записи Майкрософт

Сайти, служби, властивості та комп'ютери Майкрософт, які працюють у Windows 10, можуть використовувати обліковий запис Майкрософт як засіб ідентифікації користувача. Раніше обліковий запис Майкрософт називався Windows Live ID. Він містить секрети, що визначаються користувачем, і складається з унікальної адреси електронної пошти та пароля.

Коли користувач входить за допомогою облікового запису Майкрософт, пристрій підключено до служб хмар. Багато параметрів, переваг та програм користувача можна спільно використовувати на різних пристроях.

Як працює обліковий запис Майкрософт

Обліковий запис Microsoft дозволяє користувачам входити на веб-сайти, які підтримують цю службу, за допомогою одного набору облікових даних.

Облікові дані користувачів перевіряються сервером автентифікації облікового запису Майкрософт, пов'язаним із веб-сайтом. Microsoft Store є прикладом зв'язку. Коли нові користувачі входять на веб-сайти, для яких можна використовувати облікові записи Майкрософт, вони надсилаються на найближчий сервер автентифікації, який запитує ім'я користувача та пароль. Windows використовує постачальник підтримки безпеки Schannel для відкриття підключення tls/SSL для цієї функції. Користувачі можуть використовувати диспетчер облікових даних для зберігання облікових даних.

Коли користувачі входять на веб-сайти, для яких дозволено використовувати обліковий запис Майкрософт, на своїх комп'ютерах встановлюється обмежений за часом файл cookie, який включає потрійний тег зашифрованого ідентифікатора DES. Цей зашифрований тег ідентифікатора був узгоджений між сервером автентифікації та веб-сайтом. Цей тег ідентифікатора надсилається на веб-сайт, і веб-сайт встановить ще один обмежений зашифрований HTTP-файл cookie на комп'ютері користувача. Якщо ці файли cookie дійсні, користувачам не потрібно вказати ім'я користувача та пароль. Якщо користувач активно виходить з облікового запису Microsoft, ці файли cookie видаляються.

Створення облікових записів Майкрософт

Щоб запобігти шахрайству, система Майкрософт перевіряє IP-адресу під час створення облікового запису користувачем. Користувач, який намагається створити кілька облікових записів Майкрософт з однаковою IP-адресою, зупиняється. Облікові записи Майкрософт не призначені для створення пакетів, наприклад, для групи користувачів домену у вашій організації.

Існує два способи створення облікового запису Майкрософт:

– **Використовуйте існуючу адресу електронної пошти**. Користувачі можуть використовувати дійсні адреси електронної пошти для реєстрації облікових записів корпорації Майкрософт. Служба перетворює адресу електронної пошти запитувача на обліковий запис Майкрософт. Користувачі також можуть вибирати свої особисті паролі.

– **Зареєструйтесь, щоб отримати адресу електронної пошти Майкрософт**. Користувачі можуть зареєструватися для отримання облікового запису електронної пошти за допомогою служб веб-пошти Майкрософт. Цей обліковий запис можна використовувати для входу на веб-сайти, які включені для використання облікових записів корпорації Майкрософт.

Захист інформації про обліковий запис Майкрософт

Облікові дані шифруються двічі. Перше шифрування ґрунтується на паролі облікового запису. Облікові дані шифруються знову під час їх надсилання через Інтернет. Збережені дані недоступні для інших служб Майкрософт або інших служб.

– **Необхідний надійний пароль**. Не можна використовувати порожні паролі. Щоб отримати додаткові відомості, див. розділ Як забезпечити безпеку та безпеку облікового запису Майкрософт.

– **Потрібне додаткове підтвердження особистості**. Перш ніж отримати доступ до інформації та параметрів профілю користувача на другому

підтримуваному комп'ютері Windows вперше, необхідно встановити довіру для цього пристрою, надавши додаткове підтвердження особи. Це можна зробити, надавши Windows код, який надсилається на номер мобільного телефону або дотримуючись інструкцій, надісланих на альтернативну адресу електронної пошти, вказану користувачем у параметрах облікового запису.

– **Усі дані профілю користувача шифруються на клієнті перед передачею в хмару**. За замовчуванням дані користувача не переміщуються бездротовою широкою мережею (WWAN), таким чином захищаючи дані профілю. Усі дані та параметри, що залишають пристрій, передаються через протокол TLS/SSL.

Відомості про безпеку облікового запису Майкрософт

Користувачі можуть додавати відомості про безпеку до облікових записів Майкрософт через інтерфейс **облікових записів** на комп'ютерах під керуванням підтримуваних версій Windows. Ця функція дозволяє користувачеві оновлювати інформацію про безпеку, надані під час створення облікових записів. Ці відомості про безпеку включають альтернативну адресу електронної пошти або номер телефону, тому якщо пароль скомпрометований або забутий, можна надіслати код перевірки для перевірки їхньої особи. Користувачі можуть використовувати свої облікові записи Майкрософт для зберігання корпоративних даних в особистому програмі OneDrive або поштовій програмі, тому власнику облікового запису безпечно зберігати ці відомості про безпеку в актуальному стані.

Обліковий запис Майкрософт для підприємства

Хоча обліковий запис Майкрософт призначений для обслуговування споживачів, ви можете знайти ситуації, коли користувачі домену можуть скористатися своїм особистим обліковим записом Майкрософт у вашій організації. У цьому списку описані деякі переваги.

– **Завантажте програми Microsoft Store**. Якщо ваше підприємство вирішить розповсюджувати програмне забезпечення через Microsoft Store, користувачі можуть використовувати свої облікові записи Майкрософт для завантаження та використання на п'яти пристроях з будь-якою версією Windows 10, Windows 8.1, Windows 8 або Windows RT.

– **Єдиний вхід**. Користувачі можуть використовувати облікові дані облікового запису Microsoft для входу на пристрої під керуванням Windows 10, Windows 8.1, Windows 8 або Windows RT. При цьому Windows працює з програмою Microsoft Store, щоб забезпечити для них можливості, що пройшли автентифікацію. Користувачі можуть зв'язати обліковий запис Майкрософт з обліковими даними для входу до програм або веб-сайтів Microsoft Store, щоб ці облікові дані переміщувалися на всіх пристроях із підтримуваними версіями.

– **Синхронізація персоналізованих параметрів**. Користувачі можуть зв'язати параметри операційної системи, які найчастіше використовуються, з обліковим записом Майкрософт. Ці параметри доступні щоразу, коли користувач входить з цим обліковим записом на будь-якому пристрої під керуванням підтримуваної версії Windows і підключений до хмари. Після входу

користувача пристрій автоматично намагається отримати параметри користувача з хмари та застосувати їх до пристрою.

– **Синхронізація програм**. Програми Microsoft Store можуть зберігати настройки користувача, щоб ці параметри були доступні для будь-якого пристрою. Як і у випадку з параметрами операційної системи, ці параметри програми для конкретних користувачів доступні при кожному вході користувача з тим же обліковим записом Майкрософт на будь-якому пристрої, на якому запущено підтримувану версію Windows і підключено до хмари. Після входу користувача цей пристрій автоматично завантажує настройки з хмари та застосовує їх під час встановлення програми.

– **Інтегровані служби соціальних мереж**. Контактні дані та статус друзів та партнерів користувачів автоматично залишаються актуальними на таких сайтах, як Hotmail, Outlook, Facebook, Twitter та LinkedIn. Користувачі також можуть отримувати доступ до фотографій, документів та інших файлів з таких сайтів, як OneDrive, Facebook та Flickr.

Керування обліковим записом Майкрософт у домені

Залежно від IT-моделей та бізнес-моделей, використання облікових записів Майкрософт у вашій організації може ускладнювати або надавати рішення. Перш ніж дозволити використання цих типів облікових записів в організації, слід враховувати такі рекомендації:

– Обмеження використання облікового запису Майкрософт.
– Налаштування підключених облікових записів.
– Підготовка облікових записів Майкрософт в організації.
– Аудит дій облікового запису.
– Виконання скидання пароля.
– Обмеження встановлення та використання додатків.

Обмеження використання облікового запису Майкрософт

Наступні параметри групової політики допомагають керувати використанням облікових записів Майкрософт в організації:

– Блокування автентифікації користувача облікового запису Майкрософт для всіх споживачів.
– Облікові записи: блокування облікових записів Майкрософт.

Блокування автентифікації користувача облікового запису Майкрософт для всіх споживачів

Цей параметр визначає, чи користувачі можуть надавати облікові записи Майкрософт для автентифікації для програм або служб.

Якщо цей параметр увімкнено, всі програми та служби на пристрої заборонено використовувати облікові записи Майкрософт для автентифікації. Це стосується як існуючих користувачів пристрою, так і нових користувачів, які можуть бути додані.

Однак будь-яка програма або служба, що вже пройшли автентифікацію користувача, не будуть порушені включенням цього параметра до закінчення терміну дії кеша автентифікації. Рекомендовано увімкнути цей параметр перед тим, як будь-який користувач увійде на пристрій, щоб запобігти появі кешованих маркерів.

Якщо цей параметр вимкнено або не налаштовано, програми та служби можуть використовувати облікові записи Майкрософт для автентифікації. Цей **параметр вимкнено за** замовчуванням.

Цей параметр не впливає на можливість входу користувачів на пристрої за допомогою облікових записів Майкрософт або надання облікових записів Майкрософт через браузер для перевірки автентичності за допомогою веб-застосунків.

Шлях до цього параметра: Конфігурація комп'ютера\Адміністративні шаблони\Компоненти Windows\обліковий запис Майкрософт.

Облікові записи: блокування облікових записів Майкрософт

Цей параметр забороняє використання програми «**Параметри** « для додавання облікового запису Майкрософт для автентифікації єдиного входу для служб Майкрософт та деяких фонових служб або використання облікового запису Майкрософт для єдиного входу до інших програм або служб.

Якщо цей параметр увімкнено, існує два варіанти5

– **Користувачі не можуть додавати облікові записи Майкрософт**. Існуючі підключені облікові записи, як і раніше, можуть входити на пристрій (і відображатися на екрані входу). Однак користувачі не можуть використовувати програму «**Параметри»** для додавання нових підключених облікових записів або підключення локальних облікових записів до облікових записів Майкрософт.

– **Користувачі не можуть додавати або виконувати вхід за допомогою облікових записів Майкрософт**. Користувачі не можуть додавати нові підключені облікові записи (або підключати локальні облікові записи до облікових записів корпорації Майкрософт) або використовувати існуючі підключені облікові записи за допомогою **параметрів**.

Цей параметр не впливає на додавання облікового запису Microsoft для автентифікації програми. Наприклад, якщо цей параметр увімкнено, користувач, як і раніше, може надати обліковий запис Майкрософт для автентифікації за допомогою програми **Пошта**, але користувач не може використовувати обліковий запис Майкрософт для автентифікації єдиного входу для інших програм або служб (іншими словами, користувачеві буде запропоновано пройти автентифікацію для інших програм або служб).

Цей параметр **не визначено** за замовчуванням.

Шлях до цього параметра: Конфігурація комп'ютера\Параметри Windows\Параметри безпеки\Локальні політики\Параметри безпеки.

Налаштування підключених облікових записів

Користувачі можуть підключити обліковий запис Майкрософт до свого облікового запису домену та синхронізувати установки та налаштування між ними. Це дозволяє користувачам переглядати той самий фон робочого стола, параметри програми, журнал браузера та вибране, а також інші параметри облікового запису Майкрософт на інших пристроях.

Користувачі можуть вимкнути обліковий запис Майкрософт від облікового запису домену в будь-який час таким чином: у **параметрах комп'ютера** торкніться або клацніть **Користувачі**, торкніться або натисніть кнопку «**Вимкнути** «, а потім натисніть кнопку «**Готово** «.

Підготовка облікових записів Майкрософт в організації

Облікові записи Майкрософт – це приватні облікові записи користувачів. Корпорація Майкрософт не надає жодних методів підготовки облікових записів Майкрософт для підприємства. Підприємства повинні використовувати облікові записи домену.

Аудит дій облікового запису

Оскільки облікові записи Майкрософт знаходяться в Інтернеті, Windows не має механізму аудиту їх використання, доки обліковий запис не буде пов'язаний з обліковим записом домену. Але цей зв'язок не обмежує користувача від вимкнення облікового запису або від'єднання від домену. Неможливо перевірити активність облікових записів, які не пов'язані з вашим доменом.

Виконання скидання пароля

Тільки власник облікового запису Microsoft може змінити пароль. Паролі можна змінити на порталі входу до облікового запису Майкрософт.

Обмеження встановлення та використання додатків

В організації можна налаштувати політики керування програмами для регулювання установки та використання програм для облікових записів Майкрософт. Для отримання додаткових відомостей див. AppLocker та упаковані програми та правила інсталятора упакованих програм AppLocker.

OneDrive

Допомагає користувачам в організації зберігати, синхронізувати та обмінюватися файлами в Microsoft 365.

Параметри для сім'ї

У розділі **Параметри для сім'ї** містяться посилання на параметри та подальша інформація для батьків щодо комп'ютера з Windows 10. Він не призначений для корпоративних чи бізнес-середовищ. У Windows 10 версії 1709 цей розділ можна приховати від користувачів комп'ютера. Цей параметр може бути корисним, якщо ви не бажаєте, щоб співробітники вашої організації могли бачити або мати доступ до цього розділу.

Основи безпеки Windows

Корпорація Майкрософт прагне постійно інвестувати у покращення процесу розробки програмного забезпечення, створення програмного забезпечення з високим рівнем безпеки та відповідність вимогам безпеки. Корпорація Майкрософт впроваджує рекомендації щодо безпеки та конфіденційності на ранніх етапах життєвого циклу всіх процесів розробки програмного забезпечення. Ми створимо безпеку з нуля для ефективного захисту у середовищі загроз.

Наша надійна основа безпеки використовує життєвий цикл розробки помилок (SDL) Майкрософт, підтримку стандартів та сертифікатів безпеки продуктів, а також підписування коду Azure. В результаті ми покращуємо безпеку, створивши програмне забезпечення з меншою кількістю дефектів та вразливостей, а не застосовуючи оновлення після виявлення вразливостей.

Додаткові відомості про основи безпеки див. у наступній таблиці:

Концепція	Опис
Перевірка FIPS 140-2	Публікація 140-2 федерального стандарту обробки інформації (FIPS) є стандартом державних організацій США. FIPS засновано на розділі 5131 в Акті 1996 року про структуру управління інформаційними технологіями. Він визначає мінімальні вимоги безпеки для криптографічних модулів в IT-продуктах. Корпорація Майкрософт активно виконує зобов'язання щодо забезпечення відповідності вимогам стандарту FIPS 140-2, перевіряючи криптографічні модулі з моменту його першого створення у 2001 році.
Загальні критерії сертифікації	Корпорація Майкрософт підтримує програму сертифікації загальних критеріїв, гарантує, що продукти включають функції та функції, необхідні для відповідних профілів захисту загальних критеріїв, та завершує сертифікацію загальних критеріїв продуктів Microsoft Windows.
Життєвий цикл розробки захищених програм (Майкрософт)	Життєвий цикл розробки безпеки (SDL) – це процес забезпечення безпеки, орієнтований на розробку програмного забезпечення. SDL відіграє важливу роль у впровадженні безпеки та конфіденційності програмного забезпечення та мови та регіональних параметрів корпорації Майкрософт..
Програма Microsoft Bug Bounty	Якщо ви виявите вразливість у продукті, службі або пристрої Майкрософт, ми хочемо дізнатися від вас! Якщо звіт про вразливість впливає на продукт або службу в рамках однієї з наших програм, наведених нижче, ви можете отримати нагороду відповідно до опису програми.

Життєвий цикл розробки захищених програм (Майкрософт)

Життєвий цикл розробки безпеки (SDL) – це процес забезпечення безпеки, орієнтований на розробку програмного забезпечення. Починаючи з 2004 року, SDL є ініціативою корпорації Майкрософт та обов'язковою політикою, яка відіграє важливу роль у впровадженні безпеки та конфіденційності у програмне забезпечення та мову та регіональні параметри корпорації Майкрософт. Завдяки поєднанню цілісного та практичного підходу SDL покликаний зменшити кількість та серйозність уразливостей у програмному забезпеченні. SDL забезпечує безпеку та конфіденційність на всіх етапах процесу розробки.

Программа Microsoft Bug Bounty

Ви дослідник безпеки? Ви знайшли вразливість у продукті, службі або пристрої Майкрософт? Якщо так, то ми хочемо почути від вас!

Якщо звіт про вразливість впливає на продукт або службу, яка знаходиться в межах однієї з наших програм щедрості, ви можете отримати нагороду відповідно до описів програми.

Загальні критерії сертифікації

Корпорація Майкрософт прагне оптимізувати безпеку своїх продуктів та служб. У рамках цього зобов'язання корпорація Майкрософт підтримує програму сертифікації загальних критеріїв, гарантує, що продукти включають функції та функції, необхідні для відповідних профілів захисту загальних критеріїв, та завершує сертифікацію загальних критеріїв продуктів Microsoft Windows.

Перевірка FIPS 140-2

Огляд стандарту FIPS 140-2

Публікація 140-2 федерального стандарту обробки інформації (FIPS) є стандартом державних організацій США. FIPS засновано на розділі 5131 в Акті 1996 року про структуру управління інформаційними технологіями. Він визначає мінімальні вимоги безпеки для криптографічних модулів в IT-продуктах. Програма перевірки криптографічного модуля (CMVP) – це спільна робота Національного інституту стандартів та технологій США (NIST) та Центру кібербезпеки Канади (CCCS). Він перевіряє криптографічні модулі на відповідність вимогам безпеки для криптографічних модулів (частина FIPS 140-2) та пов'язаним стандартам шифрування FIPS. Вимоги до безпеки FIPS 140-2 охоплюють 11 областей, пов'язаних із проектуванням та реалізацією криптографічного модуля. Бібліотека інформаційних технологій NIST управляє пов'язаною програмою, яка перевіряє затверджені FIPS алгоритми шифрування в модулі.

Підхід корпорації Майкрософт до перевірки FIPS 140-2

Корпорація Майкрософт активно виконує зобов'язання щодо забезпечення відповідності вимогам стандарту FIPS 140-2, перевіряючи криптографічні модулі з моменту його першого створення у 2001 році. Корпорація Майкрософт перевіряє свої криптографічні модулі NIST CMVP, як описано вище. Ці криптографічні модулі використовують кілька продуктів Майкрософт, включаючи Windows 10, Windows Server та багато хмарних служб.

Використання Windows у затвердженому режимі роботи FIPS 140-2

Windows 10 і Windows Server можна налаштувати для роботи в затвердженому режимі FIPS 140-2, який зазвичай називають режимом FIPS. Якщо ви увімкнете режим FIPS, модулі бібліотеки примітивів шифрування (bcryptprimitives.dll) та бібліотеки примітивів шифрування режиму ядра (CNG.sys) будуть виконувати самообробку перед виконанням криптографічних операцій Windows. Ці самообслуговування виконуються відповідно до розділу 4.9 FIPS 140-2. Вони гарантують правильну роботу модулів.

Бібліотека криптографічних примітивів та бібліотека криптографічних примітивів режиму ядра є єдиними модулями, які торкнулися режиму FIPS. Режим FIPS не завадить Windows та його підсистемам з використанням алгоритмів шифрування, не перевірених FIPS. FIPS – це просто поради для програм або компонентів, відмінних від бібліотеки криптографічних примітивів та бібліотеки криптографічних примітивів режиму ядра.

У державних установах США, як і раніше, потрібен режим FIPS для державних пристроїв на Windows. Інші клієнти повинні самостійно вирішити, чи підходить для них режим FIPS. Існує безліч програм і протоколів, які використовують політику режиму FIPS, щоб визначити, які функції шифрування слід запускати. Клієнтам, які прагнуть дотримуватися стандарту FIPS 140-2, слід вивчити параметри конфігурації своїх програм та протоколів. Це дослідження допоможе переконатись, що їх можна налаштувати для використання перевіреного шифрування FIPS 140-2.

Windows та відповідність вимогам до конфіденційності:

Корпорація Майкрософт приділяє особливу увагу конфіденційності даних у всіх продуктах та послугах. Пропонуємо адміністраторам та відповідальним за дотримання законодавства ознайомитися з вимогами щодо захисту даних у Windows. Корпорація Майкрософт збирає дані під час взаємодії з користувачами пристроїв Windows. Ці відомості можуть містити персональні дані, які можуть бути використані для надання, захисту та покращення Windows, а також для забезпечення мережевих функцій. Ці відомості дозволяють адміністраторам та відповідальним за дотримання законодавства налагодити співпрацю, щоб краще забезпечувати конфіденційність персональних даних та дотримуватися пов'язаних з ними положень, таких як загальні вимоги до захисту даних (GDPR).

1. Прозорість збору даних у Windows

Прозорість є важливою частиною процесу збирання даних у Windows. Детальні відомості про функції та процеси, що використовуються для збору даних, доступні для користувачів та адміністраторів прямо у Windows як під час, так і після налаштування пристрою.

1.1. Процедура налаштування пристрою та підтримка багаторівневої прозорості

При настроюванні пристрою користувач може налаштувати конфіденційність. Ці параметри конфіденційності є ключем для визначення обсягу персональних даних, що збираються. По кожному параметру конфіденційності користувачеві надаються відомості про параметр разом із посиланнями на додаткову інформацію. Ця інформація пояснює, які дані збираються, як дані використовуються та як керувати параметром після завершення налаштування пристрою. Користувач також може ознайомитися із заявою про конфіденційність під час підключення до мережі на етапі налаштування. Короткий огляд параметрів конфіденційності наведено у статті Учасники програми попередньої оцінки Windows першими побачать новий макет екрана параметрів конфіденційності у Windows 10 – запис у блогах про Windows.

1.2 Контроль збору даних

Засіб перегляду діагностичних даних (DDV) – це програма Microsoft Store (доступна у Windows 10 починаючи з версії 1803 та Windows 11), що дозволяє користувачеві переглядати дані діагностики Windows, які збираються на пристрої з Windows і надсилаються до корпорації Майкрософт у режимі реального часу. DDV групує інформацію в прості категорії, що описують дані, що збираються. Адміністратор також може використовувати засіб перегляду діагностичних даних для модуля PowerShell для перегляду діагностичних даних, що збираються з пристрою, замість інтерфейсу користувача засобу перегляду діагностичних даних. Докладніші відомості див. у розділі Засіб перегляду діагностичних даних для PowerShell.

2. Управління збором даних у Windows

Можна керувати параметрами конфіденційності у Windows різними способами. Користувачі можуть змінити параметри конфіденційності, відкривши програму «Параметри» у Windows. Організація також може керувати параметрами конфіденційності за допомогою групової політики або управління мобільними пристроями (MDM). У наступних розділах наведено загальні відомості про те, як керувати параметрами конфіденційності, розглянутими раніше у цій статті.

2.1 Налаштування конфіденційності для користувачів

Якщо пристрій з Windows налаштований, користувач може керувати параметрами збору даних, відкривши програму «Параметри» у Windows. Адміністратори можуть керувати параметрами конфіденційності шляхом налаштування політики на пристрої (див. розділ 2.2 нижче). У цьому випадку користувач побачить оповіщення **Деякі параметри приховані або керуються організацією** під час переходу на сторінку «Параметри". У цьому випадку користувач може змінювати параметри лише відповідно до політик, встановлених адміністратором на пристрої.

2.2 Керування параметрами конфіденційності для адміністраторів

Адміністратори можуть налаштовувати конфіденційність та керувати ними в межах своєї організації за допомогою групової політики, параметрів керування мобільними пристроями (MDM) або параметрів реєстру Windows.

У таблиці нижче наведено загальні відомості про параметри конфіденційності, описані вище в цьому документі, з детальною інформацією про те, як можна налаштувати ці політики. У таблиці також наводиться інформація про значення за замовчуванням для кожного з цих параметрів конфіденційності на випадок, якщо ви не керуєте цим параметром за допомогою політики і не пропускаєте процедуру запуску при першому увімкненні комп'ютера (OOBE) під час налаштування пристрою. Якщо ви хочете мінімізувати збір даних, тут також наводяться рекомендовані значення для налаштування.

2.3 Посібник з налаштування конфігурації

У цьому розділі наводяться загальні відомості та посилання на докладніші відомості, а також інструкції для адміністраторів та відповідальних за дотримання законодавства. За допомогою цих інструкцій ви зможете керувати

настройками пристрою, щоб керувати цілями щодо відповідності вимогам вашої організації. Сюди включені відомості про налаштування пристрою та встановлення параметрів пристрою після завершення процедури налаштування, щоб звести до мінімуму обсяг даних, що збираються, і забезпечити конфіденційність у роботі користувачів з пристроєм.

2.3.1 Керування процесом налаштування пристрою

Розгортання Windows можна налаштувати за допомогою різних способів, які надають адміністратору можливості для керування, включаючи те, як пристрій налаштований, що увімкнено за замовчуванням, а також що користувач може змінювати пристрій після входу в систему.

Якщо ви хочете отримати можливість повністю контролювати та застосовувати обмеження до даних, що надсилаються до корпорації Майкрософт, можна використовувати Менеджер конфігурацій як рішення для розгортання. Диспетчер конфігурацій можна використовувати для розгортання налаштованого способу завантаження за допомогою різних методів розгортання. Можна додатково обмежити надсилання до корпорації Майкрософт будь-яких діагностичних даних, які стосуються диспетчера конфігурацій, відключивши цей параметр, як описано тут.

Крім того, адміністратори можуть також використовувати програму Windows Autopilot. Autopilot знижує загальне навантаження на розгортання, що дозволяє адміністраторам повністю налаштовувати запуск при першому включенні комп'ютера. Тим не менш, оскільки Windows Autopilot є хмарним рішенням, адміністратори повинні знати, що мінімальний набір ідентифікаторів пристроїв відправляється до корпорації Майкрософт під час початкового завантаження пристрою. Ця залежна від пристрою інформація використовується для ідентифікації пристрою, щоб він міг отримувати налаштовані адміністратором профіль та політики Autopilot.

2.3.2 Керування мережними функціями та основними службами Windows

Windows включає компоненти, які підключаються до Інтернету для надання розширених функцій та додаткових можливостей на основі служб. Ці компоненти називають мережевими функціями. Наприклад, антивірусна програма Microsoft Defender – це мережна функція, що забезпечує оновлений захист для підтримки безпеки пристроїв в організації.

Основні служби – це служби продукту, які підключаються до корпорації Майкрософт для забезпечення безпеки, своєчасного оновлення та належної роботи продукту. Наприклад, ліцензійна служба, яка підтверджує наявність дійсної ліцензії на використання Windows.

Основні служби та функції мережі Windows надають список найпоширеніших основних служб і мережевих функцій Windows.

Якщо Ви використовуєте мережну функцію, дані надсилаються в корпорацію Майкрософт і обробляються нею, щоб надати цю мережну функцію. Адміністратори можуть керувати тим, які дані надсилаються з їх організації до корпорації Майкрософт, налаштування параметрів, пов'язаних з можливостями, що надаються мережними функціями та основними службами Windows. Для

отримання додаткових відомостей див. розділ Керування з'єднаннями з операційної системи Windows до служб Майкрософт. У цій статті наведено різні методи, які можна використовувати для налаштування кожного параметра, вплив на функціональність, а також вказано, які версії Windows можна застосувати.

У статті Керування кінцевими точками підключення для Windows 11 Корпоративна список кінцевих точок, до яких мережеві функції Windows передають дані для останнього випуску Windows, а також описи будь-яких функцій, які можуть бути порушені обмеженням збору даних.

2.3.3 Базовий план обмеженої функціональності

Організації може знадобитися мінімізувати обсяг даних, надісланих у Microsoft або спільних з програмами Майкрософт, шляхом керування підключеннями та налаштування додаткових параметрів на своїх пристроях. Аналогічно Базовим параметрам безпеки Windows корпорація Майкрософт випустила обмежений базовий рівень функціональності, спрямований на налаштування параметрів для мінімізації даних, що надсилаються до Майкрософт. Проте застосування цих налаштувань може вплинути на функціональність пристрою. У статті Управління підключеннями від компонентів операційної системи Windows до служб Майкрософт викладаються докладні відомості про те, як застосувати базовий план, наводиться повний перелік параметрів, що входять до базового плану, а також розповідається про те, які функції торкнуться. Адміністратори, які не бажають застосовувати базовий план, також можуть знайти відомості про те, як налаштувати кожен параметр окремо, щоб знайти оптимальний баланс між надсиланням даних та впливом на необхідні для організації функції.

2.3.4 Діагностичні дані: керування повідомленнями про зміну рівня при вході

Починаючи з Windows 10, версія 1803 та Windows 11, якщо адміністратор змінив параметр збору діагностичних даних, користувачі будуть повідомлені про цю зміну при першому вході до пристрою. Наприклад, якщо ви налаштували пристрій на надсилання додаткових діагностичних даних, користувач отримає повідомлення під час наступного входу до пристрою. Ці оповіщення можна вимкнути за допомогою налаштування групової політики Конфігурація комп'ютера > Адміністративні шаблони > Компоненти Windows > Збір даних та попередні збирання > Налаштування повідомлень про зміну згоди на збір даних телеметрії або політики MDM ConfigureTelemetryOptInChangeNotification.

2.3.5 Діагностичні дані: керування вибором кінцевого користувача для зміни параметра

Windows 10 версії 1803 і пізніших версій та Windows 11 дозволяє користувачам змінювати рівень діагностичних даних на нижче значення, ніж задане адміністратором. Наприклад, якщо ви налаштували пристрій на надсилання необов'язкових діагностичних даних, користувач може змінити параметр так, щоб надсилалися лише обов'язкові діагностичні дані, відкривши програму «Параметри» у Windows і перейшовши до розділу Діагностика та відгуки. Адміністратори можуть обмежити можливість зміни цього параметра

користувачами, увімкнувши групову політику.Налаштування інтерфейсу згоди на збір даних телеметрії або політику MDM ConfigureTelemetryOptInSettingsUx.

2.3.6 Діагностичні дані: керування видаленням даних залежно від пристрою

У Windows 10 версії 1809 і пізніших версій і Windows 11 користувач може видалити діагностичні дані, зібрані на його пристрої, відкривши програму «Параметри» у Windows, перейшовши в розділ Діагностика та відгуки та натиснувши кнопку Видалити під заголовком Видалити діагностичні дані. Адміністратор також може видалити діагностичні дані з пристрою за допомогою командлета PowerShell Clear-WindowsDiagnosticData.

Адміністратор може вимкнути можливість користувача видаляти дані діагностики з пристрою, налаштувавши групову політику Конфігурація комп'ютера > Адміністративні шаблони > Компоненти Windows > Збір даних та попередні збирання > Вимкнути видалення діагностичних даних або політику MDM DisableDeviceDelete.

2.3.7 Діагностичні дані: увімкнення конфігурації обробника діагностичних даних Windows

Конфігурація обробника діагностичних даних Windows дозволяє IT-адміністраторам бути керуючими відповідно до Загального регламенту Європейського Союзу захисту даних (GDPR) для діагностичних даних Windows, зібраних з пристроїв з Windows, які приєднані до Azure Active Directory (AAD) і відповідають вимогам до конфігурації. Щоб отримати додаткові відомості, див. Увімкнення конфігурації процесора діагностичних даних Windows у статті Настроювання діагностичних відомостей Windows у вашій організації. Діагностичні дані Windows не включають дані, які обробляє корпорація Майкрософт у зв'язку з наданням можливостей, заснованих на службах.

Діагностичні дані Windows, зібрані з пристроїв, для яких увімкнена конфігурація процесора діагностичних даних Windows, можуть бути пов'язані з конкретним ідентифікатором користувача Azure Active Directory або ідентифікатором пристрою. Конфігурація обробника діагностичних даних Windows надає елементи керування, які допомагають відповідати на запити суб'єкта даних (DSR) для видалення діагностичних даних при закритті облікового запису користувача для певного ідентифікатора користувача Azure AD. Крім того, можна експортувати запити суб'єкта даних для діагностичних даних, пов'язаних з певним ідентифікатором користувача Azure AD. Щоб отримати додаткові відомості, див. Процес здійснення прав суб'єкта даних. Корпорація Майкрософт також забезпечить закриття облікового запису клієнта або тому, що ви вирішили закрити свій обліковий запис клієнта Azure або Azure AD, або тому що ви вирішили закрити обліковий запис клієнта Azure або Azure AD або тому, що ви вирішили, що більше не хочете бути контролером даних для діагностики даних Windows, але, як і раніше, хочете залишатися клієнтом Azure.

IT-адміністраторам, які включили конфігурацію обробника діагностичних даних Windows, рекомендується враховувати наступне:

– Обмежте можливість користувача входити до облікового запису Microsoft (MSA) за допомогою блокування групової політики облікового запису Майкрософт.

– Обмежте можливість користувача надсилати відгуки, оскільки будь-які відгуки або додаткові журнали, надіслані користувачем, не керуються параметром конфігурації процесора діагностичних даних Windows. Ви можете видалити програму «Центр відгуків» за допомогою PowerShell, а можливість надсилання відгуків у Microsoft Edge можна заблокувати за допомогою групової політики відгуків.

3. Процедура реалізації прав суб'єкта даних

У цьому розділі описано різні способи, які корпорація Майкрософт надає користувачам та адміністраторам для реалізації прав суб'єктів даних стосовно даних, зібраних на пристрої з Windows.

Для IT-адміністраторів, у яких є пристрої, які використовують конфігурацію процесора діагностичних даних Windows, див. Запити суб'єктів даних для GDPR та CCPA. В іншому випадку переходьте до розділів нижче.

3.1 Видалення

Користувачі можуть видалити дані на основі пристроїв, відкривши програму «Параметри» у Windows, перейшовши до розділу «Діагностика та відгуки» та натиснувши кнопку «Видалити» під заголовком «Видалити діагностичні дані». Адміністратори можуть також використовувати командлет PowerShell Clear-WindowsDiagnosticData.

3.2 Перегляд

Засіб перегляду діагностичних даних (DDV) надає можливість перегляду діагностичних даних, що збираються на пристрої Windows. Адміністратори також можуть використовувати командлет PowerShell Get-DiagnosticData.

3.3 Експорт

Засіб перегляду діагностичних даних (DDV) забезпечує можливість експорту діагностичних даних, отриманих під час роботи програми шляхом натискання кнопки «Експорт даних» у верхньому меню. Адміністратори можуть також використовувати сценарій командлета PowerShell Get-DiagnosticData.

3.4 Пристрої, підключені до облікового запису Майкрософт

Якщо користувачі входять до інтерфейсу Windows або програми на пристрої за допомогою облікового запису Майкрософт, вони можуть переглядати, видаляти та експортувати дані, пов'язані зі своїм обліковим записом Майкрософт, на Інформаційній панелі конфіденційності.

4. Передача даних через кордони

Корпорація Майкрософт виконує вимоги чинного законодавства щодо збору, використання та зберігання персональних даних, у тому числі щодо їх передачі через кордони.

5. Відомості про пов'язані продукти Windows

У розділах нижче наведено докладні відомості про те, як збираються та обробляються конфіденційні дані та у зв'язаних продуктах Windows.

5.1 Windows Server 2016 та пізніших версій

Windows Server використовує самі механізми, як і Windows 10 (і пізніших версій), для обробки персональних даних.

5.2 Surface Hub

Surface Hub є загальним пристроєм, який використовується в організації. Ідентифікатор пристрою, який збирається у складі діагностичних даних, не пов'язаний з користувачем. Для видалення діагностичних даних Windows, які надсилаються до корпорації Майкрософт щодо Surface Hub, можна використовувати засіб видалення діагностичних даних Surface Hub, доступний у Microsoft Store.

5.3 Аналітика комп'ютерів

Аналітика комп'ютерів – це набір рішень для порталу Azure, які надають широку інформацію про стан пристроїв у розгортанні. Аналітика комп'ютерів – це окрема від Windows пропозиція, яка залежить від увімкнення режиму мінімального збору даних на пристрої для роботи.

5.4 Комп'ютери, керовані Майкрософт

Комп'ютери, керовані Майкрософт (MMD), це служба, яка надає користувачам безпечні сучасні можливості та завжди забезпечує оновлення пристроїв з урахуванням останніх версій Windows Корпоративна, Office 365 професійний плюс і служб безпеки Microsoft.

5.5 Підтримка оновлень

Підтримка оновлень – це служба, яка дозволяє організаціям відстежувати оновлення безпеки, якості та функцій для випусків Windows Професійна, для освітніх закладів та Корпоративна, а також переглядати звіт про проблеми пристроїв та оновлень, пов'язані з відповідністю вимогам, які потребують уваги. Підтримка оновлень використовує діагностичні дані Windows для всіх звітів.

Розділ 6. Моделі безпеки в інформаційній та/або кібербезпеці.

6.1. ДСТУ ISO/IEC 15408
6.2. Модель порушника.
6.3. Модель загроз.
6.4. Модель вразливостей

6.1. ДСТУ ISO/IEC 15408

При побудові моделі безпеки в інформаційній та/або кібербезпеці, для аналізу інформаційних ризиків необхідно використовувати моделі системи інформаційної безпеки, засновані на міжнародних стандартах. Для цього як правило використовуються наступні стандарти: ДСТУ ISO/IEC 27002 та ДСТУ ISO/IEC 15408. ДСТУ ISO/IEC 27002 розглядався раніше, тому розглянемо ДСТУ ISO/IEC 15408.

ДСТУ ISO/IEC 15408. Інформаційні технології. Методи захисту. Критерії оцінки.

Безпека інформаційних технологій (IT) стоїть у ряду найактуальніших проблем інформатизації суспільства. Її розв'язання значною мірою визначається досконалістю відповідної нормативно-методичної бази. Дана доповідь присвячена одному з найбільш значущих в цьому плані документів – міжнародному стандарту ISO/IEC 15408 "Критерії оцінки безпеки інформаційних технологій "

Стандарт ISO 15408 – один з найбільш поширених стандартів у галузі безпеки. У його створенні взяли участь організації зі США, Канади, Англії, Франції, Німеччини, Голландії. У стандарті, що отримав назву «Загальні критерії оцінки безпеки інформаційних технологій» (The Common Criteria for Information Technology Security Evaluation), докладно розглянуто загальні підходи, методи та функції забезпечення захисту інформації в організаціях.

Функції системи інформаційної безпеки забезпечують виконання вимог конфіденційності, цілісності, достовірності та доступності інформації. **Всі функції представлені у вигляді чотирирівневої ієрархічної структури**: клас – сімейство – компонент – елемент.

За аналогією представлені вимоги якості. Подібна градація дозволяє описати будь-яку систему інформаційної безпеки і зіставити створену модель з поточним станом справ.

У стандарті виділені 11 класів функцій:

– аудит;
– ідентифікація та автентифікація;
– криптографічний захист;
– конфіденційність;
– передача даних;
– захист даних користувача;
– управління безпекою;

– захист функцій безпеки системи;
– використання ресурсів;
– доступ до системи;
– надійність засобів.

Оцінка інформаційної безпеки базується на моделях системи безпеки, що складаються з перерахованих у стандарті функцій. У ISO 15408 міститься **ряд зумовлених моделей** (так званих **профілів),** що описують стандартні модулі системи безпеки. З їх допомогою можна не створювати моделі поширених засобів захисту самостійно, винаходячи велосипед, а користуватися вже готовими наборами описів, цілей, функцій і вимог до цих засобів. Простим прикладом профілів може служити модель міжмережевого екрану.

Сертифікований профіль являє собою повний опис певної частини (або функції) системи безпеки. У ньому міститься аналіз внутрішнього і зовнішнього середовища об'єкта, вимоги до його функціональності і надійності, логічне обгрунтування його використання, можливості та обмеження розвитку об'єкта.

Стандарт ISO 15408 вигідно відрізняє **відкритість.** Описує ту чи іншу область системи безпеки профіль можна створити самостійно за допомогою розробленої в ISO 15408 структури документа. У стандарті визначена також послідовність дій для самостійного створення профілів.

Загальні критерії (ЗК) визначені у стандарті ISO 15408 дозволяють підвищити довіру до засобів захисту і самої інформації, що захищається за рахунок трьох основних якостей:

1. Можливості гнучкого завдання вимог до засобів захисту інформації з урахуванням їх призначення і умов застосування.
2. Більш повного і обґрунтованого набору вимог безпеки.
3. Наявності методології оцінки, що забезпечує об'єктивність і порівнянність результатів.

Загальні критерії являють собою набір з п'яти окремих взаємопов'язаних частин. До них відносяться:

– Введення і загальна модель.
– Функціональні вимоги безпеки.
– Вимоги до надійності захисних механізмів.
– Попереднє визначення профілі захисту.
– Процедури реєстрації профілів захисту.

Основними відмітними рисами ЗК є наступні:

1. Перш за все, ЗК – це певна методологія та система формування вимог і оцінки безпеки ІТ. Системність простежується, починаючи від термінології та рівнів абстракції представлення вимог аж до їх застосування при оцінці безпеки на всіх етапах життєвого циклу продуктів і систем ІТ.
2. Загальні критерії характеризуються найбільш повною на сьогоднішній день сукупністю вимог безпеки ІТ.
3. У ЗК проведено чіткий поділ вимог безпеки на функціональні вимоги і вимоги довіри до безпеки. Функціональні вимоги (11 класів, 66 родин, 135 компонентів) відносяться до функцій безпеки (ідентифікації, автентифікації, управління доступом, аудиту і т. д.), а вимоги довіри (8 класів, 44 сімейства, 93

компонента) – до досягнення впевненості в коректності реалізації та ефективності функцій безпеки шляхом оцінки технології розробки, тестування, аналізу вразливостей експлуатаційної документації, постачання і супроводу продуктів та систем ІТ.

4. Загальні критерії включають шкалу довіри до безпеки (оціночні рівні довіри – ОРД), яка може використовуватися для отримання різного ступеня впевненості у безпеці продуктів і систем ІТ

5. Систематизація і класифікація вимог щодо ієрархії «клас» – «сімейство» – «компонент» – «елемент»з унікальними ідентифікаторами вимог забезпечує зручність їх використання.

6. Компоненти вимог в родинах і класах ранжовані за ступенем повноти і строгості, а вимоги довіри згруповані в пакети вимог

7. Гнучкість у підході до формування вимог безпеки для різних типів продуктів і систем ІТ та умов їх застосування забезпечується можливістю цілеспрямованого формування необхідних наборів вимог у вигляді певних в ЗК стандартизованих структур (пакетів вимог, профілів захисту і завдань з безпеки).

8. Загальні критерії володіють відкритістю і розширюваністю, тобто дозволяють уточнювати існуючі і вводити додаткові вимоги.

Як показують оцінки фахівців у галузі інформаційної безпеки за рівнем систематизації, повноті і можливостям деталізації вимог, універсальності і гнучкості в застосуванні ЗК представляють найбільш досконалий з існуючих в даний час стандартів. Причому, що дуже важливо, в силу особливостей побудови він має практично необмежені можливості для розвитку і являє собою базовий стандарт, що містить методологію завдання вимог і оцінки безпеки ІТ, а також систематизований каталог вимог безпеки. Як функціональних стандартів, в яких формулюються вимоги до безпеки певних типів продуктів і систем ІТ, передбачається використання профілів захисту (ПЗ), що створюються за методологією і на основі каталогу вимог ЗК. У ПЗ можуть бути включені і будь-які інші вимоги, які є необхідними для забезпечення безпеки конкретного типу продуктів або систем ІТ.

– керівництво з розробки профілів захисту і завдань з безпеки;

– процедури реєстрації профілів захисту;

– загальна методологія оцінки безпеки інформаційних технологій;

– Інструментальні засоби автоматизації розробки профілів захисту і завдань з безпеки.

Загальні критерії отримали широке визнання у світі. У 1998 році урядовими організаціями Канади, Франції, Німеччини, Великобританії і США було підписано угоду про взаємне визнання оцінок (The International Mutual Recognition Arrangement – MRA), отриманих на основі Загальних критеріїв.

У травні 2000 року представниками вже чотирнадцяти країн було підписано більш універсальне (у порівнянні з MRA) угоду CCRA (CC Recognition Arrangement). Угода CCRA значно розширює можливості приєднання нових країн-учасниць. Як очікується, найближчим часом їхня кількість наблизиться до двадцяти.

У країнах, що беруть участь в Угоді з Загальними критеріями (перш за все, в США, Великобританії, Франції та ін), розроблено вже декілька десятків профілів захисту для різних типів продуктів ІТ:

– систем управління доступом;

– операційних систем;

– систем управління базами даних;

– міжмережевих екранів;

– компонентів інфраструктури управління ключами;

– смарт-карт і ін.

Частина з них пройшла експертизу і включена в національні реєстри. Існує міжнародний реєстр сертифікованих профілів захисту, а також знаходяться в процесі оцінки і сертифікованих продуктів ІТ. У рамках ОК пройшли оцінку і сертифікацію більше 40 продуктів і систем ІТ і близько 20 знаходиться в процесі оцінки.

Проблема забезпечення безпеки інформаційних технологій займає усе більш значне місце в реалізації комп'ютерних систем та мереж у міру того, як зростає їх роль в інформатизації суспільства. Забезпечення безпеки інформаційних технологій (ІТ) являє собою комплексну проблему, яка вирішується в напрямках вдосконалення правового регулювання застосування ІТ, вдосконалення методів і засобів їх розробки, розвитку системи сертифікації, забезпечення відповідних організаційно-технічних умов експлуатації. Ключовим аспектом вирішення проблеми безпеки ІТ є вироблення системи вимог, критеріїв та показників для оцінки рівня безпеки ІТ.

ДСТУ ISO/IEC 15408 містить загальні критерії оцінки безпеки інформаційних технологій.

ДСТУ ISO/IEC 15408-1 встановлює загальний підхід до формування вимог до оцінки безпеки (функціональні та довіри), основні конструкції (профіль захисту, завдання з безпеки) подання вимог безпеки в інтересах споживачів, розробників і оцінювачів продуктів і систем ІТ. Вимоги безпеки об'єкта оцінки (00) за методологією Загальних критеріїв визначаються виходячи з цілей безпеки, які, у свою чергу, грунтуються на аналізі призначення 00 і умов середовища його використання (загроз, припущень, політики безпеки).

ДСТУ ISO/IEC 15408-2 містить універсальний систематизований каталог функціональних вимог безпеки і передбачає можливість їх деталізації і розширення за певними правилами.

ДСТУ ISO/IEC 15408-3 включає в себе систематизований каталог вимог довіри, визначають заходи, які повинні бути прийняті на всіх етапах життєвого циклу продукту або системи ІТ для забезпечення впевненості в тому, що вони задовольняють пред'явленим до них функціональним вимогам. Тут же містяться оціночні рівні довіри, що визначають шкалу вимог, які дозволяють з зростаючої ступенем повноти і строгості оцінити проектну, тестову та експлуатаційну документацію, правильність реалізації функцій безпеки 00, вразливості продукту або системи ІТ, стійкість механізмів захисту і зробити висновок про рівень довіри до безпеки об'єкта оцінки.

Особливості ISO 15408 в порівнянні з іншими стандартами в галузі безпеки:

– Стандарт дозволяє визначити повний перелік вимог до засобів безпеки, а також критерії їх оцінки (показники захищеності інформації).

– Стандарт визначає повний перелік об'єктів аналізу і вимог до них, не загострюючи уваги на методах створення, управління та оцінки системи безпеки.

– Стандарт дозволяє оцінити повноту системи інформаційної безпеки з технічної точки зору, не розглядаючи при цьому комплекс організаційних заходів щодо забезпечення захисту інформації.

Вивчення існуючих критеріїв оцінки безпеки дозволяє зробити наступні висновки:

1. Для того, щоб результати сертифікаційних випробувань можна було порівнювати між собою, вони мають проводитися в рамках надійної схеми, що встановлюється відповідними стандартами в цій галузі і дозволяє контролювати якість оцінки безпеки.

2. В даний час в деяких країнах існують такі схеми, але вони базуються на різних критеріях оцінки. Однак, ці критерії мають між собою багато спільного, тому що використовують подібні концепції, що дозволяє здійснювати їх порівняння. "Єдині критерії" підтримують сумісність з вже існуючими. Це дозволяє використовувати наявні результати та методики оцінок.

3. Єдині критерії визначають загальний набір понять, структур даних і мова для формулювання питань і тверджень щодо безпеки. Це дозволяє експертам, які проводять оцінку, використовувати вже у цій області досвід.

4. Вимоги, що містяться в "Єдиних критеріях", можуть також використовуватися при виборі відповідних засобів забезпечення безпеки. Потенційні користувачі ІКС, спираючись на результати сертифікації, можуть визначити чи задовольняє даний програмний продукт або система їх вимогам безпеки.

5. Крім цього, "Єдині критерії" покращують існуючі критерії, вводячи нові концепції і уточнюючи зміст наявних.

Розглянемо більш детально стандарт.

ДСТУ ISO/IEC 15408-1:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 1. Вступ та загальна модель (ISO/IEC 15408-1:2022, IDT)

Цей документ встановлює загальні концепції та принципи оцінювання безпеки ІТ і визначає загальну модель оцінювання, що надається різними частинами стандарту, який у цілому призначений для використання в якості основи для оцінки властивостей безпеки ІТ-продуктів.

Цей документ містить огляд усіх частин серії ISO/IEC 15408. Він описує різні частини серії ISO/IEC 15408; визначає терміни та скорочення, які слід використовувати в усіх частинах стандарту; встановлює основну концепцію мети оцінювання (TOE); описує контекст оцінювання та описує аудиторію, якій

адресовані критерії оцінювання. Дано вступ до основних концепцій безпеки, необхідних для оцінки ІТ-продуктів.

Цей документ представляє:

– ключові поняття профілів захисту (PP), модулів PP, конфігурацій PP, пакетів, цілей безпеки (ST) і типів відповідності;

– опис організації компонентів безпеки по всій моделі;

– різні операції, за допомогою яких функціональні компоненти та компоненти гарантії, наведені в ISO/IEC 15408-2 та ISO/IEC 15408-3, можуть бути налаштовані шляхом використання дозволених операцій;

– загальну інформацію про методи оцінювання, наведені в ISO/IEC 18045;

– настанову щодо застосування ISO/IEC 15408-4 з метою розробки методів оцінювання (EM) і діяльності з оцінювання (EA), виведених із ISO/IEC 18045;

– загальну інформацію про попередньо визначені рівні гарантії оцінювання (EAL), визначені в ISO/IEC 15408-5;

– інформація щодо обсягу схем оцінювання.

ДСТУ ISO/IEC 15408-2:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 2. Функціональні вимоги (ISO/IEC 15408-2:2022, IDT)

Цей документ визначає необхідну структуру та зміст функціональних компонентів безпеки з метою оцінки безпеки. Він містить каталог функціональних компонентів, який відповідає загальним вимогам безпеки багатьох ІТ-продуктів.

Він включає в себе наступні розділи:

1 Область застосування.

2 Нормативні посилання.

3 Терміни та визначення, умовні позначення та скорочення термінів.

4 Огляд.

4.1 Організація цієї частини ISO/IEC 15408.

5 Парадигма функціональних вимог.

6 Функціональні компоненти безпеки.

6.1 Огляд.

6.2 Каталог компонентів.

7 Клас FAU: Аудит безпеки.

7.1 Автоматична відповідь аудиту безпеки (FAU_ARP).

7.2 Генерація даних аудиту безпеки (FAU_GEN).

7.3 Аналіз аудиту безпеки (FAU_SAA).

7.4 Аудит безпеки (FAU_SAR).

7.5 Вибір події аудиту безпеки (FAU_SEL).

7.6 Зберігання подій аудиту безпеки (FAU_STG).

8 Клас FCO: Комунікація.

8.1 Невідмова від походження (FCO_NRO).

8.2 Невідмова від отримання (FCO_NRR).

9 Клас FCS: Криптографічна підтримка.

9.1 Керування криптографічними ключами (FCS_CKM).

9.2 Криптографічна операція (FCS_COP).
10 FDP класу: Захист даних користувача.
10.1 Політика контролю доступу (FDP_ACC).
10.2 Функції контролю доступу (FDP_ACF).
10.3 Автентифікація даних (FDP_DAU).
10.4 Експорт із TOE (FDP_ETC).
10.5 Політика керування потоком інформації (FDP_IFC).
10.6 Функції керування потоком інформації (FDP_IFF).
10.7 Імпорт із-за меж TOE (FDP_ITC).
10.8 Внутрішня передача TOE (FDP_ITT).
10.9 Захист залишкової інформації (FDP_RIP).
10.10 Відкат (FDP_ROL).
10.11 Цілісність збережених даних (FDP_SDI).
10.12 Захист передавання конфіденційності даних користувача між TSF (FDP_UCT).
10.13 Захист передавання цілісності даних користувача між TSF (FDP_UIT).
11 Клас FIA: Ідентифікація та автентифікація.
11.1 Помилки автентифікації (FIA_AFL).
11.2 Визначення атрибутів користувача (FIA_ATD).
11.3 Специфікація секретів (FIA_SOS).
11.4 Автентифікація користувача (FIA_UAU).
11.5 Ідентифікація користувача (FIA_UID).
11.6 Прив’язка користувача до суб’єкта (FIA_USB).
12 Клас FMT: Управління безпекою.
12.1 Керування функціями в TSF (FMT_MOF).
12.2 Керування атрибутами безпеки (FMT_MSA).
12.3 Управління даними TSF (FMT_MTD).
12.4 Відкликання (FMT_REV).
12.5 Термін дії атрибута безпеки (FMT_SAE).
12.6 Специфікація функцій керування (FMT_SMF).
12.7 Ролі керування безпекою (FMT_SMR).
13 Клас FPR: конфіденційність.
13.1 Анонімність (FPR_ANO).
13.2 Псевдонім (FPR_PSE).
13.3 Від’єднаність (FPR_UNL).
13.4 Неспостережуваність (FPR_UNO).
14 Клас FPT: Захист TSF.
14.1 Захист від помилок (FPT_FLS).
14.2 Доступність експортованих даних TSF (FPT_ITA).
14.3 Конфіденційність експортованих даних TSF (FPT_ITC).
14.4 Цілісність експортованих даних TSF (FPT_ITI)..
14.5 Внутрішня передача даних TOE TSF (FPT_ITT).
14.6 Фізичний захист TSF (FPT_PHP).
14.7 Довірене відновлення (FPT_RCV).

14.8 Виявлення повтору (FPT_RPL).
14.9 Протокол синхронізації стану (FPT_SSP).
14.10 Мітки часу (FPT_STM).
14.11 Послідовність даних TSF між TSF (FPT_TDC).
14.12 Тестування зовнішніх об'єктів (FPT_TEE).
14.13 Внутрішня узгодженість реплікації даних TSF TOE (FPT_TRC).
14.14 Самоперевірка TSF (FPT_TST).
15 Клас FRU: Використання ресурсів.
15.1 Відмовостійкість (FRU_FLT).
15.2 Пріоритет обслуговування (FRU_PRS).
15.3 Розподіл ресурсів (FRU_RSA).
16 Class FTA: Доступ TOE.
16.1 Обмеження обсягу вибраних атрибутів (FTA_LSA).
16.2 Обмеження на кілька одночасних сеансів (FTA_MCS).
16.3 Блокування та завершення сеансу (FTA_SSL).
16.4 Банери доступу до TOE (FTA_TAB).
16.5 Історія доступу до TOE (FTA_TAH).
16.6 Встановлення сеансу TOE (FTA_TSE).
17 Клас FTP: Довірений шлях/канали.
17.1 Довірений канал Inter-TSF (FTP_ITC).
17.2 Довірений шлях (FTP_TRP).
Додаток A (обов’язковий) Примітки щодо застосування функціональних вимог безпеки.
Додаток B (обов'язковий) Функціональні класи, родини та компоненти.
Додаток C (обов'язковий) Клас FAU: Аудит безпеки.
Додаток D (обов'язковий) Клас FCO: зв'язок.
Додаток E (обов’язковий) Клас FCS: Криптографічна підтримка.
Додаток F (обов'язковий) Клас FDP: Захист даних користувача.
Додаток G (обов'язковий) Клас FIA: Ідентифікація та автентифікація.
Додаток H (обов'язковий) Клас FMT: Управління безпекою.
Додаток I (обов’язковий) Клас FPR: конфіденційність.
Додаток J (обов’язковий) Клас FPT: Захист TSF.
Додаток K (обов'язковий) Клас FRU: Використання ресурсів.
Додаток L (обов'язковий) Class FTA: доступ до TOE.
Додаток M (обов’язковий) Клас FTP: Довірений шлях/канали

ДСТУ ISO/IEC 15408-3:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 3. Вимоги до гарантії безпеки (ISO/IEC 15408-3:2008, IDT)

ISO/IEC 15408-3:2008 визначає вимоги довіри до критеріїв оцінювання. Він включає в себе рівні достовірності оцінки, які визначають шкалу для вимірювання достовірності для цілей компонентів оцінювання (TOE), складені пакети достовірності, які визначають шкалу для вимірювання достовірності для складених TOE, окремі компоненти довіри, з яких складаються рівні та пакети достовірності., а також критерії оцінки профілів захисту та цілей безпеки.

ISO/IEC 15408-3:2008 визначає зміст і представлення вимог довіри у формі класів достовірності, сімейств і компонентів і надає вказівки щодо організації нових вимог довіри. Компоненти впевненості в сімействах впевненості представлені в ієрархічному порядку.

Моделі безпеки в інформаційній та/або кібербезпеці

Інформаційна безпека – це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, використання й розвиток в інтересах громадян або комплекс заходів, спрямованих на забезпечення захищеності інформації особи, суспільства і держави від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки запису чи знищення (у цьому значенні частіше використовують термін «захист інформації»).

Інформаційна безпека за сферою застосування

Інформаційна безпека держави – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається заподіяння шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Інформаційна безпека організації – цілеспрямована діяльність її органів та посадових осіб з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток. Здійснюється часто Службою інформаційної безпеки.

Інформаційна безпека особистості характеризується як стан захищеності особистості, різноманітних соціальних груп та об'єднань людей від впливів, здатних проти їхньої волі та бажання змінювати психічні стани і психологічні характеристики людини, модифікувати її поведінку та обмежувати свободу вибору.

Поняття інформаційної безпеки не обмежується безпекою технічних інформаційних систем чи безпекою інформації у чисельному чи електронному вигляді, а стосується усіх аспектів захисту даних чи інформації незалежно від форми, у якій вони перебувають.

Створення **моделі управління захистом інформації** ґрунтується на послідовному визначенні об’єктів управління, цілей і завдань управління, показників і критеріїв ефективності управління, функцій управління, складу системи та організаційної структури управління, на розробці методів і засобів управління.

Проблеми інформаційної безпеки істотно залежать від типу інформаційних систем і сфери їх застосування. У локальних системах малого масштабу систему захисту побудувати набагато простіше, ніж в системах розподіленого типу, що пояснюється особливостями цих систем, основними з яких є:

– територіальна розосередженість компонентів системи і як наслідок наявність обміну інформацією між ними;

– широкий спектр способів подання, зберігання і передачі інформації;

– одночасна участь в процесах опрацювання інформації великою кількістю користувачів з різними правами доступу;

– використання різнорідних програмно-технічних засобів обробки і систем телекомунікацій.

Саме тому фахівцями була запропонована **структурна модель інформаційної безпеки систем розподіленого типу**, яка відображена на рис. 6.1.

Структурна модель передбачає, що рішення проблеми безпеки в інформаційних системах розподіленого типу полягає в аналізі наступних основних компонентів:

– визначення основних завдань захисту інформації;

– визначенні суб'єктів інформаційних процесів;

– класифікації основних можливих загроз безпеки;

– визначенні рівнів вразливості інформаційних систем;

– визначенні джерел інформації;

– ознайомленні з особливостями джерел загроз;

– дослідженні способів та напрямів захисту та звичайно цілей захисту.

Забезпечення безпеки інформації полягає у вирішенні трьох взаємопов'язаних завдань: конфіденційність, цілісність, доступність.

– Завдання забезпечення **конфіденційності** полягає в захисті інформації в процесі її створення, зберігання, обробки та обміну від ознайомлення з нею особами, які не мають права доступу до неї.

– Завдання щодо забезпечення **цілісності** полягає в захисті від навмисної або ненавмисної зміни інформації та алгоритмів її обробки особами, які не мають на те права.

– Забезпечення **доступності** полягає в наданні користувачам всієї наявної в системі інформації відповідно до встановлених їм правам.

Додатково також використовують такі властивості:

– Апелювання (англ. non-repudiation) – можливість довести, що автором є саме заявлена людина (юридична особа), і ніхто інший.

– Підзвітність (англ. accountability) – властивість інформаційної системи, що дозволяє фіксувати діяльність користувачів, використання ними пасивних об'єктів та однозначно встановлювати авторів певних дій в системі.

– Вірогідність (англ. reliability) – властивість інформації, яка визначає ступінь об'єктивного, точного відображення подій, фактів, що мали місце.

– Автентичність (англ. authenticity) – властивість, яка гарантує, що суб'єкт або ресурс ідентичні заявленим.

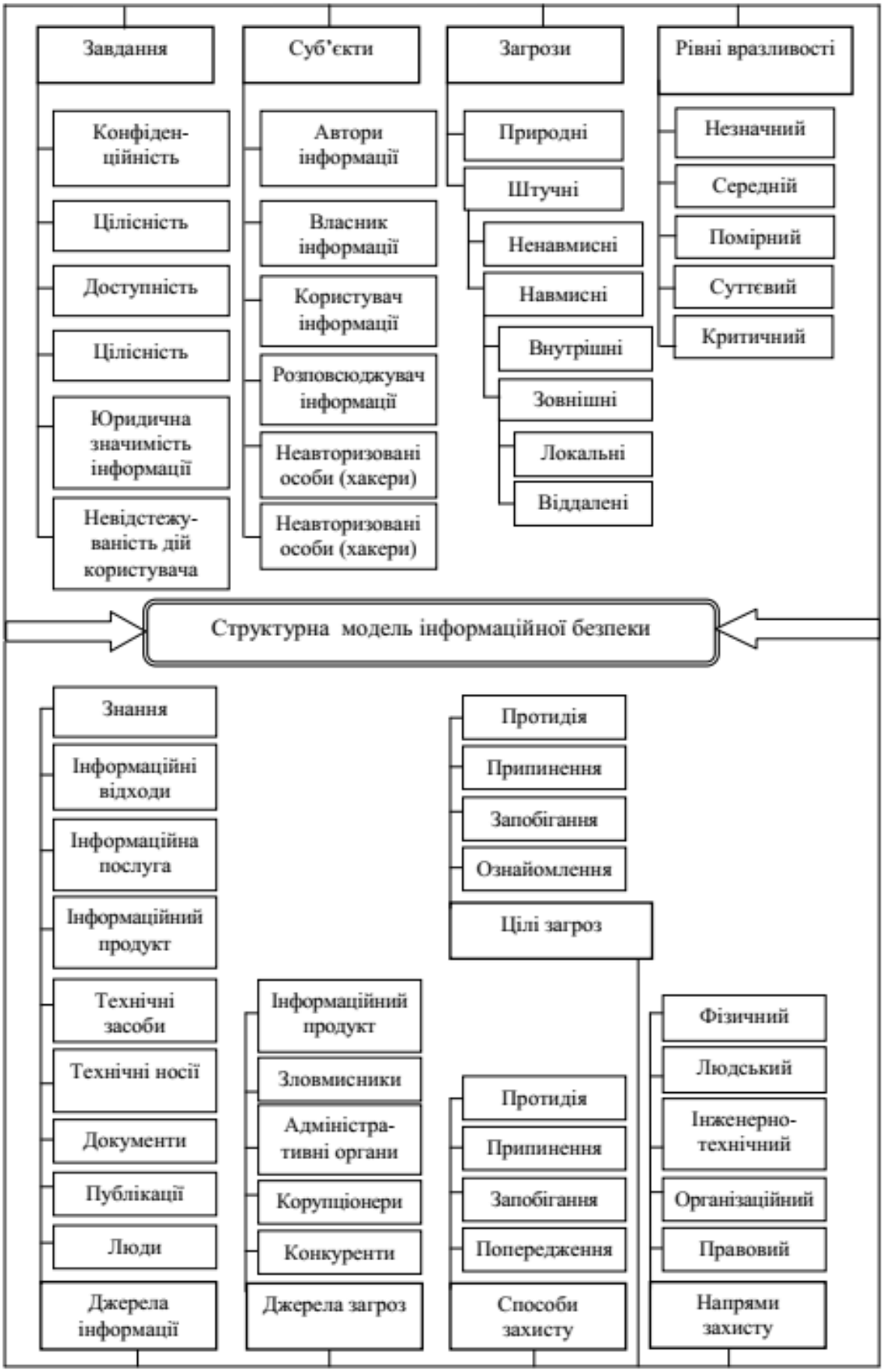


Рисунок 6.1 – Структурна модель інформаційної безпеки

Основними суб'єктами в інформаційних процесах є:

– автори і власники інформації;

– авторизовані користувачі інформації;

– неавторизовані особи (особи, які намагаються отримати самовільний доступ до інформації);

– окремі співробітники або колективи;

– які беруть участь в розробці, забезпеченні працездатності програмно-технічних засобів інформаційних систем і наповненні системи інформацією.

Системи захисту повинні забезпечувати захист прав авторів і власників інформації та одночасно надавати доступ до інформації користувачам відповідно до їх прав.

Під **загрозою безпеки** інформаційних систем розуміється потенційно можлива дія, подія або процес, який за допомогою впливу на інформацію та інші компоненти системи може завдати шкоди інтересам суб'єктів.

Джерелами загроз виступають конкуренти, злочинці, корупціонери, адміністративно-управлінські органи.

Джерела загроз переслідують при цьому наступні цілі:

– ознайомлення з відомостями, що охороняються;

– їх модифікація в корисливих цілях;

– знищення для нанесення прямих матеріальних збитків.

Неправомірне заволодіння конфіденційною інформацією можливо шляхом її розголошення джерелами відомостей, за рахунок витоку інформації через технічні засоби та через несанкціонований доступ до відомостей, що охороняються.

Джерелами конфіденційної інформації є:

– люди;

– їх знання;

– документи;

– публікації;

– технічні носії інформації;

– технічні засоби забезпечення виробничої та трудової діяльності;

– продукція;

– послуги і відходи виробництва.

Основними напрямками захисту інформації є:

– правовий;

– організаційний;

– інженерно-технічний;

– людський;

– фізичний захист інформації

як індикатори комплексного підходу до забезпечення інформаційної безпеки.

Засобами захисту інформації є:

– фізичні засоби;

– апаратні засоби;

– програмні засоби;

– криптографічні методи, які можуть бути реалізовані як апаратно, програмно, так і змішано-програмно-апаратними засобами.

В якості **засобів захисту** виступають всілякі заходи, шляхи, способи і дії, що забезпечують попередження протиправних дій, їх запобігання, припинення та протидію несанкціонованому доступу.

Окрім системного підходу, доцільно врахувати і положення процесного підходу до моделювання систем інформаційної безпеки. **Сутність процесного підходу до формування моделі інформаційної безпеки** полягає в тому, що захист інформації розглядається як особливий вид діяльності в організації, який здійснюється при моделюванні, проектуванні як сукупність процесів захисту інформації:

– наявність мети процесу, тобто бажаного результату захисту інформації, що досягається при здійсненні процесу;

– зміни предметної області, в якій реалізується процес. За суттю, реалізація процесу завжди пов'язана зі зміни системи та є цілеспрямованим переходом цієї системи з існуючого в бажаний стан;

– обмеженість необхідних ресурсів на виконання операцій і дій, що складають процес; безперервність процесу. Процес є модель функції захисту, яка здійснюється

– організацією протягом усього свого існування;

– комплексність та розмежування процесу. Комплексність процесу передбачає врахування всіх внутрішніх і зовнішніх факторів, які прямо або опосередковано впливають на розвиток процесу і результати процесу.

У той же час кожен **процес** має чітко визначені **межі предметної області**, наприклад процес аналізу загроз, процес сертифікації засобів захисту, процеси стратегічного управління безпекою тощо.

Формалізуючи модель інформаційної безпеки у математичному вигляді, доцільно визначити її функціональну залежність від завдань захисту інформації, суб’єктів інформаційних процесів, загроз безпеки, рівнів вразливості інформаційних систем, джерел інформації, джерел загроз, способів захисту, напрямів захисту, цілей захисту:

– стан системи інформаційної безпеки;

– сукупність суб’єктів системи інформаційної безпеки;

– сукупність завдань системи інформаційної безпеки;

– сукупність загроз системи інформаційної безпеки;

– рівні вразливості системи інформаційної безпеки;

– сукупність джерел інформації системи інформаційної безпеки;

– сукупність джерел загроз системи інформаційної безпеки;

– сукупність способів захисту інформаційних ресурсів;

– сукупність напрямів захисту інформаційних ресурсів;

– сукупність цілей захисту інформаційних ресурсів.

Інформаційна безпека є функцією з множини області значень складових системи інформаційної безпеки. Постійне зростання потреби в інформації обумовлює необхідність нарощування та ефективного використання інформаційних ресурсів, формування інформаційного потенціалу організаційних утворень, що виступає основною передумовою зміни стану системи інформаційної безпеки, перебудови або вдосконаленні її моделі.

6.2. Модель порушника

Модель порушника – це всебічна структурована характеристика порушника, яка використовується сумісно з моделлю загроз для розробки політики безпеки інформації. В Україні прийнята така структура моделі порушника:

Категорія осіб, до якої може належати порушник:

– внутрішні порушники;
– користувачі;
– інженерний склад;
– співробітники відділів, що супроводжують ПЗ;
– технічний персонал, що обслуговує будинок;
– співробітники служби безпеки;
– керівники;
– зовнішні порушники.

Мета порушника:

– отримання необхідної інформації;
– отримання можливості вносити зміни в інформаційні потоки у відповідності зі своїми намірами;
– нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

Повноваження порушника в ІКС:

– запуск фіксованого набору задач (програм);
– створення і запуск власних програмних засобів;
– керування функціонуванням і внесення змін у конфігурацію системи;
– підключення чи зміна конфігурації апаратних засобів.

Технічна оснащеність порушника:

– апаратні засоби;
– програмні засоби;
– спеціальні засоби.

Кваліфікація порушника: для аналізу загроз завжди приймається висока кваліфікація.

6.3. Модель загроз

Загроза (англ. – Threat) – це будь-які обставини чи події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитку ІКС. Тобто, загроза – це будь-який потенційно можливий несприятливий вплив. **Несприятливий вплив** – це вплив, що призводить до зниження цінності інформаційних ресурсів.

Атака (англ. – Attack) – це навмисна спроба реалізації загрози. Якщо атака є успішною (здійснено подолання засобів захисту), це називають **проникненням** (англ. – Penetration). Наслідком успішної атаки є порушення безпеки інформації в системі, яке називають **компрометацією (**англ. – Compromise).

Слід звернути увагу на те, що при комплексному підході до захисту інформації ми повинні розглядати не лише впливи, спрямовані на інформаційні ресурси, але й будь-які впливи, що можуть нанести збитки ІКС.

Загроза часто може бути слідством наявності вразливих місць системи. Визначимо терміном «**вразливість системи»** (англ. – System vulnerability) – нездатність системи протистояти реалізації визначеної загрози чи сукупності загроз.

Розповсюдженим випадком вразливостей систем є вади захисту. **Вади захисту** (англ. – Security flaw) – сукупність причин, умов і обставин, наявність яких може призвести до порушення нормального функціонування системи або до порушення політики безпеки інформації. Здебільшого, під вадами захисту розуміють особливості побудови програмних (а іноді і апаратних) засобів захисту, через які останні за певних обставин не здатні протистояти загрозам і виконувати свої функції. Тобто, вади захисту є окремим випадком вразливостей системи.

В літературі іноді зустрічається інше трактування термінів, яке не є коректним. Наприклад, іноді замість терміну “загроза” вживають термін “атака”. Однак, враховуючи визначення наведені вище, слід розрізняти атаку, яка є дією, спробою реалізувати певну загрозу, і загрозу, яка є потенційною можливістю здійснення несприятливого впливу. Зазначимо, що атака – це здебільшого цілеспрямований вплив, як правило, умисний. Загрози можуть бути випадковими, але від цього втрати внаслідок їх реалізації не стають меншими. Тому захищати інформацію необхідно саме від загроз, а не лише від атак.

Особи, які реалізують загрози називають порушниками. **Порушник** (англ. – User violator) – фізична особа (у загальному випадку не обов’язково користувач системи), яка здійснює порушення політики безпеки системи. Треба розрізняти терміни «порушник» та «**зловмисник**». Останній термін підкреслює умисність порушення, тоді як у загальному випадку порушник може здійснювати порушення неумисно (наприклад, через необережність або недостатню обізнаність).

Широко уживаний термін “**хакер**” (англ. – hacker) є досить неоднозначним тому ми не будемо використовувати його як синонім терміну “порушник”.

Класифікація загроз інформаційної безпеки

Історія розвитку інформаційних систем свідчить про те, що нові вразливості систем з'являються регулярно. З такою ж регулярністю, але ж з певним запізненням вони нейтралізуються. У проміжок часу між появою нової вразливості та її нейтралізацією система є особливо вразливою і може бути скомпрометованою. Особливо небезпечним є випадок коли нова вразливість вперше виявляється потенційним порушником. Тому, такий **«послідовний»** підхід до забезпечення інформаційної безпеки **не є ефективним**.

Більш ефективним є підхід **упередженого** захисту інформації, який базується на передбаченні всіх можливих, передбачуваних та потенційних загроз та розробці **комплексної системи захисту інформації** (повне визначення буде наведено пізніше). Найбільш ефективний та економічний варіант комплексної системи захисту інформації базується на аналізі всіх можливих загроз інформації та вразливостей інформаційної системи та передбаченні дій потенційного порушника. Тому, розглянемо їх змістовніше.

Загрози інформаційної безпеки класифікуються за низькою ознак:

– за складовими інформаційної безпеки;

– за компонентами інформаційних систем, на які загрози націлені;

– за характером впливу;

– за розміщенням джерела загроз.

Класифікація загроз інформаційної безпеки за її складовими

Класифікація загроз інформаційної безпеки за її складовими полягає у визначенні загроз (загрози), які безпосередньо направлені на таки складові інформаційної безпеки, як **конфіденційність, доступність, цілісність**. Усі загрози, що класифікуються за іншими ознаками можуть впливати на усі складові інформаційної безпеки.

Класифікація загроз інформаційної безпеки за компонентами інформаційних систем, на які вони націлені

Класифікація загроз інформаційної безпеки за компонентами інформаційних систем, на які загрози націлені полягає у визначенні загроз (загрози), які безпосередньо направлені на таки складові інформаційної системи, як інформація, що обробляється в обчислювальної системі, обчислювальна система, програмне забезпечення, апаратура, персонал та інші.

В якості прикладів загроз компонентам інформаційних систем, що суттєво впливають на стан захищеності інформації, можна навести такі:

– зміна архітектури системи;

– зміна складу та/або можливостей апаратних і програмних засобів;

– підключення до мережі (особливо глобальної);

– відмінності в категорії та/або кваліфікації персоналу.

Класифікація загроз інформаційної безпеки за характером впливу

Загрози інформаційної безпеці за характером впливу класифікують як **випадкові та навмисні** дії природного або техногенного характеру.

Випадкові загрози

Випадкові загрози – це загрози, які не пов'язані з умисними діями зловмисників та реалізуються у випадкові моменти часу. Випадкові загрози поділяють на загрози від аварій та стихійних лих, збоїв та відмов технічних засобів, помилок при розробці елементів інформаційної системи, алгоритмічні та програмні помилки, помилки користувачів чи обслуговуючого персоналу та інші (за статистикою – до 65% збитків у порівнянні з іншими загрозами). Реалізація цих загроз веде до найбільшої втрати інформації (за статистикою – до 80% збитків у порівнянні з іншими загрозами). Це – знищення, порушення цілісності, доступності, інколи – конфіденційності інформації.

Треба зазначити, що механізм реалізації випадкових загроз є добре вивченим та існують добре апробовані методи протидії (нейтралізації) таким загрозам. З найефективніших методів протидії випадковим загрозам є спеціальні методи управління якістю розробки та експлуатації програмно-апаратних засобів, методи резервування інформації та інші.

Навмисні загрози

Навмисні загрози – це цілеспрямовані дії зловмисника. Цей клас загроз динамічний, постійно оновлюється новими загрозами, як правило, недостатньо вивчений. Навмисні загрози поділяють на:

– «спеціальні впливи»;
– несанкціонований доступ до інформації;
– використання технічних каналів витоку інформації;
– несанкціоновану зміну структури;
– та інші.

Спроба реалізації будь якої навмисної загрози по відношенню до об'єкту інформаційної діяльності підпадає під дію відповідних статей Карного кодексу України.

«Спеціальні впливи»

«Спеціальні впливи». Загрози інформаційної безпеці від традиційних «спеціальних впливів» до цього часу залишаються актуальними. Частіше за все їх використовують для отримання інформації про систему захисту інформації або її знищення з метою подальшого проникнення до інформаційної системи.

Методами «спеціальних впливів» є:

– підслуховування;
– візуальне спостереження;
– викрадення документів або носіїв інформації;
– викрадення програм або атрибутів системи захисту інформації;
– підкуп або шантаж співробітників;
– сбір та аналіз відходів машинних носіїв інформації;
– підпалення
– та інші.

Підслуховування може здійснюватись на відстані починаючи з одиниць метрів до десятків кілометрів від об'єкту. В приміщеннях підслуховування найбільш часто здійснюється за допомогою мініатюрних магнітофонів або мікрофонів (закладок, радіозакладок, жучків та ін.). Мікрофони фіксують інформацію та здійснюють подальшу її передачу по радіо- чи іншим каналам зв'язку. Суттєвим недоліком цього методу є необхідність попереднього фізичного проникнення на об'єкт з метою розміщення там необхідного обладнання.

Існують засоби зняття інформації (підслуховування) за відбитим від віконного скла променем лазерного випромінювача (відстань – до 1км.). При цьому для підслуховування попереднє проникнення у приміщення не потрібне.

Розмови у сусідніх приміщеннях можуть контролюватись за допомогою стетоскопічних мікрофонів (можлива товщина стін – 50 – 100см.). Для прослуховування розмов у приміщення крім того може використовуватись метод високочастотного нав'язування. Цій метод базується на впливі високочастотного електромагнітного випромінювання на елементи, які здатні модулювати ці поля сигналами, що містять мовну інформацію. Такими елементами можуть бути порожнини з електропровідними поверхнями, телефонний апарат та інше.

Поза приміщеннями підслуховування проводиться за допомогою зверхчутливого мікрофону (відстань – 50 – 100м.).

Порушення інформаційної безпеки може здійснюватись методами та засобами візуального спостереження (дистанційної відеорозвідки). Ці методи використовується не часто та мають допоміжний характер. Засобами візуального спостереження є теле-, фото-, кіно- апаратура. Існують зразки мобільних (у тому числі літаючих) мікроботів візуального спостереження.

Інші методи «спеціальних впливів» характеризувати не будемо.

Несанкціонований доступ до інформації

Несанкціонований доступ до інформації. Серед найбільш розповсюджених загроз інформації є загроза несанкціонованого доступу до інформації (НСД). Несанкціонований доступ до інформації – це доступ до інформації, який порушує правила розмежування доступу (ПРД) з використанням штатних засобів обчислювальної техніки або автоматизованих систем.

Правила розмежування доступу – це сукупність положень, які регламентують права доступу осіб або процесів (суб'єктів доступу) до одиниць інформації (об'єктів доступу). Права доступу до інформаційних ресурсів визначається керівництвом щодо кожного співробітника у відповідності до його функціональних обов'язків.

Виконання правил розмежування доступу реалізується **системою розмежування доступу (СРД)**. Несанкціонований доступ до інформації можливий лише з використанням штатних засобів обчислювальної техніки або автоматизованих систем. Розрізняють наступні джерела виникнення НСД:

– відсутність або помилки СРД;
– збої чи відмова в роботі обчислювальної системи;
– помилкові дії користувачів чи обслуговуючого персоналу;
– фальсифікація повноважень;
– та інші.

Технічні канали витоку інформації

Технічні канали витоку інформації. Технічні канали витоку інформації являють собою небезпечне джерело загроз інформації. Технічні канали витоку інформації – це сукупність об'єкту інформаційної діяльності, технічного засобу зняття інформації та фізичного середовища, в якому розповсюджується інформаційний сигнал.

В основі процесів витоку інформації по технічним каналам є:

– перетворення фізичних величин;

– випромінювання електромагнітних коливань;

– паразитні зв'язки та наведення на дроти та елементи електронних пристроїв.

Процес обробки та передачі інформації технічними засобами супроводжується електромагнітними випромінюваннями в оточуючий простір та наведення електричних сигналів в мережах електричного живлення, лініях зв'язку, сигналізації, заземлення та інших дротах. Таки процеси отримали назву **побічних електромагнітних випромінювань та наведень (ПЕМВН)**. За допомогою спеціального обладнання таки сигнали приймаються, виділяються, підсилюються та можуть спостерігатись чи записуватися. Отримати таки сигнали можна з використанням спеціальних приймачів електромагнітного випромінювання чи приєднавшись безпосередньо до мереж електричного живлення, ліній зв'язку, сигналізації, заземлення та інших. Зняття інформації частіше за все проводиться поза периметром контрольованого доступу об'єкту інформаційної діяльності.

Наведемо таки приклади. Дальність сталого прийому з використанням дипольної антени складає 50 метрів, використання направленої антени та підсилювача може збільшити відстань прийому випромінювання збільшується до 1 кілометра. Прийом та відтворення інформації, яку випромінює неекранований електричний кабель, може здійснюватись на відстані до 300 метрів.

Зловмисник також має можливість знімати та відтворювати «наведену» інформацію безпосередньо підключаючись до мереж електричного живлення, ліній зв'язку, сигналізації, заземлення та інших дротів

Загрози інформації по технічним каналам витоку, у випадку їх реалізації, направлені на **конфіденційність** інформації.

Разом з тим високочастотний електромагнітний імпульс великої потужності може знищити інформацію на магнітних носіях на відстані десятків метрів. Пристрій, здатній генерувати такий імпульс здатний розміщуватись у звичайному дипломаті. Така загроза інформації направлена на **цілісність** інформації. Електромагнітне випромінювання високої потужності може також загрожувати **доступності** інформації, яка передається по каналах мобільного безпровідного зв'язку.

Несанкціонована модифікація структури

Несанкціонована модифікація структури. Цей клас загроз інформації може бути реалізованим на алгоритмічному, програмному або апаратному рівнях на будь якому етапі життєвого циклу обчислювальної системи. Несанкціонована модифікація структури апаратного або програмного засобу на етапах розробки або модернізації отримало назву «закладка».

Програмні або апаратні закладки, призначені для несанкціонованого входу до системи шляхом обходу її засобів захисту отримали назву «люки».

Закладки впроваджують з метою прямого шкідливого впливу на засіб, несанкціонованого входу до системи, дискредитації засобу конкурентом та за іншими міркуваннями.

Закладки, здійсненні на етапі розробки апаратного або програмного засобу виявити дуже важко у зв'язку складності сучасних технологій та високої кваліфікації розробників.

Шкідливі програми

Шкідливі програми. Це один класів загроз інформації, який реалізується шляхом розробки та використання спеціальних програм. У залежності від механізму дії шкідливі програми поділяють на декілька класів. Серед найбільш розповсюджених класів є:

– логічні бомби;

– хробаки;

– троянські коні;

– комп'ютерні віруси та інші.

Логічні бомби – це спеціальні програми, або їх частини, які постійно знаходяться в комп'ютерній системі і активізуються лише за наявності певних умов (наприклад, досягнення певного часу події).

Хробаки – це спеціальні програми, які знаходяться в комп'ютерній системі, здатні до переміщення та самовідтворення. Неконтрольоване розмноження хробаків в комп'ютерній системі, або мережі веде до перевантаження останніх, переповненню пам'яті та блокуванню системи.

Троянські коні – це модифіковані користувацькі програми, які разом з визначеними функціями можуть виконувати додаткові несанкціоновані шкідливі функції.

Комп'ютерні віруси – це невеликі спеціальні програми, здатні до самовідтворення шляхом копіювання та переміщення. За певних обставин віруси можуть бути шкідливими. Вірусам притаманні ознаки майже всіх шкідливих програм. Тому, часто, шкідливі програми називають вірусами.

Класифікація загроз інформаційної безпеки за розміщенням їх джерела

Розрізняють два класи загроз інформації за розміщенням їх джерела в середині інформаційної системи, або поза неї.

Найбільш небезпечною загрозою вважається **внутрішня загроза**, джерелом якої є співробітники установи – користувачі інформаційної системи. Серед користувачів є специфічна категорія – керівництво. Часто, керівники

вимагають собі підвищені привілеї в системі, а також не визнають щодо себе жодних обмежень. До того ж, адміністратори системи формально підпорядковані керівництву, а не навпаки.

Потенційні можливості легального користувача в ІКС значно більші, ніж у будь-якого зовнішнього порушника. Користувач має в системі певні повноваження. Користувач має багато інформації про систему, а іншу інформацію може порівняно легко отримати (когось спитати, підслухати, "неформально" проконсультуватись – йому це значно простіше, ніж будь-якій сторонній особі). Користувач, як правило, незадоволений обмеженнями своїх прав у системі. Користувач цікавиться інформаційними технологіями і бажає перевірити свої досягнення на практиці. Часто користувач не дуже кваліфікований, і все, що він буде робити, фактично зведеться до методу спроб і помилок.

Саме легальні користувачі є найбільшою проблемою адміністраторів, постійно створюючи реальні загрози порушення безпеки інформації. Але, з іншого боку, не користувачі створені для того, щоб заважати адміністраторам, а адміністратори – для того, щоб обслуговувати користувачів. Єдиним можливим виходом з цього становища є взаємна повага і співпраця. Але на це не варто покладатись без відповідного документування прав і обов'язків всіх категорій користувачів і адміністраторів.

Особливості поведінки користувачів (в тому числі керівників) повинні бути враховані ще на стадії проектування КСЗІ в ІКС під час розробки моделі порушника.

Зовнішні загрози визначаються застосуванням обчислювальних мереж. Враховуючи те, що окремі компоненти обчислювальних мереж розподілені у просторі, місце розташування зловмисника за визначенням невідомо.

Поняття порушника інформаційної безпеки

В подальшому будемо використовувати терміни **"порушник" і "зловмисник"** у тих значеннях, які було наведено вище.

Нагадаємо, що **порушниками** називають особи, які реалізують загрози. **Порушник** – фізична особа (у загальному випадку не обов'язково користувач системи), яка здійснює порушення політики безпеки системи. Треба розрізняти терміни «порушник» та «**зловмисник**». Останній термін підкреслює умисність порушення, тоді як у загальному випадку порушник може здійснювати порушення неумисно (наприклад, через необережність або недостатню обізнаність).

Іноді будемо використовувати термін **"хакер"** (англ. – hacker) по відношенню до тих, хто глибоко розуміє принципи роботи обчислювальних систем, особливо ПЗ. Ці знання дозволяють їм виявляти вразливості систем. Тобто, хакери – це ті, хто знаходять вразливості і знають, як їх використати.

Погляди на застосування терміну "хакер" різняться. Деякі фахівці вважають, що справжні хакери – це ті, хто діє виключно в інтересах безпеки інформації (так звані "білі хакери", англ. – "white hats"). Про виявлені вразливості такі хакери повідомляють лише тих, хто повинен виправити помилки

ПЗ, які і спричинили наявність вразливості. Такі хакери можуть тісно співпрацювати з розробниками ПЗ і з експертами з комп'ютерної безпеки.

Існують люди, які мають кваліфікацію хакерів, але використовують свої знання і уміння або з корисливою метою, або взагалі з метою вандалізму. Згадані вище фахівці вважають, що називати хакерами таких зловмисників некоректно. Їх пропонують називати іншими термінами, як, наприклад, **"кракер"** (англ. – "cracker"), що іноді перекладають як **"зломник"**.

У масовій свідомості, саме зі словом "хакер" пов'язані всі комп'ютерні зловмисники. До речі, існує значна частина зловмисників, які не мають високої кваліфікації. Для здійснення атаки достатньо знайти необхідний інструментарій і інструкції з його використання, все це доступно в Інтернет будь-кому.

Результатом аналізу можливих загроз є **модель загроз** – абстрактний структурований опис загроз.

Нормативними документами України рекомендовано таку структуру опису загрози:

На порушення яких властивостей інформації або ІКС спрямована загроза:

– порушення конфіденційності,

– порушення цілісності,

– порушення доступності інформації,

– порушення спостереженості та керованості ІКС.

Джерела виникнення загрози:

– які суб'єкти ІКС або суб'єкти, зовнішні по відношенню до неї, можуть ініціювати загрозу (див. вище модель порушника).

Можливі способи здійснення загрози:

– технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо- та радіотехнічні, хімічні та інші канали;

– каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;

– несанкціонованим доступом шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп'ютерних вірусів.

Перші два способи за принципом відносяться до фізичного доступу, останній – до логічного доступу.

6.4. Модель вразливостей

У комп'ютерній безпеці термін «**вразливість**» (англ. *vulnerability*, на сленгу – *дірка*) використовується для позначення нестачі в системі, використовуючи який можна навмисно порушити її цілісність і викликати неправильну роботу. Вразливість може бути результатом помилок програмування, недоліків, допущених при проектуванні системи, ненадійних

паролів, вірусів та інших шкідливих програм, скриптових та SQL-ін'єкцій. Деякі вразливості відомі тільки теоретично, інші активно використовуються і мають відомі експлойти.

Зазвичай вразливість дозволяє атакуючому «обдурити» додаток – виконати непередбачені творцем дії або змусити програму вчинити дію, на яку той не повинен мати рацію. Це робиться шляхом впровадження у програму даних або коду в такі місця, що програма сприйме їх як «свої». Деякі вразливості з'являються через недостатню перевірку даних, що вводяться користувачем, і дозволяють вставити в інтерпретований код довільні команди (SQL-ін'єкція, XSS, SiXSS). Інші вразливості виникають через складніші проблеми, такі як порушення безпеки при роботі з пам'яттю, наприклад переповнення буфера. Пошук вразливостей іноді називають *зондуванням*, наприклад коли говорять про зондування віддаленого комп'ютера – мають на увазі, пошук відкритих мережевих портів і наявність вразливостей, пов'язаних із додатками, які використовують ці порти.

Метод інформування про вразливість є одним із пунктів суперечки у спільноті комп'ютерної безпеки. Деякі фахівці відстоюють негайне повне розкриття інформації про вразливість, як тільки їх знайдено. Інші радять повідомляти про вразливості лише тим користувачам, які наражаються на найбільший ризик, а повну інформацію публікувати лише після затримки або не публікувати зовсім. Такі затримки можуть дозволити тим, хто був повідомлений, виправити помилку за допомогою розробки та застосування патчів, але також можуть збільшувати ризик для тих, хто не посвячений у деталі.

Існують інструментальні засоби, які можуть допомогти у виявленні вразливостей у системі. Хоча ці інструменти можуть забезпечити аудитору хороший огляд можливих вразливостей, які у системі, вони можуть замінити участь людини у оцінці.

Для забезпечення захищеності та цілісності системи необхідно постійно стежити за нею: встановлювати оновлення, використовувати інструменти, які допомагають протидіяти можливим атакам. Вразливості виявлялися у всіх основних операційних системах, включаючи Microsoft Windows, Mac OS, різні варіанти UNIX (у тому числі GNU/Linux) та OpenVMS. Так як нові вразливості знаходять безперервно, єдиний шлях зменшити ймовірність їх використання проти системи – постійна пильність та використання оновлених версій програмного забезпечення.

Виявлення вразливостей

Для виявлення вразливостей проводяться пентести, в ході яких зазвичай визначається перелік систем, що перевіряються, і конкретна мета, а потім аналізується доступна інформація і підбираються засоби для досягнення цієї мети. Метою тесту проникнення може бути " *білий ящик* " (про який попередня і системна інформація надається тестувальнику заздалегідь) чи " *чорний ящик* " (про який надається лише основна інформація – якщо така є – крім назви компанії).

Система управління інформаційною безпекою

Набір політик, що стосуються системи менеджменту інформаційної безпеки (ISMS), був розроблений для управління контрзаходами, щоб стратегія безпеки була реалізована відповідно до правил і положень, що застосовуються до цієї організації.

Моделі вразливості та факторів ризику

Ресурс (фізичний чи логічний) може мати одну або кілька вразливостей, якими може скористатися зловмисник. Результат може потенційно поставити під загрозу конфіденційність, цілісність чи доступність ресурсів, що належать організації та/або іншим залученим сторонам (клієнтам, постачальникам).

Приклади вразливостей

Поширені типи вразливостей включають:

– Порушення безпеки доступу до пам'яті, такі як:
  - Переповнення буфера. **Переповнення буфера** (англ. *Buffer Overflow*) – явище, що виникає, коли комп'ютерна програма записує дані поза виділеного у пам'яті буфера. Переповнення буфера зазвичай виникає через неправильну роботу з даними, отриманими ззовні, і пам'яттю, за відсутності жорсткого захисту з боку підсистеми програмування (компілятор або інтерпретатор) та операційної системи. В результаті переповнення можуть бути зіпсовані дані, розташовані за буфером (або перед ним). Переповнення буфера є одним з найбільш популярних способів злому комп'ютерних систем, оскільки більшість мов високого рівня використовує технологію стекового кадру – розміщення даних у стеку процесу, змішуючи дані програми з керуючими даними (у тому числі адреси початку стекового кадру та адреси повернення з виконуваної функції). Переповнення буфера може викликати аварійне завершення або зависання програми, що веде до *відмови обслуговування* (Denial of Service, DoS). Окремі види переповнень, наприклад, переповнення в стековому кадрі, дозволяють зловмиснику завантажити і виконати довільний машинний код від імені програми та з правами облікового запису, від якого вона виконується.
  - Висячі покажчики. **Висячий покажчик** або **висяче посилання** (англ. *Dangling pointer, wild pointer, dangling reference*) – покажчик, що не вказує на допустимий об'єкт відповідного типу. Це особливий випадок порушення безпеки пам'яті. Висячі покажчики виникають тоді, коли об'єкт видалений або переміщений без зміни значення покажчика на нульове, так що покажчик все ще вказує область пам'яті, де раніше зберігалися дані. Оскільки система може перерозподілити раніше звільнену пам'ять (у тому числі в інший процес), то обірваний покажчик може призвести до непередбачуваної поведінки програми. Якщо програма записує дані в пам'ять, використовуючи такий покажчик, дані можуть непомітно руйнуватися, що призводить до тонких помилок, які дуже важко

знайти. Цей вид помилок дуже небезпечний, і поряд з витоком пам'яті трапляється досить часто. Ряд мов знижують ймовірність появи висячих покажчиків, зокрема, використовуючи автоматичне складання сміття або іншими методами, підвищуючи безпеку доступу до пам'яті.

– Помилки перевірки даних, такі як:
  - Помилки форматуючого рядка.
  - Неправильна підтримка інтерпретації метасимволів командної оболонки.
  - SQL-ін'єкція. **Впровадження SQL-коду** (англ. *SQL injection/SQLi*) – один із поширених способів злому сайтів і програм, що працюють з базами даних, заснований на впровадженні в запит довільного SQL -коду. Впровадження SQL, залежно від типу використовуваної СУБД та умов впровадження, може дати можливість атакуючому виконати довільний запит до бази даних (*наприклад, прочитати вміст будь-яких таблиць, видалити, змінити або додати дані*), отримати можливість читання та/або запису локальних файлів та виконання довільних команд на сервері, що атакується. Атака типу застосування SQL може бути можлива через некоректну обробку вхідних даних, що використовуються в SQL-запитах. Розробник прикладних програм, що працюють з базами даних, повинен знати про такі вразливості та вживати заходів протидії впровадженню SQL.
  - Ін'єкція коду.
  - Ін'єкція E-mail. **E-mail-ін'єкція** – це техніка атаки, яка використовується для експлуатації поштових серверів і поштових додатків, що конструюють IMAP/SMTP вирази з введеного користувачем, який не перевіряється належним чином. Залежно від типу операторів, які використовуються зловмисником, виділяють два типи ін'єкцій: **IMAP ін'єкція** та ін'єкція **SMTP**. IMAP/SMTP ін'єкції дозволяють отримати доступ до поштового сервера, якого раніше доступу не було. У деяких випадках ці внутрішні системи не мають такого самого рівня безпеки, що й решта інфраструктури. Таким чином, зловмисники можуть виявити, що поштовий сервер дає найкращі результати з точки зору експлуатації. Цей метод дозволяє уникнути можливих обмежень, які можуть існувати на рівні додатків (CAPTCHA, максимальна кількість звернень тощо).
  - Обхід каталогів.
  - Міжсайтовий скриптинг у веб-додатках. **XSS** (англ. *Cross-Site Scripting* – «міжсайтовий скриптинг ») – тип атаки на веб-системи, що полягає у впровадженні у сторінку шкідливого коду, що видається веб-системою (який буде виконаний на комп'ютері користувача при відкритті ним цієї сторінки) і взаємодії цього коду з веб-сервер зловмисника. Є різновидом атаки «Впровадження коду». Специфіка подібних атак полягає в тому, що шкідливий код

може використовувати авторизацію користувача у веб-системі для отримання до неї розширеного доступу або отримання авторизаційних даних користувача. Шкідливий код може бути вставлений у сторінку як через вразливість у веб-сервері, так і через вразливість на комп'ютері. Для терміну використовують скорочення XSS, щоб не було плутанини з каскадними таблицями стилів, що використовують скорочення CSS. XSS знаходиться на третьому місці в рейтингу ключових ризиків Web-додатків, згідно з OWASP 2021. Довгий час програмісти не приділяли їм належної уваги, вважаючи їх безпечними. Однак це думка помилкова: на сторінці або в HTTP-Cookie можуть бути дуже вразливі дані (наприклад, ідентифікатор сесії адміністратора або номери платіжних документів), а там, де немає захисту від CSRF, атакуючий може виконати будь-які дії, доступні користувачеві. Міжсайтовий скриптинг може бути використаний для проведення DoS-атаки.

- Міжсайтовий скриптинг за наявності SQL-ін'єкції. **SiXSS** (англ. *Sql Injection Cross Site Scripting* – "Міжсайтовий скриптинг за наявності SQL-ін'єкції") - тип атаки на вразливі інтерактивні інформаційні системи в Інтернеті; впровадження виконуваних на клієнтському комп'ютері шкідливих скриптів у сторінку, що видається системою, за допомогою впровадження коду в SQL-ін'єкцію. Як правило, дана вразливість виникає на стороні клієнта за наявності виведення принтабельних полів за допомогою виконання SQL-ін'єкції.

– Стан гонки, (англ. *race condition*), також **конкуренція** – помилка проектування багатопоточної системи або програми, при якій робота системи або програми залежить від того, в якому порядку виконуються частини коду. Свою назву помилка отримала від схожої помилки проектування електронних схем. Термін *стан гонки* відноситься до інженерного жаргону і виник внаслідок неакуратного дослівного перекладу англійського еквівалента. У суворішому академічному середовищі прийнято використовувати термін **невизначеність паралелізму**. Стан гонки – "плаваюча" помилка (гейзенбаг), що виявляється у випадкові моменти часу і "зникла" при спробі її локалізувати. До них відносяться вразливості такі як:

- Помилки часу-перевірки-до-часу-використання.
- Перегони символьних посилань.

– Помилки плутанини привілеїв, такі як:

- Підробка міжсайтових запитів у веб-додатках. **CSRF** (англ. *cross-site request forgery* – «міжсайтова підробка запиту», також відома як XSRF) – вид атак на відвідувачів веб-сайтів, що використовує недоліки протоколу HTTP. Якщо жертва заходить на сайт, створений зловмисником, від її особи таємно надсилається запит на інший сервер (наприклад, на сервер платіжної системи), який здійснює якусь шкідливу операцію (наприклад, переказ грошей на рахунок зловмисника). Для здійснення даної атаки жертва повинна бути автентифікована на сервері, на який надсилається запит, і цей запит

не повинен вимагати будь-якого підтвердження з боку користувача, яка не може бути проігнорована або підроблена атакуючим скриптом. Даний тип атак, всупереч поширеній помилці, з'явився досить давно: перші теоретичні міркування з'явилися в 1988, а перші вразливості були виявлені в 2000. А сам термін запровадив Пітер Уоткінс у 2001 році. Основне застосування CSRF – вимушення виконання будь-яких дій на вразливому сайті від імені жертви (зміна пароля, секретного питання відновлення пароля, пошти, додавання адміністратора тощо. буд.). Також за допомогою CSRF можлива експлуатація відбитих XSS, виявлених на іншому сервері.

– Ескалація привілеїв, **Підвищення привілеїв** – це використання комп'ютерного бага, вразливостей, помилок у конфігурації операційної системи або програмного забезпечення з метою підвищення рівня доступу до обчислювальних ресурсів, які зазвичай захищені від користувача. У результаті, додаток, що має більші повноваження, ніж передбачалося системним адміністратором, може здійснювати неавторизовані дії. "Підвищенням привілеїв" називають ситуацію, коли користувач комп'ютерної системи якимось чином підвищує свої повноваження в цій системі (іншими словами: отримав можливість робити те, чого раніше робити не міг). Така помилка в програмі, як використання коду через переповнення буфера, завжди небажана. Однак, серйозною цю помилку можна вважати лише в тому випадку, якщо вона підвищує привілеї користувача. Зокрема, якщо використання коду відбувається на локальній машині, це привілей не підвищує: користувач і без цього може виконувати файли, що виконуються. Якщо ж вдається впровадити код через мережу, то це вже підвищення привілеїв: у користувача з'явилася можливість виконувати машинний код. До цього типу відносяться вразливості такі як:

- Шатерна атака. **"Підривна атака"** (англ. *shatter attack*) – програмна технологія, яка використовується хакерами для обходу обмежень безпеки між процесами одного сеансу в операційній системі Microsoft Windows. Вона спирається на брак архітектури системи передачі повідомлень і дозволяє одному додатку впровадити довільний код в будь-який інший додаток або службу, що працюють у тому самому сеансі. В результаті може статися несанкціоноване підвищення привілеїв.

– Вразливість нульового дня. **0-day** (англ. *zero day*) – термін, що позначає неусунені вразливості, а також шкідливі програми, проти яких ще не розроблені захисні механізми. Сам термін означає, що у розробників було 0 днів на виправлення дефекту: вразливість або атака стає публічно відома до моменту випуску виробником ПЗ виправлень помилки (тобто потенційно вразливість може експлуатуватися на копіях, що працюють, програми без можливості захиститися від неї).

– Недекларовані можливості. У контексті інформаційної безпеки в центрі уваги виявляються функціональні можливості програмного забезпечення, використання яких може порушити його правильну роботу, а також цілісність, доступність або конфіденційність інформації. Вітчизняні стандарти

інформаційної безпеки для таких недокументованих можливостей запроваджують спеціальне поняття – **недекларовані можливості** (скор. **НДМ**), що застосовується, зокрема, під час сертифікації програмного забезпечення.

Аналіз вразливостей

Під аналізом вразливостей розуміються процеси, спрямовані на пошук будь-яких загроз, вразливих точок та ризиків потенційного несанкціонованого проникнення зловмисників у ІС (інформаційну систему).

Вразливість – слабкий компонент ІС будь-якої організації. Загроза – можливість негативного впливу з боку зловмисників, що може спричинити компрометацію комерційної та іншої конфіденційної інформації. Третя особа у такому аналізі – зловмисник, який використовує вразливість для реалізації загроз.

Якщо присутні вразливості, це негативно позначається на роботі всього підприємства, оскільки воно стає менш захищеним перед несумлінними конкурентами, це спрощує роботу зловмисників із заподіяння шкоди та дозволяє третім особам отримати доступ до конфіденційних даних.

Джерело загрози може бути як випадковим, так і навмисним. Третій варіант – техногенні та природні фактори, які ніколи не варто виключати.

Кожна загроза має свій список вразливостей, за допомогою яких зловмисник може реалізувати свої плани.

Аудит інформаційної безпеки

Аналіз вразливостей у галузі інформаційної безпеки (ІБ)

Ефективна ІБ забезпечує як захист від крадіжки будь-яких даних із мережі підприємства, а й фінансову захист бізнесу загалом. Підприємства, які хочуть відрізнятися якісною ІБ, постійно працюють над запобіганням:

– витоків будь-яких корпоративних даних;
– віддаленого редагування захищеної інформації;
– зміни рівня захисту від загроз, які можуть спровокувати втрату довіри інвесторів, постачальників, контрагентів тощо.

Загрози можуть мати кілька джерел, тому дуже важливо своєчасно їх класифікувати та створити схему їхнього аналізу. Це дозволить отримати найбільше охоплення потенційних вразливостей у бізнес-процесах підприємства.

В ІБ вкрай важливо дотримуватися чотирьох принципів:

– конфіденційність;
– цілісність;
– доступність;
– достовірність.

Різновиди аналізованих загроз

Щоб провести якісний аналіз вразливостей інформаційної структури, необхідно розрізняти види загроз, які можуть виникнути у системі конкретної організації. Такі небезпеки поділяються на окремі класи.

1 клас. Потенційне джерело загрози, яке може бути:

- безпосередньо в інформаційній системі (ІС);
- в межах видимості ІС (наприклад, пристрої для несанкціонованого звукозапису);
- поза зоною видимості ІС (перехоплення даних у процесі їх відправлення кудись).

2 клас. Вплив на ІС, що може нести:

- активну загрозу (троян, вірус);
- пасивну загрозу (копіювання конфіденційної інформації зловмисником).

3 клас. Метод забезпечення доступу, який може бути реалізований:

- безпосередньо (крадіжка паролів);
- за допомогою нестандартних каналів зв'язку (наприклад, вразливості операційної системи).

Головні цілі атаки на ІТ-інфраструктуру компанії:

- отримання контролю над цінними ресурсами та даними;
- організація несанкціонованого доступу до корпоративної мережі;
- обмеження діяльності підприємства у певній галузі.

Другий метод найчастіше реалізується на замовлення недобросовісних компаній-конкурентів чи політичними діячами.

Що конкретно може загрожувати інформаційній безпеці будь-якого підприємства:

- шкідливе програмне забезпечення;
- шахраї-хакери;
- інсайдери-працівники, які діють зі злими намірами або з необережності;
- природні явища.

Реалізувати загрозу можна кількома способами. Наприклад, організувати перехоплення даних, залишити програмну чи апаратну «закладку» або порушити роботу локальних бездротових корпоративних мереж, організувати доступ до інфраструктури компанії для інсайдерів.

Оцінка ймовірності загроз

Для оцінки ймовірності настання загрози професіоналами застосовується якісна шкала, що складається із трьох рівнів. Розглянемо їх докладніше.

Рівень 1 – Н («низька ймовірність»)

Відрізняється мінімальною ймовірністю появи. Така загроза не має жодних передумов (минулих інцидентів, мотивів) для того, щоб вона була реалізована. Загрози рівня Н, як правило, виникають не частіше ніж 1 раз на 5 – 10 років.

Рівень 2 – С («середня ймовірність»)

Така загроза ймовірність виникнення трохи вища, ніж попередня, тому що в минулому, приміром, вже були подібні інциденти або відомо, що атакуюча

сторона має плани щодо реалізації такої загрози. Загрози з рівнем З призводять до реальних інцидентів приблизно на рік.

Рівень 3 – В («висока ймовірність»)

Загроза має найвищі шанси на реалізацію. На підтвердження цього – статистична інформація, наявність подібних інцидентів у минулому, серйозна мотивація зловмисників. Ймовірна частота виникнення загроз рівня В – раз на тиждень чи частіше.

Методики аналізу вразливостей

Існує кілька способів, за допомогою яких можна провести аналіз вразливостей системи. Один із них заснований на ймовірнісній методиці, і при його застосуванні потрібно спиратися на такі фактори:

– потенціал зловмисника (виявляється шляхом оцінок експертів);
– джерело загрози (де можлива атака – в зоні видимості або за її межами);
– метод впливу (мережевий, апаратний чи соціальний);
– об'єкт загрози (корпоративні дані, засоби для шифрування, передачі, роботи з ними чи співробітники компанії).

У процесі аналізу вразливостей в інформаційній системі дуже важливо враховувати можливі місця дислокації. Щоб це реалізувати, потрібно оперативно виявити та усунути помилки в операційній системі та програмному забезпеченні, а пізніше систематично встановлювати всі патчі безпеки від розробників.

Аналіз вразливостей, які пов'язані з неправильним настроюванням захисних засобів, повинен проводитись регулярно. Ідеальне рішення – налаштувати безперервний моніторинг ІС щодо виникнення вразливостей. Окремо від вищеописаного аналізу обов'язково необхідно проводити певні заходи з робочим персоналом компанії: видавати права доступу до даних та ресурсів, права на встановлення спеціалізованого програмного забезпечення, а також права на копіювання інформації та застосування зовнішніх носіїв даних.

Лекція 7. Захист інформації, що обробляється та зберігається в інформаційно-телекомунікаційних системах (ІКС)

7.1. Процедури ідентифікації, автентифікації, авторизації користувачів.

7.2. Захист ресурсів і процесів в інформаційно-телекомунікаційних системах на основі моделей безпеки (кінцевих автоматів, управління потоками, Bell-LaPadula, Biba, Clark-Wilson, та інші).

7.3. Резервування інформації та компонентів інформаційно-телекомунікаційних системах.

7.1. Процедури ідентифікації, автентифікації, авторизації користувачів

Захист інформації, що обробляється та зберігається в інформаційно-телекомунікаційних системах відбувається згідно закону України «Про захист інформації в інформаційно-комунікаційних системах». Відповідно до цього закону наводиться наступне визначення:

Інформаційно-комунікаційна система – сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле.

Інформаційна (автоматизована) система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів.

Електронна комунікаційна система – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання та/або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

Захист інформації в системі – діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі.

Комплексна система захисту інформації – взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації.

Для захисту інформації, що обробляється та зберігається в інформаційно-телекомунікаційних системах використовуються процедури ідентифікації, автентифікації й авторизації необхідні для підтвердження істинності суб'єкта, забезпечення його роботи в системі, і визначення законності прав суб'єкта на даний об'єкт або на визначені дії з ним.

Ідентифікація – це процес розпізнавання елемента системи, зазвичай за допомогою заздалегідь визначеного ідентифікатора або іншої унікальної інформації; кожний суб'єкт або об'єкт системи повинний бути однозначно ідентифікуємим.

Автентифікація – це перевірка істинності ідентифікації користувача, процесу, пристрою або іншого компоненту системи (звичайно здійснюється перед дозволом доступу); а також перевірка цілісності й авторства даних при їхньому збереженні або передачі для запобігання несанкціонованої модифікації.

Авторизація – це надання суб'єкту прав на доступ до об'єкта.

Приведемо приклад з доступом в онлайн-банкінг. Кожну дію користувача й системи розглянемо докладно.

Перебуваючи на сайті банку, користувач вирішує зайти в особистий кабінет, щоб зробити грошовий переказ. На сторінці особистого кабінету система спочатку просить ввести ідентифікатор. Це може бути логін, ім'я й прізвище, адреса електронної пошти або номер мобільного телефону.

Який конкретно вид даних необхідно ввести – залежить від ресурсу. Дані, які вказувалися при реєстрації, необхідно ввести для одержання доступу. Якщо при реєстрації вказувалося кілька типів даних – і логін, і адреса електронної пошти, і номер мобільного, то система сама підкаже що їй конкретно потрібно.

Введення цих даних необхідний для ідентифікації людини за монітором як користувача конкретно цього банку.

Якщо користувач як ідентифікатор увів «Олександр Ковальчук», і система знайшла у своїй базі запис про користувача з таким іменем, то ідентифікація завершилася.

Після ідентифікації випливає процес автентифікації, у якому користувачеві потрібно довести, що він є людиною, яка реєструвалася під іменем Олександр Ковальчук.

Для доказу необхідна наявність одного з типів автентифікаційних даних:

- Щось, властиве тільки користувачеві. Біометричні дані: сканери особи, відбитки пальців або сітківки ока.
- Щось, відоме тільки користувачеві. Сюди ставляться pin-коди, паролі, графічні ключі, секретні слова.
- Щось, наявне в користувача. У даній якості може виступати токен, тобто компактний пристрій, призначене для забезпечення інформаційної безпеки користувача, також використовується для ідентифікації власника. Найпростіші токени не вимагають фізичного підключення до комп'ютера – у них є дисплей, де відображається число, яке користувач уводить у систему для здійснення входу; більш складні підключаються до комп'ютерів за допомогою USB і Bluetooth-Інтерфейсів.

Найпоширеніший тип автентифікаційних даних – це пароль. Саме тому так важливо створювати й правильно зберігати свої паролі.

Після введення користувачем пароля система перевіряє: чи відповідає умовний пароль «Q45fp02@13» користувачеві з іменем Олександр Ковальчук. У такий спосіб відбувається автентифікація.

Якщо всі вірно, і пари логін-пароль вірні, то система надасть користувачеві доступ до його ресурсів і здійснення банківських операцій, тобто відбудеться авторизація.

Описані процеси завжди відбуваються тільки в такому порядку: ідентифікація, автентифікація, авторизація. Увесь ланцюжок втратить зміст, якщо, наприклад, сайт спочатку надасть доступ до коштів користувача, а потім буде уточнювати, чи він це насправді.

Процеси ідентифікації, автентифікації й авторизації характерні не тільки для онлайн-банкінгу, але й для електронної пошти, соціальних мереж і інших ресурсів.

Розглянемо яким чином реалізуються ці процедури.

Ідентифікація

Ідентифіка́ція: (лат. *identifico* – ототожнювати) – процедура розпізнавання користувача в системі, як правило, за допомогою наперед визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається системою.

Ідентифікація використовується для отримання інформації про суб'єкт системи на основі наданого ним ідентифікатора. Є початковою процедурою надання доступу до системи. Після неї здійснюється автентифікація та авторизація.

Механізм ідентифікації

Ідентифікація дозволяє суб'єктові (користувачу, процесу, який діє від імені певного користувача) повідомити своє ім'я за допомогою унікального параметра – ідентифікатора (логін, наприклад), який є відомим іншій стороні. Під час ідентифікації здійснюється порівняння заявленого суб'єктом параметра на відповідність відомому іншій стороні. В разі успішної ідентифікації відбувається Автентифікація. Шляхом автентифікації інша сторона переконується що суб'єкт саме той за кого він себе видає (використовується пароль у випадку парольної автентифікації або інший секретний параметр).

Цифровий підпис

Цифровий підпис представлений у комп’ютері у вигляді ряду бінарних цифр. Він обчислюється з використанням таких правил і наборів параметрів, згідно з якими можна перевірити особу, що підписала, і цілісність даних. Цифровий підпис робиться з використанням криптографічної технології, що відома як Криптографія відкритого ключа, на основі унікально зв’язаних пар цифр, де один ключ застосовується для створення підпису (приватний ключ), а другий – для підтвердження підпису (відкритий ключ). В основі цифрового підпису лежать два процеси: генерування підпису і перевірка підпису. При генеруванні підпису застосовується приватний ключ для отримання цифрового підпису. В процесі перевірки підпису використовується відкритий ключ, який відповідає приватному ключу. В кожного користувача є пара ключів підпису: приватний і відкритий. Вважається, що відкриті ключі можуть бути відомі широкому колу осіб. Приватними ж ключами не діляться ні з ким. Кожен може перевірити підпис користувача за допомогою відкритого ключа, що належить цьому користувачу. Зв’язок між відкритим і приватним ключами такий, що неможливо отримати ключ за допомогою розрахунків на основі ключа перевірки.

Інфраструктура відкритого ключа (ІВК) сприяє управлінню і розповсюдженню цим ключем. Цифровий підпис може бути підрозділений на три алгоритми по відношенню до генерування і перевірки, і далі подано їх опис.

Таблиця 7.1 – Приклади ідентифікації

Варіант ідентифікації	**Чинники автентифікації**	**Результат ідентифікації (ідентифікатор)**
Ідентифікація користувача	1) Логін/пароль («я знаю»)	Логін
Ідентифікація по банківській карті	1) мікропроцесорна банківська карта («я маю»); 2) ПІН-код («я знаю»)	Обліковий номер картки (PAN) – зчитується з банківської картки
Ідентифікація по банківській картці з біоверифікацією	1) мікропроцесорна банківська карта («я маю»); 2) біометричний фактор (відбиток пальця) («я є»)	Обліковий номер картки (PAN) – зчитується з банківської картки
Ідентифікація товару за штрих-кодом	1) штрих-код («я маю»)	Обліковий номер товару
Ідентифікація файлу за контрольною сумою	1) контрольна сума («я є»)	ім'я файлу
Ідентифікація громадянина з електронного підпису	1) носій електронного підпису («я маю»); 2) пароль доступу до носія («я знаю»)	Ідентифікатор сертифіката (СНІЛС – для сертифіката ключа перевірки кваліфікованого електронного підпису)

Присвоєння суб'єкту ідентифікатора (тобто реєстрацію суб'єкта в інформаційній системі) іноді також називають ідентифікацією.

Автентифікація

Автентифіка́ція (з грец. αυθεντικός; реальний або істинний) – процедура встановлення належності користувачеві інформації в системі пред'явленого ним ідентифікатора..

З позицій інформаційної безпеки автентифікація є частиною процедури надання доступу для роботи в інформаційній системі, наступною після ідентифікації і передує авторизації.

Механізм автентифікації

Один із способів автентифікації в інформаційній системі полягає у попередній ідентифікації на основі користувацького ідентифікатора («логіна», від англ. *login* – реєстраційного імені користувача) і пароля – певної конфіденційної інформації, знання якої передбачає володіння певним ресурсом в мережі. Отримавши введений користувачем логін і пароль, комп'ютер порівнює їх зі значенням, яке зберігається в спеціальній захищеній базі даних і,

у випадку успішної автентифікації проводить авторизацію з подальшим допуском користувача до роботи в системі.

Види автентифікації

Слабка автентифікація

Традиційну автентифікацію за допомогою пароля називають ще однофакторною або слабкою, оскільки, за наявності певних ресурсів, перехоплення або підбір пароля є справою часу. Не останню роль в цьому грає людський чинник – чим стійкішим до злому методом підбору є пароль, тим важче його запам'ятати людині і тим вища ймовірність, що він буде додатково записаний, що підвищить ймовірність його перехоплення або викрадення. І навпаки – легкі для запам'ятовування паролі (наприклад, часто вживані слова або фрази, дати народження, імена близьких, назви моніторів чи найближчого обладнання) в плані стійкості до злому є дуже не вдалими. Як вихід, впроваджуються одноразові паролі, проте їхнє перехоплення також можливе.

Багатофакторна автентифікація

Автентифікація, що здійснюється з використанням двох чи більше факторів.

Багатофакторна автентифікація (**БФА**, англ. *multi-factor authentication*, MFA) – розширена автентифікація, метод контролю доступу до комп'ютера, в якому користувачеві для отримання доступу до інформації необхідно пред'явити більше одного «доказу механізму автентифікації». До категорій таких доказів відносять:

- Знання – інформація, яку знає суб'єкт. Наприклад, пароль, пін-код.
- Володіння – річ, якою володіє суб'єкт. Наприклад, електронна або магнітна карта, токен, флеш-пам'ять.
- Властивість, якою володіє суб'єкт. Наприклад, біометрія, унікальні природні відмінності: обличчя, відбитки пальців, райдужна оболонка очей, капілярні візерунки, послідовність ДНК.

Фактори автентифікації

Ще до появи комп'ютерів використовувалися різні відмінні риси суб'єкта, його характеристики. Зараз використання тієї чи іншої характеристики в системі залежить від необхідної надійності, захищеності та вартості впровадження. Виділяють 3 фактори автентифікації:

- **Фактор знання, щось, що ми знаємо – пароль**. Це таємні відомості, якими повинен володіти тільки авторизований суб'єкт. Паролем може бути мовне слово, текстове слово, комбінація для замку або особистий ідентифікаційний номер (PIN). Парольний механізм може бути досить легко втілений і має низьку вартість. Але має суттєві недоліки: зберегти пароль у таємниці часто буває складно, зловмисники постійно вигадують нові способи крадіжки, злому і підбору пароля (див. бандитський криптоаналіз, метод грубої сили). Це робить парольний механізм слабозахищеним. Велика кількість секретних питань, такі як «Де ви народилися?», елементарні приклади фактора знань, тому що вони можуть бути відомі широкому загалу людей, або бути досліджені.

– **Фактор володіння, щось, що ми маємо – пристрій автентифікації**. Тут важлива сама обставина володіння суб'єктом якимось особливим предметом. Це може бути особиста печатка, ключ від замка, для комп'ютера це файл даних, що містять характеристику. Характеристика часто вбудовується в особливий пристрій автентифікації, наприклад, пластикова картка, смарт-картка. Для зловмисника роздобути такий пристрій стає більш складно, ніж зламати пароль, а суб'єкт може відразу ж повідомити в разі крадіжки пристрою. Це робить даний метод більш захищеним, ніж парольний механізм, проте вартість такої системи більш висока.

– **Фактор властивості, щось, що є частиною нас – біометрика**. Характеристикою є фізична особливість суб'єкта. Це може бути портрет, відбиток пальця або долоні, голос або особливість очка. З точки зору суб'єкта, даний спосіб є найбільш простим: не треба запам'ятовувати пароль, ні переносити з собою пристрій автентифікації. Однак біометрична система повинна володіти високою чутливістю, щоб підтверджувати авторизованого користувача, але відкидати зловмисника зі схожими біометричними параметрами. Також вартість такої системи досить велика. Але, незважаючи на свої недоліки, біометрика залишається досить перспективним фактором.

Безпека

Багатофакторна автентифікація може істотно зменшити імовірність викрадення особистих даних в інтернеті, оскільки знання пароля жертви недостатньо для здійснення шахрайства. Тим не менш, в залежності від реалізації, системи з багатофакторною автентифікацією можуть бути вразливими для атак типу «фішингу», «людина-в-браузері», «людина посередині», тощо.

Вибираючи для системи той чи інший фактор або спосіб автентифікації, необхідно, насамперед, відштовхуватися від необхідної ступеня захищеності, вартості побудови системи, забезпечення мобільності суб'єкта.

Таблиця 7.2 – Таблиця для порівняння

Рівень ризику	**Вимоги до системи**	**Технологія автентифікації**	**Приклади застосування**
Низький	Потрібно здійснити автентифікацію для доступу до системи, причому крадіжка, злом, розголошення конфіденційних відомостей **не будуть мати значних наслідків**	Рекомендується мінімальна вимога – використання багаторазових паролів	Реєстрація на порталі в мережі Інтернет

Середній	Потрібно здійснити автентифікацію для доступу до системи, причому крадіжка, злом, розголошення конфіденційних відомостей заподіють **невеликий збиток**	Рекомендується мінімальна вимога – використання одноразових паролів	Здійснення банківських операцій
Високий	Потрібно здійснити автентифікацію для доступу до системи, причому крадіжка, злом, розголошення конфіденційних відомостей завдадуть **значної шкоди**	Рекомендується мінімальна вимога – використання багатофакторної автентифікації	Проведення великих міжбанківських операцій керівним апаратом

Двофакторна автентифікація

Двофакторна автентифікація (**ДФА**, англ. *two-factor authentication*, також відома як *двоетапна верифікація*), є типом багатофакторної автентифікації. ДФА – представляє собою технологію, що забезпечує ідентифікацію користувачів за допомогою комбінації двох різних компонентів.

Хорошим прикладом двофакторної автентифікації є авторизація Google і Microsoft. Коли користувач заходить з нового пристрою, крім автентифікації по імені та паролю, його просять ввести шестизначний (Google) або восьмизначний (Microsoft) код підтвердження. Ви можете отримати його за допомогою SMS, або голосового дзвінка на ваш телефон, він може бути взятий з заздалегідь складеного реєстру разових кодів або ви можете використовувати додаток-автентифікатор, генеруючий новий одноразовий пароль за короткі проміжки часу. Вибрати один з методів можна в налаштуваннях вашого Google або Microsoft-акаунта.

Перевага двофакторної автентифікації через мобільний пристрій:

– Не потрібні додаткові токени, тому що мобільний пристрій завжди під рукою.

– Код підтвердження постійно змінюється, а це безпечніше, ніж однофакторний логін-пароль

Недоліки двофакторної автентифікації через мобільний пристрій:

– Мобільний телефон повинен ловити мережу, коли відбувається автентифікація, інакше повідомлення з паролем просто не дійде.

– Ви ділитеся з кимось вашим мобільним телефоном, що впливає на ваше особисте життя і може бути в майбутньому на нього буде приходити спам.

– Текстові повідомлення (SMS), які, потрапляючи на ваш мобільний телефон, можуть бути перехоплені.

– Текстові повідомлення приходять з деякою затримкою, так як деякий час йде на перевірку.

– Сучасні смартфони використовуються як для одержання пошти, так і для отримання SMS. Як правило електронна пошта на мобільному телефоні завжди включена. Таким чином, усі акаунти, для яких пошта є ключем, можуть бути зламані (перший фактор). Мобільний пристрій (другий фактор). Висновок: смартфон змішує два чинника в один.

Зараз майже всі великі сервіси, такі як Microsoft, Google, Yandex, Dropbox, Facebook, вже надають можливість використовувати двофакторну автентифікацію. Причому для всіх з них можна використовувати єдиний додаток *автентифікатор*, що відповідає певним стандартам, такі як Google Authenticator, Microsoft Authentificator, Authy або FreeOTP.

Законодавство та регулювання

Стандарт безпеки даних для індустрії платіжних карток (PCI), вимога 8.3, вимагає використання багатофакторної автентифікації (MFA) для всього віддаленого доступу до мережі, що походить із-за межі мережі, до середовища даних карт (CDE). Починаючи з PCI-DSS версії 3.2, використання MFA потрібне для будь-якого адміністративного доступу до CDE, навіть якщо користувач знаходиться в межах надійної мережі.

Практична реалізація

Багато продуктів з функцією багатофакторної автентифікації вимагають від користувача клієнтське програмне забезпечення, для того, щоб система багатофакторної автентифікації запрацювала. Деякі розробники створили окремі настановні пакети для входу в мережу, ідентифікаційних даних веб-доступу VPN-підключення. Щоб використовувати з цими продуктами токен або смарт-карту, потрібно встановити на PC чотири або п'ять пакетів спеціального програмного забезпечення. Це можуть бути пакети, які використовуються для здійснення контролю версії або це можуть бути пакети для перевірки конфліктів з бізнес-додатками. Якщо доступ може бути проведений з використанням вебсторінок, то тоді можна обійтися без непередбачених витрат. З іншими програмними рішеннями багатофакторної автентифікації, такими як «віртуальні» токени або деякі апаратні токени, жодне не може бути встановлено безпосередніми користувачами.

Багатофакторна автентифікація не стандартизована. Існують різні форми її реалізації. Отже, проблема полягає в її здатності до взаємодії. Існує багато процесів і аспектів, які необхідно враховувати при виборі, розробці, тестуванні, впровадженні та підтримці цілісної системи управління ідентифікацією безпеки, включаючи всі релевантні механізми автентифікації і супутніх технологій: це все описав Brent Williams, в контексті «Identity Lifecycle»

Багатофакторна автентифікація має ряд недоліків, які перешкоджають її поширенню. Зокрема людині, яка не розбирається в цій області, складно стежити за розвитком апаратних токенів або USB-штекерів. Багато користувачів не можуть самостійно встановити сертифіковане програмне забезпечення, так як не володіють відповідними технічними навичками. Загалом, багатофакторні рішення вимагають додаткових витрат на встановлення та оплату експлуатаційних витрат. Багато апаратні комплекси, засновані на токенах,

запатентовані, і деякі розробники стягують з користувачів щорічну плату. З точки зору логістики, розмістити апаратні токени важко, так як вони можуть бути пошкоджені або втрачені. Випуск токенів в таких областях, як банки, або інших великих підприємствах повинен бути відрегульований. Крім витрат на установку багатофакторної автентифікації значну суму також становить оплата технічного обслуговування.

Посилена автентифікація

У відповідності до вимог Європейської директиви PSD2 в платіжних системах використовується так звана посилена автентифікація, коли для автентифікації використовуються принаймні два різних типи факторів. Типами факторів є:

– властивість, якою володіє суб'єкт;
– знання – інформація, яку знає суб'єкт;
– володіння – річ, якою володіє суб'єкт.

Сувора автентифікація

Автентифікація, під час якої використовується інформація без розкриття цієї інформації. Як правило, реалізується за допомогою асиметричних криптографічних алгоритмів.

Способи автентифікації

Парольна

Здійснюється на основі володіння користувачем певною конфіденційною інформацією.

Біометрична

Біометрична автентифікація основана на унікальності певних антропометричних характеристик людини. У галузі інформаційних технологій термін біометрія застосовується в значенні технології ідентифікації особистості. Біометричний захист ефективніший ніж такі методи як, використання смарт-карток, паролів, PIN-кодів. Найчастіше використовуються:

1. Параметри голосу.
2. Візерунок райдужної оболонки ока і карта сітківки ока – Автентифікація за райдужною оболонкою ока.
3. Риси обличчя.
4. Форма долоні.
5. Відбитки пальців.
6. Форма і спосіб особистого підпису – Електронний цифровий підпис, Верифікація підпису.

Етапи

Основні етапи проектування системи біометричної автентифікації на основі динамічного підпису в цілому. Розробка математичної моделі динамічного підпису і методів його обробки. Реалізація алгоритму роботи модуля автентифікації системи на основі створеної математичної моделі і методів обробки. Реалізація системи автентифікації у складі інформаційної

системи. Тестування системи автентифікації. Модифікація коду фрагментів системи у процесі функціонування системи.

Перший етап – проектування, полягає у аналізі вимог, які ставляться до системи і на їх основі проектується архітектура системи автентифікації в цілому. Враховується сфера застосування системи, зокрема задається її точність, надійність, зручність; операційна система (ОС) у якій буде функціонувати ПЗ та інші параметри. У випадку розробки універсальної системи необхідно передбачити можливість зміни цих параметрів інтегратором (адміністратором) системи, а також бажано розробляти кросплатформенне ПЗ, незалежне від ОС. Розробити рольову модель роботи системи – скористатися апаратом об'єктно-орієнтованого аналізу і об'єктно-орієнтованого проектування. Рекомендується використовувати уніфіковану мову програмування UML для проектування і моделювання інформаційної системи, а також дотримуватися наступних принципів: модульність – кожна компонента системи є модулем, який просто модифікується, замінюється і виконує відведену йому специфічну роль; підтримка відкритих стандартизованих протоколів для передачі даних, взаємодії об'єктів і форматів збереження файлів; документованість – усі методи (функції), класи, об'єкти детально і доступно документувати.

Другий етап – розробка математичної моделі є ключовим. Необхідно вдало підібрати підхід до побудови моделі: стохастичний чи детермінований, на думку авторів це стохастичний підхід. Розробка математичної моделі передбачає: розробку моделі, яка враховувала б ключові особливості об'єкта дослідження і вибір діагностичних ознак; проведення аналізу цих діагностичних ознак і розробка методів для попередньої обробки. У випадку використання статистичного підходу – дослідити статистичні характеристики діагностичних ознак. Ці дослідження дозволяють зробити висновки про адекватність моделі.

Третій етап – на основі математичної моделі розробляється алгоритм, який реалізується на деякій мові програмування. Особливу увагу слід привернути на реалізацію системи вводу підпису

За допомогою унікального предмета

Здійснюється за допомогою додаткових предметів (токен автентифікації, смарт-карта) або атрибутів (криптографічний сертифікат).

Протоколи автентифікації

Протоколи автентифікації – категорія криптографічних протоколів, які забезпечують надійну автентифікацію особи.

Існує багато різноманітних протоколів автентифікації:

- AKA.
- CAVE-based authentication.
- Challenge-handshake authentication protocol (CHAP).
- CRAM-MD5.
- Diameter.
- EAP.
- Host Identity Protocol (HIP).
- Kerberos.

- MS-CHAP і MS-CHAPv2 різновиди CHAP.
- LAN Manager.
- NTLM, також відомий як NT LAN Manager.
- Password-authenticated key agreement протоколи.
- Password Authentication Protocol (PAP).
- Protected Extensible Authentication Protocol (PEAP).
- RADIUS.
- Secure Remote Password protocol (SRP).
- TACACS і TACACS+.
- RFID-Authentication Protocols.
- Woo Lam 92 (protocol).
- Протокол Нідхема-Шредера.

Авторизація

Авторизація – керування рівнями та засобами доступу до певного захищеного ресурсу, як у фізичному розумінні (доступ до кімнати готелю за карткою), так і в галузі цифрових технологій (наприклад, автоматизована система контролю доступу) та ресурсів системи залежно від ідентифікатора і пароля користувача або надання певних повноважень (особі, програмі) на виконання деяких дій у системі обробки даних. З позицій інформаційної безпеки Авторизація є частиною процедури надання доступу для роботи в інформаційній системі, після ідентифікації і автентифікації.

7.2. Захист ресурсів і процесів в інформаційно-телекомунікаційних системах на основі моделей безпеки (кінцевих автоматів, управління потоками, Bell-LaPadula, Biba, Clark-Wilson, та інші)

Формальне визначення політики безпеки називають математичною моделлю безпеки. Згідно вимог нормативних документів у галузі захисту інформації в інформаційних системах, системи захисту інформації будують на основі математичних моделей захисту інформації. Використання цих моделей дозволяє теоретично обґрунтувати відповідність системи захисту інформації вимогам заданої політики безпеки. Формальна теорія захисту інформації почала розвиватися відносно недавно, але сьогодні існує багато математичних моделей, які описують різні аспекти безпеки і надають доказову теоретичну базу для побудови сучасних систем захисту інформації

Захист інформації за допомогою кінцевих автоматів

Кінцевий або Скінче́нний автома́т (англ. *finite-state machine*, машина зі скінченною кількістю станів) – особливий різновид автомата – абстракції, що використовується для опису шляху зміни стану об'єкта в залежності від поточного стану та інформації отриманої ззовні. Його особливістю є скінченність множини станів автомату.

Кінцеві автомати – з погляду інформатики це автомати, які є дискретні перетворювачі інформації. До них відносяться перетворювачі, в яких міститься кінцева множина вхідних і кінцеве вихідних сигналів, а також кінцева множина внутрішніх станів

Поняття скінченного автомата було запропоновано як математичну модель технічних приладів дискретної дії, оскільки будь-який такий пристрій (в силу скінченності своїх розмірів) може мати тільки скінченну кількість станів.

Виявлення кіберзагроз з використанням моделі кінцевих автоматів засноване на моделюванні кінцевими автоматами процесів інформаційної взаємодії абонентів інформаційної системи (ІС) за протоколами передачі даних. Кінцевий автомат описується множинами вхідних даних, вихідних даних і внутрішніх станів. Кіберзагрози фіксуються по «аномальним» переходам ІС зі стану в стан. Передбачається, що в ІС «штатні» переходи системи зі стану в стан визначено, а невідомі стану і переходи в ці стану реєструються як аномальні. Перевагою цієї моделі є спрощений підбір класифікаційних ознак для ІС та розгляд малого числа переходів зі стану в стан. Модель дозволяє виявляти кіберзагрози в потоці обробки даних мережевими протоколами в режимі близькому до реального масштабу часу. До недоліків моделі слід віднести необхідність розробки великого числа складних експертних правил для порівняльного аналізу необхідних і аномальних станів і переходів системи. Експертні правила оцінки станів ІС взаємопов'язані з характеристиками мережевих протоколів передачі даних

Захист інформації за допомогою управління потоками

Однією з основних функцій системи розмежування доступу є управління потоками даних з метою запобігання запису даних на носії невідповідного рівня. Для цього використовується **політика безпеки інформаційних потоків**.

Крім керування доступом суб’єктів до об’єктів системи проблема захисту інформації має ще один аспект. Для одержання інформації про який-небудь об’єкт системи зовсім необов'язково шукати шляхи несанкціонованого доступу до нього. Необхідну інформацію можна одержати, спостерігаючи за обробкою необхідного об'єкта, тобто використовуючи канали витоку інформації. У системі завжди існують інформаційні потоки. Тому адміністраторові необхідно визначити, які інформаційні потоки в системі є «легальними», тобто не ведуть до витоку інформації, а як-ведуть до витоку. Тому виникає необхідність розробки правил, що регламентують керування інформаційними потоками в системі. Звичайне керування інформаційними потоками застосовується в рамках виборчої або повноважної політики, доповнюючи їх і сприяючи підвищенню надійності системи захисту.

Захист інформації за допомогою моделі безпеки Bell-LaPadula

Основна теорема безпеки Белла-Лападули вказує, що якщо інформаційна система стартує роботу з безпечного стану і перехід зі стану в стан безпечний, то всі стан системи безпечні.

Модель **Белла-ЛаПадули (BLP)** – це модель кінцевого автомата, яка використовується для забезпечення контролю доступу в державних і військових програмах. Він був розроблений Девідом Елліоттом Беллом і Леонардом Дж. ЛаПадулою за чіткими вказівками Роджера Р. Шелла, щоб формалізувати політику багаторівневої безпеки (MLS) Міністерства оборони США (DoD). Модель є формальною моделлю переходу між станами політики комп'ютерної безпекиякий описує набір правил контролю доступу, які використовують мітки безпеки на об'єктах і дозволи для суб'єктів. Мітки безпеки варіюються від найбільш конфіденційних (наприклад, «Цілком таємно») до найменш чутливих (наприклад, «Несекретно» або «Публічно»).

Модель Белла-ЛаПадули є прикладом моделі, де немає чіткого розмежування між захистом і безпекою.

Особливості

Модель Белла-ЛаПадули фокусується на конфіденційності даних і контрольованому доступі до секретної інформації, на відміну від моделі цілісності Біби, яка описує правила захисту цілісності даних. У цій формальній моделі сутності інформаційної системи поділяються на суб'єкти та об'єкти. Визначено поняття « безпечний стан » і доведено, що кожен перехід стану зберігає безпеку шляхом переходу від безпечного стану до безпечного стану, таким чином індуктивно доводячи, що система задовольняє цілі безпеки моделі. Модель Белла-ЛаПадули побудована на концепції кінцевої машини з набором допустимих станів в комп'ютерній системі. Перехід з одного стану в інший визначається функціями переходу. Стан системи визначається як «безпечний», якщо єдині дозволені режими доступу суб'єктів до об'єктів відповідають політиці безпеки. Щоб визначити, чи дозволений певний режим доступу, дозвіл суб'єкта порівнюється з класифікацією об'єкта (точніше, з комбінацією класифікації та набору відсіків, що становить рівень *безпеки*), щоб визначити, чи суб'єкт авторизований для конкретного режиму доступу. Схема очищення/класифікації виражається в термінах решітки. Модель визначає одне правило дискреційного контролю доступу (DAC) і два обов'язкових контролю доступу(MAC) правила з трьома властивостями безпеки:

1. Проста властивість безпеки стверджує, що суб'єкт із даним рівнем безпеки може не читати об'єкт із вищим рівнем безпеки.

2. Властивість безпеки * (зірочка) вказує на те, що суб'єкт із даним рівнем безпеки не може писати в будь-який об'єкт із нижчим рівнем безпеки.

3. Властивість дискреційної безпеки використовує матрицю доступу для визначення дискреційного керування доступом.

Передача інформації з документа високої конфіденційності до документа меншої конфіденційності може відбуватися в моделі Белла-ЛаПадули через концепцію довірених суб'єктів. Довірені суб'єкти не обмежені власністю Star. Довірені суб'єкти мають бути продемонстровані як надійні щодо політики безпеки.

Модель безпеки Белла-ЛаПадули спрямована на контроль доступу та характеризується фразою «записати, прочитати» (WURD).

За допомогою Bell–LaPadula користувачі можуть створювати вміст лише на своєму власному рівні безпеки або вище (тобто секретні дослідники можуть створювати секретні чи надсекретні файли, але не можуть створювати загальнодоступні файли; без запису). І навпаки, користувачі можуть переглядати вміст лише на рівні безпеки або нижчому (тобто секретні дослідники можуть переглядати загальнодоступні чи секретні файли, але не можуть переглядати надсекретні файли; читання неможливе).

Модель Белла-ЛаПадули чітко визначила її сферу застосування. Він не розглядав наступне широко:

– Приховані канали. Коротко описано передачу інформації за допомогою заздалегідь обумовлених дій.

– Мережі систем. Пізніша модельна робота справді торкалася цієї теми.

– Політики за межами багаторівневої безпеки. Робота на початку 1990-х років показала, що MLS є однією з версій булевих політик, як і всі інші опубліковані політики.

Властивості

Властивість Strong Star

Модель Белла-ЛаПадули є моделлю розмежування доступу до інформації, що захищається. Вона описується скінченним автоматом з допустимим набором станів, у яких може знаходитись інформаційна система. Усі елементи у складі інформаційної системи поділені на суб'єкти і об'єкти. Кожному суб'єкту приписується рівень доступу, який відповідає рівню конфіденційності. Аналогічно об'єкту надається рівень таємності. Поняття захищеної визначається наступним чином: кожен стан системи повинен відповідати політиці безпеки, встановленої для даної інформаційної системи. Перехід між станами описується функціями переходу. Система знаходиться у безпечному стані тільки у тому випадку, коли у кожного суб'єкта наявний доступ тільки до тих об'єктів, до яких від дозволений на основі поточної політики безпеки. Для визначення права доступу суб'єкта до об'єкта рівень доступу суб'єкта порівнюється з рівнем таємності об'єкта, і на підставі цього приймається рішення щодо надання запитаного рівня доступу. Набори рівень доступу/рівень таємності описуються матрицею доступу. Основними правилами, що забезпечують розмежування доступу, є:

Проста властивість безпеки (The Simple Security)

Суб'єкт з рівнем доступу x_s може читати інформацію з об'єкта з рівнем таємності x_o тоді і тільки тоді, коли x_sперевищує x_o. Це правило також відоме під назвою «Немає читання зверху» (No read up, NRU). Наприклад, суб'єкт, який має доступ лише до нетаємних даних, спробує прочитати об'єкт з рівнем «цілком таємно», то йому буде відмовлено.

Властивість ★ (The ★-property)

Сутність властивості ★ (читається як «властивість зірочка») полягає у тому, що суб'єкт з рівнем доступу $_s$ може писати інформацію у об'єкт з рівнем таємності x_o тільки якщо x_o перевищує x_s. Це правило також відоме під назвою «Немає запису вниз» (No write down, NWD). Наприклад, якщо суб'єкт, який має

рівень доступу «цілком таємно» спробує записати у об'єкт з рівнем таємності «таємно», то йому буде відмовлено у цьому.

Сильна властивість ★ (Strong ★ Property)

Сильна властивість ★ є альтернативною властивості ★, у якій суб'єкти можуть писати у об'єкти тільки з тим рівнем таємності, що відповідає рівню доступу суб'єкта. Таким чином, операція запису вгору, присутня при властивості ★, відсутня, а лише наявна операція запису у об'єкти з тим же рівнем доступу. Сильна властивість ★ зазвичай згадується у контексті багаторівневих систем керування базами даних і обумовлена вимогами цілісності[4]. Сильна властивість ★ передбачається моделлю Біби, де було показано, що стійка цілісність у поєднанні з моделлю Белла-ЛаПадули забезпечується читанням і записом у межах єдиного рівня таємності.

Принцип стійкості

Принцип стійкості моделі Белла-ЛаПадули стверджує, що рівень таємності/доступу суб'єкта або об'єкта не змінюється під час звернення. Є дві форми принципу стійкості. Принцип сильної стійкості стверджує, що рівень безпеки не зміниться під час нормальної роботи системи. Принцип слабкої стійкості стверджує, що рівень безпеки неможливо змінити таким чином, що порушилась політика безпеки. Принцип слабкої стійкості дозволяє дотримуватися принципу мінімуму повноважень у системі. Тобто процеси починаються з низьким рівнем ознайомленості, незалежно від рівня ознайомленості їх власників, і у процесах поступово накопичуються більш високі рівні обізнаності, по мірі потреби у діях, які вимагають підвищення рівня обізнаності.

Захист інформації за допомогою моделі безпеки Biba

Модель **Biba** або Модель **цілісності Biba**, розроблена Кеннетом Дж. Бібою в 1975 році, є формальною системою переходу між станами політики комп’ютерної безпеки, яка описує набір правил контролю доступу, призначених для забезпечення цілісності даних. Дані та суб’єкти групуються в упорядковані рівні цілісності. Модель розроблена таким чином, що суб’єкти не можуть пошкодити дані на рівні, вищому за суб’єкта, або бути зіпсованими даними з нижчого рівня, ніж суб’єкт.

Загалом модель була розроблена для розгляду цілісності як основного принципу, який є прямою протилежністю моделі Белла-ЛаПадули.

Особливості

Загалом, збереження *цілісності* даних має три цілі:

– Запобігайте зміні даних неавторизованими сторонами.

– Запобігайте неавторизованій зміні даних авторизованими сторонами.

– Підтримувати внутрішню та зовнішню узгодженість (тобто дані відображають реальний світ).

Ця модель безпеки спрямована на *цілісність* даних (а не на *конфіденційність*) і характеризується фразою: «читай, записуй». Це на відміну від моделі Белла-ЛаПадули, яка характеризується фразою «читай, записуй».

У моделі Biba користувачі можуть *створювати вміст лише на* рівні власної цілісності або нижче (ченець може написати молитовник, який можуть читати простолюдини, але не такий, який читатиме первосвященик). І навпаки, користувачі можуть *переглядати вміст лише на* рівні власної цілісності або вище (монах може читати книгу, написану первосвящеником, але не може читати брошуру, написану простолюдином). Інша аналогія, яку слід розглянути, це ланка військового командування. Генерал може писати накази полковнику, який може віддавати ці накази майору. Таким чином оригінальні накази генерала зберігаються недоторканими, а місія військових захищена (таким чином, «читайте» цілісність). І навпаки, рядовий ніколи не може віддавати накази своєму сержанту, який ніколи не може віддавати накази лейтенанту, також захищаючи цілісність місії («записати»).

Модель Біба визначає набір правил безпеки, перші два з яких подібні до моделі Белла-ЛаПадули. Ці перші два правила є протилежними правилам Белла-ЛаПадули:

1. Проста властивість цілісності стверджує, що суб'єкт із заданим рівнем цілісності не повинен зчитувати дані з нижчим рівнем цілісності (*без зчитування*).

2. Властивість цілісності * (зірочка) вказує на те, що суб'єкт із заданим рівнем цілісності не повинен записувати дані з вищим рівнем цілісності (*не записувати*).

3. Властивість виклику стверджує, що процес знизу не може запитувати вищий доступ; лише з предметами рівного або нижчого рівня.

Захист інформації за допомогою моделі безпеки Clark-Wilson

Модель цілісності **Кларка-Вілсона** забезпечує основу для визначення та аналізу політики цілісності для обчислювальної системи.

Модель в першу чергу стосується формалізації поняття інформаційної цілісності. Цілісність інформації підтримується шляхом запобігання пошкодженню елементів даних у системі через помилку або зловмисний намір. Політика цілісності описує, як елементи даних у системі повинні підтримуватися дійсними від одного стану системи до наступного, і визначає можливості різних принципалів у системі. Модель використовує мітки безпеки для надання доступу до об'єктів за допомогою процедур трансформації та моделі обмеженого інтерфейсу.

Модель була описана в статті 1987 року (*Порівняння комерційної та військової політики комп'ютерної безпеки*) Девіда Д. Кларка та Девіда Р. Вілсона. У статті розроблено модель як спосіб формалізації поняття цілісності інформації, особливо порівняно з вимогами до систем багаторівневої безпеки (MLS), описаними в Помаранчевій книзі. Кларк і Вілсон стверджують, що існуючі моделі цілісності, такі як Biba (читання/запис), краще підходили для забезпечення цілісності даних, а не конфіденційності інформації. Біба-моделі є більш корисними, наприклад, у системах банківської класифікації, щоб запобігти ненадійній модифікації інформації та спотворенню інформації на вищих рівнях класифікації. Навпаки, **Кларка–Вілсона** більш чітко можна застосувати до

бізнес-процесів і галузевих процесів, у яких цілісність інформаційного вмісту має першочергове значення на будь-якому рівні класифікації (хоча автори підкреслюють, що всі три моделі, очевидно, корисні як урядовим, так і промисловим організаціям).

Основні принципи

Відповідно до навчального посібника CISSP Стюарта та Чеппла, *шосте видання*, модель Кларка–Вілсона використовує багатогранний підхід для забезпечення цілісності даних. Замість визначення формального кінцевого автомата, модель визначає кожен елемент даних і дозволяє модифікувати лише невеликий набір програм. Модель використовує зв'язок із трьох частин суб'єкт/програма/об'єкт (де програма взаємозамінна з транзакцією), відомий як *трійка* або *трійка контролю доступу.* У межах цього відношення суб'єкти не мають прямого доступу до об'єктів. Доступ до об'єктів можливий лише через програми. Подивіться тут, щоб побачити, чим це відрізняється від інших моделей контролю доступу.

Правила застосування та сертифікації моделі визначають елементи даних і процеси, які є основою для політики цілісності. Ядро моделі базується на понятті транзакції.

– Добре сформована транзакція – це серія операцій, які переводять систему з одного узгодженого стану в інший узгоджений стан.

– У цій моделі політика цілісності стосується цілісності транзакцій.

– Принцип розподілу обов'язків вимагає, щоб засвідчувач транзакції та виконавець були різними особами.

Модель містить ряд базових конструкцій, які представляють як елементи даних, так і процеси, які працюють з цими елементами даних. Ключовим типом даних у моделі Кларка–Вілсона є обмежений елемент даних (CDI). Процедура перевірки цілісності (IVP) гарантує, що всі CDI в системі дійсні в певному стані. Транзакції, які забезпечують дотримання політики цілісності, представлені процедурами перетворення (TP). TP приймає як вхідні дані CDI або Unconstrained Data Item (UDI) і створює CDI. TP має перевести систему з одного дійсного стану в інший. UDI представляють вхідні дані системи (наприклад, дані, надані користувачем або зловмисником). TP має гарантувати (через сертифікацію), що він перетворює всі можливі значення UDI на «безпечний» CDI.

Правила

В основі моделі лежить поняття зв'язку між автентифікованим принципалом (тобто користувачем) і набором програм (тобто TP), які працюють з набором елементів даних (наприклад, UDI та CDI). Компоненти такого відношення, взяті разом, називають *трійкою Кларка–Вілсона.* Модель також має гарантувати, що різні сутності відповідають за маніпулювання зв'язками між принципалами, транзакціями та елементами даних. Як короткий приклад, користувач, здатний сертифікувати або створювати відношення, не повинен мати можливість виконувати програми, вказані в цьому відношенні.

Модель складається з двох наборів правил: правил сертифікації (C) і правил виконання (E). Дев'ять правил забезпечують зовнішню та внутрішню цілісність елементів даних. Перефразовуючи це:

– C1 – коли виконується IVP, він повинен забезпечити дійсність CDI.

– C2 – для певного пов’язаного набору CDI TP має перетворити ці CDI з одного дійсного стану в інший.

Оскільки ми повинні переконатися, що ці TP сертифіковані для роботи на конкретному CDI, ми повинні мати E1 і E2.

– E1 – система повинна підтримувати список сертифікованих зв’язків і гарантувати, що тільки TP, сертифіковані для роботи на CDI, змінюють цей CDI.

– E2 – система повинна пов’язати користувача з кожним TP і набором CDI. TP може отримати доступ до CDI від імені користувача, якщо це "легально".

– E3-Система повинна ідентифікувати особу кожного користувача, який намагається виконати TP.

Це вимагає відстеження трійок (користувач, TP, {CDI}), які називаються «дозволеними зв’язками».

– C3 – Дозволені стосунки мають відповідати вимогам «розподілу обов’язків».

Нам потрібна автентифікація, щоб відстежувати це.

– C4 – усі TP повинні додати до журналу достатньо інформації для реконструкції операції.

Коли інформація надходить у систему, їй не потрібно довіряти чи обмежуватись (тобто вона може бути UDI). Ми повинні відповідним чином поставитися до цього.

– C5 – будь-який TP, який приймає UDI як вхідні дані, може виконувати лише дійсні транзакції для всіх можливих значень UDI. TP або прийме (перетворить на CDI), або відхилить UDI.

Нарешті, щоб запобігти людям отримати доступ через зміну кваліфікації TP:

– E4. Лише сертифікатор TP може змінити список об’єктів, пов’язаних із цим TP.

CW-lite

Варіантом Кларка-Вілсона є модель CW-lite, яка послаблює початкову вимогу формальної перевірки семантики TP. Семантичну перевірку відкладено до окремої моделі та загальних формальних інструментів доказу.

7.3. Резервування інформації та компонентів інформаційно-телекомунікаційних системах

Згідно закону України «Про захист інформації в інформаційно-комунікаційних системах» власники систем для забезпечення належного функціонування систем та захисту інформації, що обробляється в них:

– **створюють резервні копії** державних інформаційних ресурсів та систем із дотриманням встановлених для таких ресурсів та систем вимог щодо їх **захисту, цілісності та конфіденційності**;

– **забезпечують створення резервних копій** державних інформаційних ресурсів та систем на окремих фізичних носіях у зашифрованому вигляді та їх подальшу передачу (переміщення) для зберігання в установленому законодавством порядку, у тому числі за межами України (зокрема в закордонних дипломатичних установах України), **протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування**.

Також згідно цього закону вводяться наступні поняття:

– **Резервна копія державних інформаційних ресурсів** – копія інформації, яка міститься в державних інформаційних ресурсах, що перебувають у володінні або розпорядженні органів державної влади, органів місцевого самоврядування, військових формувань, утворених відповідно до законів України, державних підприємств, установ та організацій, та є критичною для їх сталого функціонування, створюється, записується, обробляється або зберігається у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів з метою подальшого відновлення цієї інформації;

– **Резервування державних інформаційних ресурсів та систем** – сукупність заходів, спрямованих на забезпечення створення резервної копії (резервних копій) та зберігання державних інформаційних ресурсів та систем з метою забезпечення безперервності їх роботи та подальшого відновлення інформації, що міститься в державних інформаційних ресурсах та системах, а також інсталяційних копій програмного забезпечення та операційних систем (та/або їх образів), в яких здійснюється їх обробка. Перелік видів державних інформаційних ресурсів та систем, щодо яких може здійснюватися резервне копіювання, визначається Кабінетом Міністрів України.

На цей час окрім організаційних заходів із планування відновлювальних робіт задля забезпечення неперервності функціонування своїх ІКС організації можуть застосовувати низку рішень із арсеналу аварійностійких (катастрофостійких) технологій. За своєю суттю ці технології передбачають *резервування ресурсів інформаційної системи* та *резервне зберігання даних*.

Можна виділити кілька рівнів резервування ресурсів інформаційної системи залежно від її значимості для діяльності організації, а також від чутливості діяльності до часу простою ІКС:

– Прикладом найнижчого рівня резервування для ІКС другорядного значення може бути просто серверна площадка, обладнана необхідними інженерними системами й підготовлена для установки серверного устаткування. Такий підхід дозволяє відновити роботу системи протягом декількох днів.

– Для більш важливих інформаційних систем відокремлений обчислювальний центр повинен містити все необхідне устаткування, щоб у випадку катастрофи можна було швидко запустити резервну систему (холодне резервування).

– А для найбільш критичних систем додатково необхідні системи реплікації даних і плани аварійного відновлення, що забезпечують збереження даних і безперервність функціонування ІКС (гаряче резервування).

Іншою складовою аварійностійких технологій, що стосується інформаційних ресурсів є резервування даних. У надзвичайних ситуаціях найбільший збиток організації наносять не тимчасова неможливість доступу до критичних даних, а цілковита їх втрата. Мінімізація цього ризику досягається за рахунок резервного копіювання й реплікації даних. На рис. 7.1 наведено класифікацію методів резервування даних.

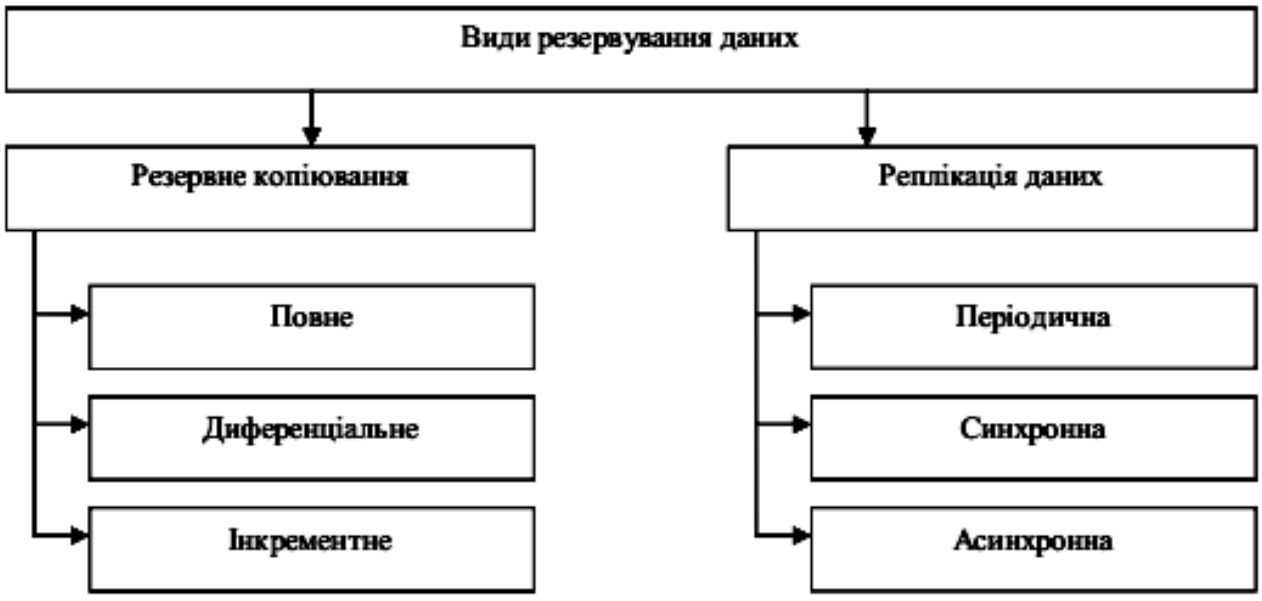


Рисунок 7.1 – Рівні резервування інформаційних систем

Резервне копіювання (*англ. backup*) – процес створення копії даних на спеціальних носіях (стримерах, матрицях дисків і т. д.), призначений для відновлення даних в основному місці їх розташування в разі їх пошкодження або руйнування. Резервне копіювання необхідне для швидкого і недорогого відновлення інформації (документів, програм) у випадку втрати робочої копії інформації з будь-якої причини. Важливо зберігати носії з резервними копіями окремо від оригінальних даних.

Повне резервування (*full backup*) зазвичай зачіпає всю операційну систему і всі дані. Створення щотижневих, щомісячних і щоквартальних архівів передбачає повне резервування. Перше щотижневе архівування повинно бути повним резервуванням, що зазвичай виконується по п'ятницях або упродовж вихідних, і передбачає копіювання всіх бажаних файлів. Подальші резервування, які проводять з понеділка по четвер аж до наступного повного резервування, можуть бути інкрементними або диференціальними, щоб заощадити час і місце на носії. Повне резервування слід проводити, принаймні, щотижня.

Диференціальне або *різницеве резервування* (*differential backup*) передбачає копіювання кожного файлу, зміненого з моменту останнього повного резервування. Диференціальне резервування прискорює процес відновлення і для відновлення вимагає лише останню повну і останню диференціальну резервні копії. Популярність диференціального резервування зростає, оскільки всі копії файлів виконуються в певні моменти часу, що, наприклад, дуже важливо при зараженні ІКС вірусами.

Інкрементне або *додаткове резервування* (*incremental backup*) передбачає копіювання тільки тих файлів, які були змінені з часу останнього повного або додаткового резервного копіювання. Подальше додаткове резервування додає тільки файли, які були змінені з моменту попереднього додаткового резервування. Таке резервування займає менше часу, оскільки копіюється менша кількість файлів. Однак, процес відновлення даних займає більше часу, тому що повинні бути відновлені дані останнього повного резервування, плюс дані всіх наступних додаткових резервувань. При цьому, на відміну від диференціального резервування нові або змінені файли не заміщають старі, а додаються на носій незалежно.

Реплікація даних – це віддалене резервне копіювання, що на відміну від звичайного резервного копіювання передбачає виділення таких додаткових ресурсів, як віддалені системи архівування, що з’єднані із ІКС організації каналами зв'язку. Розмаїтість схем і варіантів реплікації даних забезпечує можливість вибору найбільш ефективного й раціонального рішення для кожного конкретного завдання.

Періодична реплікація або *реплікація за розкладом* допомагає зберегти у відокремленому центрі копію даних на фіксований момент часу в минулому. Основний недолік цього методу – втрата актуальності даних за період часу, що дорівнює інтервалу між реплікаціями. Проте, реплікація за розкладом є доволі ощадливим рішенням для організацій, коли час відновлення не є критично важливим, а також допускається незначна втрата даних.

Синхронна реплікація гарантує найвищий рівень надійності, забезпечуючи ідентичність всіх копій даних. Висуваючи високі вимоги до каналів зв'язку, синхронна реплікація найчастіше застосовується для найбільш важливих застосувань, де необхідний максимальний захист даних.

Асинхронна реплікація забезпечує безперервність передачі даних, причому навіть в умовах нестабільності каналів зв’язку. Цей спосіб допомагає зберегти високу продуктивність інформаційних систем і контролювати завантаження каналів передачі даних, але не забезпечує настільки ж високий рівень актуальності даних, як синхронна реплікація.

Останнім часом часто застосовуються схеми множинної реплікації, коли дані передаються з основного обчислювального центра відразу до кількох резервних центрів. Нерідко в цих випадках навіть застосовуються різні способи реплікації для більш надійного й комплексного захисту даних.

Реплікація даних має деякі переваги порівняно з традиційними методами резервного копіювання:

– віддалене копіювання не вимагає участі користувачів та забезпечує необмежене в часі зберігання даних;

– деякі віддалені резервні служби можуть працювати безперервно, копіюючи зміни у файлах. Проте реплікація має й кілька істотних недоліків:

– відновлення даних може бути повільним, за обмеженої смуги пропускання каналів зв’язку;

– постачальники послуг віддаленого резервного копіювання можуть не надавати гарантій конфіденційності, тому організації-клієнти повинні самостійно шифрувати дані для віддаленого зберігання, при цьому, якщо ключ шифрування буде втрачено, то відновлення даних стане неможливим;

– деякі постачальники послуг реплікації часто мають щомісячні ліміти, які внаслідок чого обсяги резервного копіювання для організацій можуть обмежуватися.

Надійне збереження дуже важливих даних у випадку виникнення надзвичайної ситуації забезпечується за допомогою розподілених мереж зберігання даних (англ. Storage Area Network – SAN), для роботи яких необхідні надійні й високопродуктивні канали передачі даних. Технологія SAN забезпечує відмовостійкий доступ серверів до ресурсів зберігання і дозволяє знизити сукупну вартість утримання IT-інфраструктури за рахунок оптимального онлайнового управління доступу серверів до ресурсів зберігання. Розподілені мережі зберігання даних складаються з серверів резервного копіювання, системи управління та комунікаційної інфраструктури, що забезпечує фізичний зв'язок між елементами мережі зберігання даних. Подібна архітектура дозволяє забезпечити безперебійне і безпечне зберігання даних, а також обмін даними між елементами мережі зберігання даних. В основі концепції SAN лежить можливість з'єднання будь-якого з серверів з будь-яким пристроєм зберігання даних, що працює за протоколом Fibre Channel. Зручні засоби адміністрування SAN дають можливість скоротити чисельність обслуговуючого персоналу, що знижує вартість зберігання даних.

Об'єднання SAN за допомогою IP-мереж має меншу продуктивність, але за рахунок широкої поширеності й низької вартості IP-каналів цей варіант є більш доступним. Мережі зберігання даних із застосуванням технологій DWDM (системи з хвильовим ущільненням каналів) забезпечують передачу даних на великі відстані з високою швидкістю. У рішеннях цього класу використовуються волоконно-оптичні лінії зв’язку, в тому числі існуючі мережі глобальних операторів зв’язку. Висока швидкість передачі даних по SAN (200 Мбайт/с) дозволяє в реальному часі переміщати дані, що змінюються, у віддалене сховище.

Лекція 8. Програмні та програмно-апаратні комплекси засобів захисту інформації (ЗЗІ)

8.1. Антивіруси
8.2. Міжмережеві екрани.
8.3. IDS, IPS.
8.4. Системи контролю та управління доступом у мережі (Active Directory, ACL)
8.5. Системи контролю та управління фізичним доступом (СКУД)

8.1. Антивіруси

Антивірусна програма (антивірус) – спеціалізована програма для знаходження комп'ютерних вірусів, а також небажаних (шкідливих) програм загалом, та відновлення заражених (модифікованих) такими програмами файлів, а також для профілактики – запобігання зараженню (модифікації) файлів чи операційної системи шкідливим кодом.

Основні завдання

- Сканування файлів і програм в режимі реального часу.
- Сканування комп'ютера за потребою.
- Сканування інтернет-трафіку.
- Сканування електронної пошти.
- Захист від атак ворожих вебвузлів.
- Відновлення пошкоджених файлів.

Класифікація антивірусних продуктів

Класифікувати антивірусні продукти можна відразу за кількома ознаками, таким, як: використовувані технології антивірусного захисту, функціонал продуктів, цільові платформи.

По використовуваних технологіях антивірусного захисту:

- Класичні антивірусні продукти (продукти, які застосовують тільки сигнатурний метод детектування).
- Продукти проактивного антивірусного захисту (продукти, які застосовують тільки проактивні технології антивірусного захисту).
- Комбіновані продукти (продукти, які застосовують як класичні, сигнатурні методи захисту, так і проактивні).

За функціоналом продуктів:

- Антивірусні продукти (продукти, що забезпечують тільки антивірусний захист).
- Комбіновані продукти (продукти, що забезпечують не тільки захист від шкідливих програм, але і фільтрацію спаму, шифрування та резервне копіювання даних та інші функції).

За цільовими платформами: Windows, * NIX (до даного сімейства відносяться ОС BSD, Linux, etc), MacOS, для мобільних платформ (iOS, Android та ін.)

Антивірусні продукти для корпоративних користувачів можна також класифікувати по об'єктах захисту:

- для захисту робочих станцій;
- для захисту файлових і термінальних серверів;
- для захисту поштових та Інтернет-шлюзів;
- для захисту серверів віртуалізації.

Склад антивірусного програмного забезпечення

Антивірусне програмне забезпечення складається з комп'ютерних програм, які намагаються знайти, запобігти розмноженню і видалити комп'ютерні віруси та інші шкідливі програми.

Методи знаходження вірусів

Антивірусне програмне забезпечення зазвичай використовує два різних методи для виконання своїх задач:

- Перегляд (сканування) файлів для пошуку відомих вірусів, що відповідають визначенню в словнику вірусів.
- Знаходження підозрілої поведінки будь-якої з програм, що схожа на поведінку зараженої програми.

Відповідність визначенню вірусів в словнику

При цьому методі антивірусна програма під час перегляду файлу звертається до словника з відомими вірусами, що складений авторами програми-антивірусу. У разі відповідності якоїсь ділянки коду програми, що проглядається, відомому коду (сигнатурі) вірусу в словнику, програма-антивірус може виконувати одну з наступних дій:

- Видалити інфікований файл.
- Відправити файл у карантин (тобто зробити його недоступним для виконання, з метою недопущення подальшого розповсюдження вірусу).
- Намагатися відтворити файл, видаливши сам вірус з тіла файлу.

Хоча антивірусні програми створені на основі пошуку відповідності визначенню вірусу в словнику, за звичайних обставин, вони можуть досить ефективно перешкоджати збільшенню випадків зараження комп'ютерів, автори вірусів намагаються триматися на півкроку попереду таких програм-антивірусів, створюючи «олігоморфні», «поліморфні» і, найновіші, «метаморфічні» віруси, у яких деякі частини шифруються або спотворюються так, щоб неможливо було знайти спільне з визначенням в словнику вірусів.

Підозріла поведінка програмних забезпечень

Антивіруси, що використовують метод знаходження підозрілої поведінки програм, не намагаються ідентифікувати відомі віруси, замість цього вони стежать за поведінкою всіх програм. Якщо програма намагається записати якісь дані в файл, що виконується (exe-файл), програма-антивірус може зробити помітку цього файлу, попередити користувача і спитати, що треба зробити.

На відміну від методу відповідності визначенню вірусів в словнику, метод знаходження підозрілої поведінки дає захист від абсолютно нових вірусів, яких ще немає в жодному словнику вірусів. Однак треба враховувати, що програми, побудовані на цьому методі, видають також велику кількість помилкових попереджень. Програми класу Firewall давно мали в своєму складі модуль знаходження підозрілої поведінки програм.

Методи захисту від вірусів

Для захисту від вірусів використовують три групи методів:

1. Методи, засновані на *аналізі вмісту файлів* (як файлів даних, і файлів з кодами команд). До цієї групи належать сканування сигнатур вірусів, а також перевірка цілісності та сканування підозрілих команд.

2. Методи, що ґрунтуються на *відстеженні поведінки програм* при їх виконанні. Ці методи полягають у протоколюванні всіх подій, що загрожують безпеці системи та відбуваються або при реальному виконанні коду, що перевіряється, бо при його програмній емуляції.

3. Методи *регламентації порядку роботи* з файлами та програмами. Ці методи належать до адміністративних заходів забезпечення безпеки.

Метод сканування сигнатур (сигнатурний аналіз, сигнатурний метод) заснований на пошуку у файлах унікальної послідовності байтів – **сигнатури**, характерною для певного вірусу До кожного нововиявленого вірусу фахівцями антивірусної лабораторії виконується аналіз коду, виходячи з якого визначається його сигнатура. Отриманий кодовий фрагмент поміщають у спеціальну базу даних вірусних сигнатур, з якою працює антивірусна програма. Перевагою даного методу є відносно низька частка хибних спрацьовувань, а головним недоліком – принципова неможливість виявлення в системі нового вірусу, для якого відсутня сигнатура в базі даних антивірусної програми, тому потрібна своєчасна актуалізація бази сигнатур.

Метод контролю цілісності ґрунтується на тому, що будь-яка несподівана та безпричинна зміна даних на диску є підозрілою подією, яка потребує особливої уваги антивірусної системи. Вірус обов'язково залишає свідчення свого перебування (зміна даних існуючих (особливо системних або виконуваних) файлів, поява нових файлів, що виконуються і т. д.). Факт зміни даних – *порушення цілісності* – легко встановлюється шляхом порівняння контрольної суми(дайджесту), заздалегідь підрахованої для вихідного стану коду, що тестується, і контрольної суми (дайджесту) поточного стану тестованого коду. Якщо вони не збігаються, значить цілісність порушена і є всі підстави провести для цього коду додаткову перевірку, наприклад, шляхом сканування вірусних сигнатур. Зазначений метод працює швидше методу сканування сигнатур, оскільки підрахунок контрольних сум вимагає менше обчислень, ніж операції побайтового порівняння кодових фрагментів, крім того, він дозволяє виявляти сліди діяльності будь-яких, у тому числі невідомих, вірусів, для яких у базі даних ще немає сигнатур.

Метод сканування підозрілих команд (евристичне сканування, евристичний метод) заснований на виявленні в файлі, що сканується, деякого числа підозрілих команд і (або) ознак підозрілих кодових послідовностей (наприклад, команда форматування жорсткого диска або функція впровадження у виконуваний процес або виконуваний код). Після цього робиться припущення про шкідливу сутність файлу і робляться додаткові дії щодо його перевірки. Цей метод має гарну швидкодію, але досить часто він не здатний виявляти нові віруси.

Метод відстеження поведінки програм суттєво відрізняється від способів сканування вмісту файлів, згаданих раніше. Цей метод заснований на аналізі поведінки запущених програм, який можна порівняти з упійманням злочинця «за руку» на місці злочину. Антивірусні засоби даного типу часто вимагають активної участі користувача, покликаного приймати рішення у відповідь на численні попередження системи, значна частина яких може бути згодом помилковими тривогами. Частота помилкових спрацьовувань (підозра на вірус для нешкідливого файлу або пропуск шкідливого файлу) при перевищенні певного порога робить цей метод неефективним, а користувач може перестати реагувати на попередження або вибрати оптимістичну стратегію (дозволяти всі дії всім програмам, що запускаються) або відключити цю функцію. При використанні антивірусних систем, що аналізують поведінку програм, завжди існує ризик виконання команд вірусного коду, здатних завдати шкоди комп'ютеру або мережі, що захищається. Для усунення такого недоліку пізніше було розроблено метод емуляції (імітації), що дозволяє запускати тестовану програму в штучно створеному (віртуальному) середовищі, яку часто називають пісочницею (sandbox), без небезпеки пошкодження інформаційного оточення. Використання методів аналізу поведінки програм показало їхню високу ефективність при виявленні як відомих, так і невідомих шкідливих програм.

Емуляція

Деякі програми-антивіруси намагаються імітувати початок виконання коду кожної нової програми, що викликається для виконання, перед тим, як передати їй керування. Якщо програма використовує код, що змінюється самостійно, або проявляє себе як вірус (тобто починає шукати інші exe-файли, наприклад), – така програма буде вважатися шкідливою (здатною нашкодити іншим файлам). Однак цей метод також має велику кількість помилкових попереджень.

Основні види антивірусних програм

– **Програми-детектори** забезпечують пошук та виявлення вірусів в оперативній пам'яті та на зовнішніх носіях, і при виявленні видають відповідне повідомлення. Розрізняють детектори *універсальні* та *спеціалізовані*.

– **Програми-доктора (фаги)** як знаходять заражені вірусами файли, а й «лікують» їх, тобто видаляють з файлу тіло програми вірусу, повертаючи файли у вихідний стан. На початку своєї роботи фаги шукають віруси в оперативній пам'яті, знищуючи їх і лише потім переходять до «лікування» файлів. Серед фагів виділяють поліфаги, тобто програми-лікарі, призначені для пошуку та знищення великої кількості вірусів. Враховуючи, що постійно з'являються нові віруси, програми-детектори та програми-лікарі швидко застарівають, і потрібне регулярне оновлення їх версій.

– **Програми-ревізори** відносяться до найнадійніших засобів захисту від вірусів. Ревізори запам'ятовують вихідний стан програм, каталогів та системних областей диска тоді, коли комп'ютер не заражений вірусом, а потім періодично або за бажанням користувача порівнюють поточний стан з вихідним. Виявлені зміни відображаються на екрані монітора. Як правило, порівняння станів роблять

відразу після завантаження операційної системи. При порівнянні перевіряються довжина файлу, код циклічного контролю (контрольна сума файлу), дата та час модифікації та інші параметри.

– **Програми-фільтри (сторожі)** є невеликі резидентні програми, призначені виявлення підозрілих дій під час роботи комп'ютера, притаманних вірусів.

– **Програми-вакцини (імунізатори)** – це резидентні програми, що запобігають зараженню файлів. Вакцини застосовують, якщо відсутні програми-лікарі, які «лікують» цей вірус. Вакцинація можлива лише від відомих вірусів. Вакцина модифікує програму або диск таким чином, щоб це не відбивалося на їхній роботі, а вірус сприйматиме їх зараженими і тому не впровадиться. Істотним недоліком таких програм є їх обмежені можливості щодо запобігання зараженню від великої кількості різноманітних вірусів.

8.2. Міжмережеві екрани

Міжмережевий екран, **мережевий екран**, **брандмауер**, **фаєрво́л**, **файрво́л** (англ. *Firewall*, *вогняна стіна*) – узагальнювальна назва фізичних пристроїв чи програмних застосунків, зконфігурованих, щоб допускати, відмовляти, шифрувати, пропускати мережевий трафік між областями різної безпеки мережі згідно з бажаним набором безпеки.

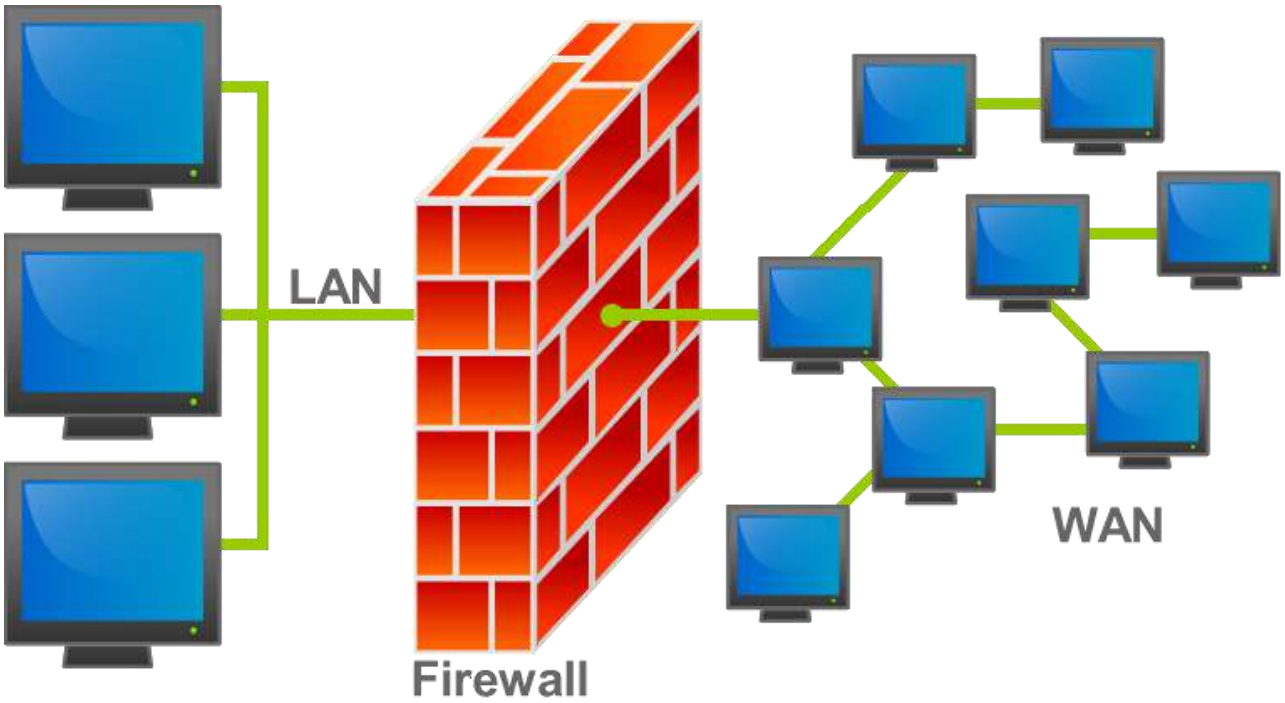


Рисунок 8.1 – Розташування фаєрвола у мережі

Функції

Фаєрвол може бути у вигляді окремого приладу (так званий *маршрутизатор* або *роутер*), або програмного забезпечення, що встановлюється на персональний комп'ютер чи проксі-сервер. Простий та дешевий фаєрвол може не мати такої гнучкої системи налаштувань правил фільтрації пакетів та *трансляції* адрес вхідного та вихідного трафіку (функція *переадресації*).

В залежності від активних з'єднань, що відслідковуються, фаєрволи розділяють на:

– *stateless* (проста фільтрація), які не відслідковують поточні з'єднання (наприклад TCP), а фільтрують потік даних виключно на основі статичних правил;

– *stateful* (фільтрація з урахуванням контексту), з відслідковуванням поточних з'єднань та пропуском тільки таких пакетів, що відповідають логіці й алгоритмам роботи відповідних протоколів та програм. Такі типи фаєрволів дозволяють ефективніше боротися з різноманітними DDoS-атаками та вразливістю деяких протоколів мереж.

Фільтрація трафіку

Фільтрація трафіку здійснюється на основі набору попередньо налаштованих правил, які називаються *ruleset*. Зручно представляти міжмережевий екран як послідовність фільтрів, які обробляють інформаційний потік. Кожен із фільтрів призначений для інтерпретації окремого правила. Послідовність правил набору істотно впливає на продуктивність міжмережевого екрану. Наприклад, багато міжмережевих екранів послідовно порівнюють трафік з правилами до тих пір, поки не буде знайдено відповідність. Для таких міжмережевих екранів правила, які відповідають найбільшій кількості трафіку, слід розташовувати якомога вище у списку, збільшуючи тим самим продуктивність.

Існує два принципи обробки трафіку, що надходить. Перший принцип говорить: "Що явно не заборонено, то дозволено". В даному випадку, якщо міжмережевий екран отримав пакет, що не потрапляє під жодне правило, то він передається далі. Протилежний принцип – "Що явно не дозволено, то заборонено" – гарантує набагато більшу захищеність, оскільки він забороняє весь трафік, який явно не дозволений правилами. Однак цей принцип обертається додатковим навантаженням на адміністратора.

У кінцевому рахунку міжмережні екрани виконують над трафіком, що надходить, одну з двох операцій: пропустити пакет далі (*allow*) або відкинути пакет (*deny*). Деякі міжмережові екрани мають ще одну операцію – *reject*, коли пакет відкидається, але відправнику повідомляється про недоступність сервісу, доступом до якого він намагався отримати. На противагу цьому, при операції *deny* відправник не інформується про недоступність сервісу, що є безпечнішим.

Типи фаєрволів

Для того щоб відповідати вимогам широкого кола користувачів, існує три типи фаєрволів: мережного рівня, прикладного рівня і рівня з'єднання. Кожен з цих трьох типів використовує свій, відмінний від інших підхід до захисту мережі:

– **Фаєрвол мережного рівня** представлений екрануючим маршрутизатором. Він контролює лише дані службової інформації пакетів мережевого і транспортного рівнів моделі OSI. Мінусом таких маршрутизаторів є те, що ще п'ять рівнів залишаються неконтрольованими. Нарешті, адміністратори, які працюють з екрануючими маршрутизаторами, повинні пам'ятати, що у більшості приладів, що здійснюють фільтрацію пакетів, відсутні механізми аудиту та подачі сигналу тривоги. Іншими словами, маршрутизатори можуть піддаватися атакам і відбивати велику їх кількість, а адміністратори навіть не будуть проінформовані.

– **Фаєрвол прикладного рівня** також відомий як проксі-сервер (сервер-посередник). Фаєрволи прикладного рівня встановлюють певний фізичний поділ між локальною мережею і Internet, тому вони відповідають найвищим вимогам безпеки. Проте, оскільки програма повинна аналізувати пакети і приймати рішення щодо контролю доступу до них, фаєрволи прикладного рівня неминуче зменшують продуктивність мережі, тому як сервер-посередник використовуються швидші комп'ютери.

– **Фаєрвол рівня з'єднання** схожий на фаєрвол прикладного рівня тим, що обидва вони є серверами-посередниками. Відмінність полягає в тому, що фаєрволи прикладного рівня вимагають спеціального програмного забезпечення для кожної мережевої служби на зразок FTP або HTTP. Натомість, фаєрволи рівня з'єднання обслуговують велику кількість протоколів.

Класифікація міжмережевих екранів

Досі немає єдиної і загальновизнаної класифікації міжмережевих екранів. Однак у більшості випадків рівень мережевої моделі OSI, що підтримується, є основною характеристикою при їх класифікації. Враховуючи цю модель, розрізняють такі типи міжмережевих екранів:

1. Керовані комутатори.
2. Пакетні фільтри.
3. Шлюзи сеансового рівня.
4. Посередники прикладного рівня.
5. Інспектори стану.

Керовані комутатори

Керовані комутатори іноді відносять до класу міжмережевих екранів, оскільки вони здійснюють фільтрацію трафіку між мережами або вузлами мережі. Однак вони працюють на канальному рівні і поділяють трафік у рамках локальної мережі, а отже не можуть бути використані для обробки трафіку із зовнішніх мереж (наприклад, з Інтернету).

Багато виробників мережного обладнання, такі як Cisco, Nortel, 3Com, ZyXEL, надають у своїх комутаторах можливість фільтрації трафіку на основі MAC-адрес, що містяться в заголовках кадрів. Наприклад, у комутаторах

сімейства Cisco Catalyst ця можливість реалізована за допомогою механізму Port Security. Однак даний метод фільтрації не є ефективним, оскільки апаратно встановлена в мережній карті MAC-адреса легко змінюється програмним шляхом, оскільки значення, вказане через драйвер, має більш високий пріоритет, ніж зашите в плату. Тому багато сучасних комутаторів дозволяють використовувати інші параметри як ознаку фільтрації – наприклад, VLAN ID. Технологія віртуальних локальних мереж (англ. *Virtual Local Area Network*) дозволяє створювати групи хостів, трафік яких повністю ізольований від інших вузлів мережі.

При реалізації політики безпеки в рамках корпоративної мережі, основу яких становлять керовані комутатори, вони можуть бути потужним та досить дешевим рішенням. Взаємодіючи лише з протоколами канального рівня, такі міжмережові екрани фільтрують трафік із дуже високою швидкістю. Основним недоліком такого рішення є неможливість аналізу протоколів вищих рівнів.

Пакетні фільтри

Пакетні фільтри функціонують на мережному рівні та контролюють проходження трафіку на основі інформації, що міститься в заголовку пакетів. Багато міжмережевих екранів цього типу можуть оперувати заголовками протоколів і вищого, транспортного, рівня (наприклад, TCP чи UDP). Пакетні фільтри одними з перших з'явилися на ринку міжмережевих екранів і досі залишаються найпоширенішим їх типом. Ця технологія реалізована в переважній більшості маршрутизаторів і навіть у деяких комутаторах.

При аналізі заголовка мережного пакета можна використовувати такі параметри:

– IP-адреси джерела та одержувача;

– тип транспортного протоколу;

– поля службових заголовків протоколів мережного та транспортного рівнів;

– порт джерела та одержувача.

Досить часто доводиться фільтрувати фрагментовані пакети, що ускладнює визначення деяких атак. Багато атак мережі використовують дану вразливість міжмережевих екранів, видаючи пакети, що містять заборонені дані, за фрагменти іншого, довіреного пакета. Одним із способів боротьби з даним типом атак є конфігурування міжмережевого екрану таким чином, щоб блокувати фрагментовані пакети. Деякі міжмережеві екрани можуть дефрагментувати пакети перед пересиланням у внутрішню мережу, але це вимагає додаткових ресурсів самого міжмережевого екрану, особливо пам'яті. Дефрагментація повинна використовуватися дуже обґрунтовано, інакше такий міжмережевий екран легко може стати жертвою DoS-атаки.

Пакетні фільтри можуть бути реалізовані в наступних компонентах мережної інфраструктури:

- прикордонні маршрутизатори;
- операційні системи;
- персональні міжмережеві екрани.

Так як пакетні фільтри зазвичай перевіряють дані тільки в заголовках мережного та транспортного рівнів, вони можуть виконувати це досить швидко. Тому пакетні фільтри, вбудовані в прикордонні маршрутизатори, є ідеальними для розміщення на кордоні з мережею з низьким ступенем довіри. Однак у пакетних фільтрах відсутня можливість аналізу протоколів вищих рівнів мережевої моделі OSI. Крім того, фільтри пакетів зазвичай уразливі до атак, які використовують підміну мережевих адрес. Такі атаки зазвичай виконуються для обходу управління доступом, що здійснюється міжмережевим екраном.

Шлюзи сеансового рівня

Міжмережевий екран сеансового рівня виключає пряму взаємодію зовнішніх хостів з вузлом, розташованим у локальній мережі, виступаючи як посередник (англ. *proxy*), який реагує на всі вхідні пакети та перевіряє їх допустимість на підставі поточної фази з'єднання. Шлюз сеансового рівня гарантує, що жоден мережний пакет не буде пропущений, якщо він не належить раніше встановленому з'єднанню. Як тільки надходить запит на встановлення з'єднання, в спеціальну таблицю міститься відповідна інформація (адреси відправника та одержувача, які використовуються протоколи мережного та транспортного рівня, стан з'єднання тощо). У випадку, якщо з'єднання встановлено, пакети, що передаються в рамках цієї сесії, просто копіюватимуться в локальну мережу без додаткової фільтрації. Коли сеанс зв'язку завершується, відомості про нього видаляються з таблиці. Тому всі наступні пакети, що «прикидаються» пакетами вже завершеного з'єднання, відкидаються.

Так як міжмережевий екран даного типу виключає пряму взаємодію між двома вузлами, шлюз сеансового рівня є єдиним елементом між зовнішньою мережею і внутрішніми ресурсами. Це створює видимість того, що на всі запити із зовнішньої мережі відповідає шлюз, і робить практично неможливим визначення топології мережі, що захищається. Крім того, оскільки контакт між вузлами встановлюється лише за умови його допустимості, шлюз сеансового рівня запобігає можливості реалізації DoS-атаки, властивої пакетним фільтрам.

Незважаючи на ефективність цієї технології, вона має серйозний недолік: як і у всіх вищезгаданих класів міжмережевих екранів, у шлюзів сеансового рівня відсутня можливість перевірки змісту поля даних, що дозволяє зловмиснику передавати «троянських коней» в мережу, що захищається.

Посередники прикладного рівня

Міжмережеві екрани прикладного рівня, до яких, зокрема, відноситься файл веб-додатків, як і шлюзи сеансового рівня, виключають пряму взаємодію двох вузлів. Однак, функціонуючи на прикладному рівні, вони здатні «розуміти» контекст трафіку, що передається. Міжмережні екрани, що реалізують цю технологію, містять кілька додатків-посередників (англ. *application proxy*), кожна з яких обслуговує свій прикладний протокол. Такий міжмережевий екран здатний виявляти в повідомленнях, що передаються, і блокувати неіснуючі або небажані послідовності команд, що часто означає DoS-атаку, або забороняти

використання деяких команд (наприклад, FTPPUT, яка дає можливість користувачеві записувати інформацію на сервер FTP).

Посередник прикладного рівня може визначати тип інформації, що передається. Наприклад, це дозволяє заблокувати поштове повідомлення, що містить файл, що виконується. Іншою можливістю міжмережевого екрану цього типу є перевірка аргументів вхідних даних. Наприклад, аргумент імені користувача довжиною 100 символів або містить бінарні дані є, принаймні, підозрілим.

Посередники прикладного рівня здатні виконувати автентифікацію користувача, а також перевіряти, що сертифікати SSL підписані конкретним центром. Міжмережні екрани прикладного рівня доступні для багатьох протоколів, включаючи HTTP, FTP, поштові (SMTP, POP, IMAP), Telnet та інші.

Недоліками даного типу міжмережевих екранів є великі витрати часу та ресурсів для аналізу кожного пакета. Тому вони зазвичай не підходять для додатків реального часу. Іншим недоліком є неможливість автоматичного підключення підтримки нових мережевих додатків та протоколів, так як для кожного з них потрібний свій агент.

Інспектори стану

Кожен із вищеперелічених типів міжмережевих екранів використовується для захисту корпоративних мереж і має ряд переваг. Однак, куди ефективніше було б зібрати всі ці переваги в одному пристрої і отримати міжмережевий екран, що здійснює фільтрацію трафіку з мережевого прикладного рівня. Ця ідея була реалізована в інспекторах станів, що поєднують у собі високу продуктивність та захищеність. Даний клас міжмережевих екранів дозволяє контролювати:

- кожен переданий пакет – на основі таблиці правил;
- кожну сесію – на основі таблиці станів;
- кожен додаток – на основі розроблених посередників.

Здійснюючи фільтрацію трафіку за принципом шлюзу сеансового рівня, цей клас міжмережевих екранів не втручається у процес встановлення з'єднання між вузлами. Тому продуктивність інспектора станів помітно вище, ніж у посередника прикладного рівня та шлюзу сеансового рівня, і можна порівняти з продуктивністю пакетних фільтрів. Ще одна перевага інспекторів стану – прозорість для користувача: для клієнтського програмного забезпечення не потрібно додаткове налаштування. Дані міжмережевих екранів мають великі можливості розширення. При появі нової служби або нового протоколу прикладного рівня для підтримки достатньо додати кілька шаблонів. Проте інспекторам станів порівняно з посередниками прикладного рівня властива нижча захищеність.

Термін інспектор стану (англ. *stateful inspection*), впроваджений компанією Check Point Software, полюбився виробникам мережного обладнання настільки, що зараз практично кожен міжмережевий екран зараховують до цієї технології, навіть якщо він і не реалізує її повністю.

Реалізація

Існує два варіанти виконання міжмережевих екранів – програмний та програмно-апаратний. У свою чергу програмно-апаратний варіант має два різновиди – у вигляді окремого модуля в комутаторі або маршрутизаторі і у вигляді спеціалізованого пристрою.

В даний час найчастіше використовується програмне рішення, яке на перший погляд виглядає більш привабливим. Це викликано тим, що для його застосування достатньо, здавалося б, лише придбати програмне забезпечення міжмережевого екрану і встановити на будь-який наявний в організації комп'ютер. Однак, як показує практика, в організації далеко не завжди знаходиться вільний комп'ютер та ще й задовольняє досить високим вимогам щодо системних ресурсів. Після того, як комп'ютер все-таки знайдений (найчастіше – куплений), слідує процес встановлення та налаштування операційної системи, а також, безпосередньо, програмного забезпечення міжмережевого екрану. Неважко помітити, що використання звичайного персонального комп'ютера далеко не так просто, як здається. *Security appliance*, на основі, як правило, FreeBSD або Linux, «урізані» для виконання лише необхідних функцій. Перевагами даних рішень є:

- Простота впровадження: дані пристрої мають встановлену та налаштовану операційну систему та вимагають мінімум налаштувань після впровадження в мережу.
- Простота управління: цими пристроями можна керувати звідки завгодно за стандартними протоколами, такими як SNMP або Telnet, або за допомогою захищених протоколів, таких як SSH або SSL.
- Продуктивність: дані пристрої працюють ефективніше, оскільки з їхньої операційної системи виключені всі сервіси, що не використовуються.
- Відмовостійкість та висока доступність: дані пристрою створені для виконання конкретних завдань з високою доступністю.

Обмеженість аналізу міжмережевого екрану

Міжмережевий екран дозволяє здійснювати фільтрацію тільки трафіку, який він здатний «розуміти». В іншому випадку, він втрачає свою ефективність, тому що не здатний свідомо прийняти рішення про те, що робити з нерозпізнаним трафіком. Існують протоколи, такі як TLS, SSH, IPsec і SRTP, що використовують криптографію для того, щоб приховати вміст, через що їх трафік не може бути проінтерпретований. Також деякі протоколи, такі як OpenPGP та S/MIME, шифрують дані прикладного рівня, через що фільтрувати трафік на підставі інформації, що міститься на даному мережному рівні, стає неможливо. Ще одним прикладом обмеженості аналізу міжмережевих екранів є тунельований трафік, так як його фільтрація є неможливою, якщо міжмережевий екран «не розуміє» механізм тунелювання. У всіх цих випадках правила, налаштовані на міжмережевому екрані, повинні визначати, що робити з трафіком, який вони не можуть інтерпретувати.

8.3. IDS, IPS

Система виявлення атак (вторгнень) (IDS)

Система виявлення атак (вторгнень) (англ. *Intrusion Detection System, IDS*) – програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу в комп'ютерну систему або мережу або несанкціонованого управління ними в основному через Інтернет. Про будь-яку активність шкідливого ПЗ або про порушення типової роботи централізовано збирається інформація SIEM-системою (англ. *Security information and event management*). SIEM-система обробляє дані отримані від багатьох джерел і використовує методи фільтрування тривог для розрізнення несанкціонованої активності від хибного спрацювання тривоги. Про що оповіщається або адміністратор або операційний центр безпеки.

Деякі системи виявлення вторгнень можуть виявити початок атаки на мережу, причому деякі з них здатні виявляти раніше не відомі атаки. Такі системи називають системами запобігання вторгненням (англ. *Intrusion Prevention System, IPS*). IPS не обмежуються лише оповіщенням, але й здійснюють різні заходи, спрямовані на блокування атаки (наприклад, розрив з'єднання або виконання скрипту, заданого адміністратором). На практиці досить часто програмно-апаратні рішення поєднують у собі функціональність двох типів систем. Їх об'єднання називають **IDPS** (**IDS і IPS**).

Хоч існує декілька типів IDS, які за розміром варіюються від окремих комп'ютерів до великих мереж, найпоширенішими класифікаціями є системи виявлення вторгнень у мережу (англ. *network intrusion detection systems, NIDS*) та системи виявлення вторгнень засновані на аналізі хостів (англ. *host-based intrusion detection systems, HIDS*). Прикладом HIDS буде система, яка відслідковує важливі файли операційної системи, прикладом NIDS буде система, яка аналізує вхідний мережевий трафік. Також можна класифікувати IDS відповідно до методів виявлення загроз: найбільш відомим є виявлення на основі сигнатур (розпізнавання поганих шаблонів, таких як шкідливе ПЗ) та виявлення аномалій (виявлення відхилень від «правильного» трафіку, часто за допомогою машинного навчання).

Порівняння IDS і файрвола

Хоча й IDS, і мережевий екран відносяться до засобів забезпечення інформаційної безпеки, мережевий екран відрізняється тим, що обмежує надходження на хост або підмережу певних видів трафіку для запобігання вторгнень і не відслідковує вторгнення, які відбуваються всередині мережі. IDS, навпаки, пропускає трафік, аналізуючи його і сигналізуючи при виявленні підозрілої активності. Виявлення порушення безпеки проводиться звичайно з використанням евристичних правил та аналізу сигнатур відомих комп'ютерних атак. Система яка розриває з'єднання називається системою запобігання вторгненням (англ. *Intrusion Prevention System, IPS*) і є однією з видів мережевого екрану на рівні застосунку.

Класифікація IDS

IDS можна класифікувати за місцем виявлення вторгнення (мережа або хост) та методу виявлення, який використовується.

Аналіз активності

Статичні і динамічні IDS

– Статичні засоби роблять «знімки» (snapshot) середовища та здійснюють їх аналіз, розшукуючи вразливе ПЗ, помилки в конфігураціях і т. д. Статичні IDS перевіряють версії прикладних програм на наявність відомих вразливостей і слабких паролів, перевіряють вміст спеціальних файлів в директоріях користувачів або перевіряють конфігурацію відкритих мережевих сервісів. Статичні IDS виявляють сліди вторгнення.

– Динамічні IDS здійснюють моніторинг у реальному часі всіх дій, що відбуваються в системі, переглядаючи файли аудиту або мережні пакети, що передаються за певний проміжок часу. Динамічні IDS реалізують аналіз в реальному часі і дозволяють постійно стежити за безпекою системи.

Мережеві IDS

– Мережеві IDS (англ. *Network-based IDS, NIDS*) розташовуються в стратегічному місці або у таких місцях мережі, де можливий контроль трафіку всіх пристроїв у мережі. Вони здійснюють контроль усього трафіку даних всієї підмережі та порівнюють трафік, який передається у підмережі з бібліотекою відомих атак. Як тільки розпізнана атака або визначено відхилення у поведінці, відразу відсилається попередження адміністратору. Наприклад, NIDS встановлюють у підмережі, де розташовані мережеві екрани, щоб побачити, чи намагається хтось втрутитися в брандмауер.

Ще один приклад, коли NIDS-система, контролює велике число TPC-запитів на з'єднання (SYN) з багатьма портами на обраному комп'ютері, виявляючи, таким чином, що хтось намагається здійснити сканування TCP – портів. Мережева IDS може запускатися або на окремому комп'ютері, який контролює свій власний трафік, або на виділеному комп'ютері, прозоро переглядають весь трафік у мережі (концентратор, маршрутизатор). Мережеві IDS контролюють багато комп'ютерів, тоді як інші IDS контролюють тільки один. Прикладом мережевої IDS є Snort.

Хостові IDS

– IDS, які встановлюються на хості і виявляють зловмисні дії на ньому називаються хостовими або системними IDS. Прикладами хостових IDS можуть бути системи контролю цілісності файлів, які перевіряють системні файли з метою визначення, коли в них були внесені зміни. Монітори реєстраційних файлів (Log – file monitors, LFM), контролюють реєстраційні файли, створювані мережевими сервісами і службами. Обманні системи, що працюють з псевдосервісами, мета яких полягає у відтворенні добре відомих вразливостей для обману зловмисників.

Методи виявлення

Аналіз сигнатур і протоколів

– Аналіз сигнатур був першим методом, застосованим для виявлення вторгнень. Він базується на простому понятті збігу послідовності зі зразком. У вхідному пакеті проглядається байт за байтом і порівнюється з сигнатурою (підписом) – характерним рядком програми, що вказує на характеристику шкідливого трафіку. Такий підпис може містити ключову фразу або команду, яка пов'язана з нападом. Якщо збіг знайдено, оголошується тривога.

– Другий метод аналізу полягає в розгляді строго форматованих даних трафіку мережі, відомих як протоколи. Кожен пакет супроводжується різними протоколами. Кожен протокол має кілька полів з очікуваними або нормальними значеннями. Якщо що-небудь порушує ці стандарти, то ймовірна зловмисність. IDS переглядає кожне поле всіх протоколів вхідних пакетів: IP, TCP, і UDP. Якщо є порушення протоколу, наприклад, якщо він містить несподівані значення в одному з полів, оголошується тривога.

PIDS (Protocol – based IDS) являє собою систему (або агента), яка відстежує і аналізує комунікаційні протоколи з пов'язаними системами або користувачами. Для вебсервера подібна IDS зазвичай веде спостереження за HTTP і HTTPS протоколами. При використанні HTTPS IDS повинна розташовуватися на такому інтерфейсі, щоб переглядати HTTPS пакети ще до їх шифрування і відправки в мережу.

APIDS (Application Protocol – based IDS) – це система (або агент), яка веде спостереження та аналіз даних, переданих з використанням специфічних для певних програм протоколів. Наприклад, на вебсервері з SQL базою даних IDS буде відслідковувати вміст SQL команд, що передаються на сервер.

Виявлення аномалій

Системи виявлення вторгнень на основі аномалій були здебільшого введені для виявлення невідомих атак, почасти через стрімкий розвиток шкідливих програм. Основний підхід полягає у використанні машинного навчання, щоб створити модель правдоподібної діяльності, з якою потім порівняється нова поведінку. Хоча такий підхід і дозволяє виявити невідомі види атак, але з недоліків є наявність хибно позитивних спрацювань: невідома раніше законна діяльність може бути також класифікована як шкідлива.

Система запобігання вторгненням (IPS)

Система запобігання вторгненням (англ. *Intrusion Prevention System*, IPS) – програмна або апаратна система мережевої та комп'ютерної безпеки, яка виявляє вторгнення або порушення безпеки і автоматично захищає від них.

Системи IPS можна розглядати як розширення систем виявлення вторгнень (IDS), так як завдання відстеження атак залишається однаковою. Однак, вони відрізняються в тому, що IPS повинна відслідковувати активність в реальному часі і швидко реалізовувати дії щодо запобігання атак.

Класифікація IPS

– **Мережеві IPS (Network – based Intrusion Prevention, NIPS):** відстежують трафік в комп'ютерній мережі і блокують підозрілі потоки даних.

– **IPS для бездротових мереж (Wireless Intrusion Prevention Systems, WIPS):** перевіряє активність в бездротових мережах. Зокрема, виявляє невірно сконфігуровані точки бездротового доступу до мережі, атаки людина посередині, спуфинг MAC-адрес.

– **Поведінковий аналіз мережі (Network Behavior Analysis, NBA):** аналізує мережевий трафік, ідентифікує нетипові потоки (виявляє аномалії), наприклад DoS і DDoS атаки.

– **Система попередження вторгнень для окремих комп'ютерів (Host – based Intrusion Prevention, HIPS):** резидентні програми, які виявляють підозрілу активність на комп'ютері.

Історія розробок

Історія розвитку сучасних IPS включає в себе історії розвитку декількох незалежних рішень, проактивних методів захисту, які розроблялися в різний час для різного роду загроз. Під проактивними методами захисту, пропонованими сьогодні ринком, розуміється наступне:

1. Поведінковий аналізатор процесів для аналізу поведінки запущених в системі процесів і виявлення підозрілих дій, тобто невідомих шкідливих програм.

2. Усунення можливостей попадання інфекції на комп'ютер, блокування портів, які використовуються вже відомими вірусами, і тих, які можуть використовуватися їх новими модифікаціями.

3. Недопущення переповнення буфера у найбільш поширених програм і сервісів, що найбільш часто використовується зловмисниками для здійснення атаки.

4. Мінімізація шкоди, завданої інфекцією, запобігання подальшого її розмноження, обмеження доступу до файлів та директорій; виявлення і блокування джерела інфекції в мережі.

Аналіз мережевих пакетів

Зазвичай в якості першої загрози, яка спонукала до протидії вторгненням, називають хробака Морріса, що вразив підключені до мережі Unix-комп'ютери в листопаді 1988 року.

Згідно іншої теорії, стимулом для створення нової фортифікаційної споруди стали дії групи хакерів спільно зі спецслужбами СРСР і НДР. У період з 1986-го по 1989 рік група, ідейним керівником якої був Маркус Гесс, передавала своїм національним спецслужбам інформацію, здобуту ними шляхом вторгнення в комп'ютери. Все почалося з невідомого рахунку всього на 75 центів в Національній лабораторії ім. Е. Лоуренса в Берклі. Аналіз його походження в кінцевому підсумку вивів на Гесса, який працював програмістом в невеликій західнонімецькій компанії і одночасно належав до екстремістської групи Chaos Computer Club, яка базувалася в Гамбурзі.

Організоване ним вторгнення починалося з дзвінка з дому через найпростіший модем, що забезпечував йому зв'язок з європейською мережею Datex-P і далі проникнення в комп'ютер бібліотеки Бременського університету, де хакер отримував необхідні привілеї і вже з ними пробивався в Національну лабораторію ім. Е. Лоуренса в Берклі.

Перший лог був зареєстрований 27 липня 1987 року, і з 400 доступних комп'ютерів він зміг влізти приблизно в 30 і після цього спокійно пересуватись в закритій мережі Milnet, використовуючи, зокрема, пастку у вигляді файлу під назвою Strategic Defense Initiative Network Project (його цікавило все, що було пов'язано зі Стратегічною оборонною ініціативою президента Рейгана). Негайною реакцією на появу зовнішніх мережевих загроз виявилося створення міжмережевих екранів, як перших систем виявлення та фільтрації загроз.

Аналіз програм і файлів

Поведінковий блокувальник

З появою нових видів загроз згадали про поведінкові блокувальники.

Перше покоління поведінкових блокаторів з'явилося ще в середині 90-х років. Принцип їх роботи – при виявленні потенційно небезпечних дій користувачеві ставилося питання, дозволити або заборонити дію. Теоретично блокіратор здатний запобігти розповсюдженню будь-яких відомих, так і невідомих вірусів. Основним недоліком перших поведінкових блокувальників було надмірна кількість запитів до користувача. Причина цього – нездатність поведінкового блокувальника судити про шкідливості тої чи іншої дії. Однак, в програмах, написаних на VBA, можна з дуже великою ймовірністю відрізнити шкідливі дії від корисних.

Друге покоління поведінкових блокувальників відрізняється тим, що вони не аналізують окремі дії, а послідовність дій і вже на підставі цього роблять висновок про шкідливості того чи іншого ПЗ.

Методи реагування на атаки

Після початку атаки

Методи реалізуються вже після того, як була виявлена інформаційна атака. Це означає, що навіть у разі успішного виконання системі, що захищається може бути завдано шкоди.

Блокування з'єднання

Якщо для атаки використовується TCP-з'єднання, то реалізується його закриття за допомогою посилки кожному або одному з учасників TCP-пакета з встановленим прапором RST. У результаті зловмисник позбавляється можливості продовжувати атаку, використовуючи мережеве з'єднання. Даний метод найчастіше реалізується з допомогою наявних мережевих датчиків.

Метод характеризується двома основними недоліками:

1. Не підтримує протоколи, відмінні від TCP, для яких не вимагається попереднього встановлення з'єднання (наприклад, UDP і ICMP).

2. Метод може бути використаний тільки після того, як зловмисник вже отримав несанкціоноване з'єднання.

Блокування записів користувачів

Якщо кілька облікових записів користувачів були скомпрометовані в результаті атаки або виявилися їх джерелами, то здійснюється їх блокування хостовими датчиками системи. Для блокування датчики повинні бути запущені від імені облікового запису, який має права адміністратора.

Також блокування може відбуватися на заданий строк, який визначається налаштуваннями Системи запобігання вторгнень.

Блокування хоста комп'ютерної мережі

Якщо з одного з хостів була зафіксована атака, то може бути проведене його блокування хостовими датчиками або блокування мережевих інтерфейсів або на нього, або на маршрутизаторі або комутаторі, за допомогою яких хост підключений до мережі. Розблокування може відбуватися через заданий проміжок часу або за допомогою активації адміністратора безпеки. Блокування не скасовується після перезапуску або відключення від мережі хоста. Так само для нейтралізації атаки можна блокувати ціль атаки, хост комп'ютерної мережі.

Блокування атаки за допомогою мережевого екрану

IPS формує і надсилає нові конфігурації в мережевому екрані (ME), за якими екран буде фільтрувати трафік від порушника. Така реконфігурація може відбуватися в автоматичному режимі з допомогою стандартів OPSEC (наприклад SAMP, CPMI).

Для ME, які не підтримують протоколи OPSEC, для взаємодії із Системою запобігання вторгнення може бути використаний модуль-адаптер:

- на який будуть надходити команди про зміну конфігурації ME;
- який буде редагувати конфігурації ME для модифікації його параметрів.

Зміна конфігурації комунікаційного обладнання

Для протоколу SNMP, IPS аналізує і змінює параметри з бази даних MIB (такі як таблиць маршрутизації, налаштування портів) з допомогою агента пристрою, щоб блокувати атаку. Також можуть бути використані протоколи TFTP, Telnet та ін.

Активне придушення джерела атаки

Метод теоретично може бути використаний, якщо інші методи виявляться марними. IPS виявляє і блокує пакети порушника, та здійснює атаку на його сайт, за умови, що його адресу однозначно визначено і в результаті таких дій не буде завдано шкоди іншим легальним вузлам.

Такий метод реалізовано в декількох некомерційних ПЗ:

– NetBuster запобігає проникненню в комп'ютер «Троянського коня». Він може також використовуватися як засіб «fool-the-one-trying to NetBus-you» ("обдури того, хто намагається проникнути до тебе на «Троянському коні»). У цьому випадку він розшукує шкідливу програму і визначає комп'ютер який запустив її, а потім повертає цю програму адресанту.

– Tambu UDP Scrambler працює з портами UDP. Продукт діє не тільки як фіктивний UDP-порт, він може використовуватися для «паралізації» апаратури хакерів за допомогою невеликої програмки UDP flooder.

Так як гарантувати виконання всіх умов неможливо, широке застосування методу на практиці поки що неможливо.

На початку атаки

Методи реалізують заходи, які запобігають виявлені атаки до того, як вони досягають мети.

З допомогою мережевих датчиків

Мережеві датчики встановлюються в розрив каналу зв'язку так, щоб аналізувати всі пакети які проходять. Для цього вони оснащуються двома мережевими адаптерами, які функціонують у «змішаному режимі», на прийом і на передачу, записуючи всі пакети в буферну пам'ять, звідки вони зчитуються модулем виявлення атак IPS. У разі виявлення атаки ці пакети можуть бути видалені.

Аналіз пакетів проводиться на основі сигнатурного або поведінкового методів.

За допомогою хостових датчиків

- **Віддалені атаки**, які реалізуються відправкою від зловмисника серією пакетів. Захист реалізується з допомогою компоненти IPS за аналогією з мережевими датчиками, але на відміну від останніх мережева компонента перехоплює і аналізує пакети на різних рівнях взаємодії, що дає запобігати атакам по криптозахищеним IPsec і SSL/TLS з'єднанням.
- **Локальні атаки** при несанкціонованому запуску зловмисником програм або інших діях, що порушують інформаційну безпеку. Перехоплюючи системні виклики всіх додатків і аналізуючи їх, датчики блокують ті виклики, які становлять небезпеку.

8.4. Системи контролю та управління доступом (Active Directory, ACL)

Список контролю доступу (ACL)

Access Control List або ACL (*список контролю доступу*) – список прав доступу до об’єкта, який визначає, хто або що може отримувати доступ до нього, і які саме операції дозволено або заборонено цьому суб'єкту проводити над об'єктом.

Списки контролю доступу є основою систем з вибірковим управлінням доступом. У типових ACL кожен запис визначає суб'єкт впливу і операцію: наприклад, запис (Taras, delete) в ACL для файлу XYZ дає можливість користувачеві Taras видалити файл XYZ.

В системі з моделлю безпеки, заснованої на ACL, коли суб'єкт запитує виконання операції над об'єктом, система спочатку перевіряє список дозволених для цього суб'єкта операцій, і тільки після цього дає (або не дає) доступ до запитуваної дії.

При централізованому зберіганні списків контролю доступу можна говорити про матрицю доступу, в якій по осях розміщені об'єкти і суб'єкти, а в клітинках – відповідні права. Однак у великій кількості систем списки контролю

доступу до об'єктів зберігаються окремо для кожного об'єкта, найчастіше безпосередньо з самим об'єктом.

Традиційні ACL системи призначають права індивідуальним користувачам, і з часом і зростанням числа користувачів в системі списки доступу можуть стати громіздкими. Варіантом вирішення цієї проблеми є призначення прав групам користувачів, а не персонально. Іншим варіантом вирішення цієї проблеми є керування доступом на основі ролей, де функціональні підмножини прав до ряду об'єктів об'єднуються в «ролі», і ці ролі призначаються користувачам. Однак, у першому варіанті групи користувачів також часто називаються ролями.

Список контролю доступу (ACL) містить правила, які надають або забороняють доступ до певних цифрових середовищ. Є два типи ACL:

– **ACL файлової системи** – фільтрує доступ до файлів і/або каталогів. ACL файлової системи повідомляє операційним системам, які користувачі можуть отримати доступ до системи та які привілеї надані користувачам.

– **Мережні ACL** – фільтрує доступ до мережі. Мережні ACL повідомляють маршрутизаторам і комутаторам, який тип трафіку може отримати доступ до мережі та яка діяльність дозволена.

Файлові системи з ACL

У файлових системах для реалізації ACL використовується ідентифікатор користувача процесу (UID в термінах POSIX).

Список доступу являє собою структуру даних (зазвичай таблицю), що містить записи, які визначають права індивідуального користувача або групи на спеціальні системні об'єкти, такі як програми, процеси або файли. Ці записи також відомі як ACE (англ. *Access Control Entries*) в операційних системах Microsoft Windows і OpenVMS.

В операційній системі Linux і Mac OS X більшість файлових систем мають розширені атрибути, що виконують роль ACL. Кожен об'єкт в системі містить покажчик на свій ACL. Привілеї (або повноваження) визначають спеціальні права доступу, що дозволяють користувачеві читати з (англ. *read*), писати в (англ. *write*), або виконувати (англ. *execute*) об'єкт. У деяких реалізаціях ACE можуть визначати право користувача або групи на зміну ACL об'єкта.

Концепції ACL в різних операційних системах різняться, незважаючи на існуючий «стандарт» POSIX. (Проекти безпеки POSIX,.1e і.2c, були відкликані, коли стало ясно що вони зачіпають занадто велику область і робота не може бути завершена, але добре опрацьовані частини, що визначають ACL, були широко реалізовані і відомі як «POSIX ACLs».)

Мережеві ACL

У мережах ACL представляють список правил, що визначають порти служб або імена доменів, доступних на вузлі або іншому пристрої третього рівня OSI, кожен зі списком вузлів та/або мереж, яким дозволений доступ до сервісу. Мережеві ACL можуть бути налаштовані як на звичайному сервері, так і на маршрутизаторі і можуть керувати як вхідним, так і вихідним трафіком, як брандмауер.

Спочатку ACL були єдиним способом захисту брандмауерів (фаєрволів, міжмережевих екранів). Сьогодні існує багато типів брандмауерів і альтернатив ACL. Однак організації продовжують використовувати списки керування доступом у поєднанні з такими технологіями, як віртуальні приватні мережі (VPN), які визначають, який трафік слід шифрувати та передавати через тунель VPN.

Причини використання ACL:

– Контроль транспортного потоку.

– Обмежений мережевий трафік для кращої продуктивності мережі.

– Рівень безпеки доступу до мережі, який визначає, до яких областей сервера/мережі/служби може отримати доступ користувач, а до яких ні.

– Детальний моніторинг трафіку, що виходить і входить в систему.

Як працює ACL

ACL файлової системи – це таблиця, яка інформує операційну систему комп'ютера про привілеї доступу, які має користувач до системного об'єкта, включаючи один файл або файловий каталог. Кожен об'єкт має властивість безпеки, яка пов'язує його зі списком керування доступом. У списку є запис для кожного користувача з правами доступу до системи.

Типові привілеї включають право читати один файл (або всі файли) у каталозі, виконувати файл або записувати файл або файли. Операційні системи, які використовують ACL, включають, наприклад, Microsoft Windows, Digital OpenVMS і системи на базі UNIX.

Коли користувач запитує об'єкт у моделі безпеки на основі ACL, операційна система вивчає ACL на предмет відповідного запису та перевіряє, чи допустима запитана операція.

Мережеві ACL встановлюються в маршрутизаторах або комутаторах, де вони діють як фільтри трафіку. Кожен мережевий ACL містить попередньо визначені правила, які контролюють, яким пакетам або оновленням маршрутизації дозволено чи заборонено доступ до мережі.

Маршрутизатори та комутатори з ACL працюють як фільтри пакетів, які передають або відхиляють пакети на основі критеріїв фільтрації. Будучи пристроєм рівня 3, маршрутизатор із фільтрацією пакетів використовує правила, щоб визначити, чи слід дозволити або заборонити доступ до трафіку. Він вирішує це на основі IP-адрес джерела та призначення, порту призначення та вихідного порту та офіційної процедури пакета.

Типи списків контролю доступу

Списки контролю доступу можна розділити на дві основні категорії:

Стандартний ACL

Список доступу, розроблений виключно з використанням вихідної IP-адреси. Ці списки контролю доступу дозволяють або блокують увесь набір протоколів. Вони не розрізняють IP-трафік, наприклад UDP, TCP і HTTPS. Вони використовують номери 1-99 або 1300-1999, щоб маршрутизатор міг розпізнати адресу як вихідну IP-адресу.

Розширений ACL

Список доступу, який широко використовується, оскільки він може диференціювати IP-трафік. Він використовує IP-адреси джерела та призначення та номери портів, щоб зрозуміти IP-трафік. Ви також можете вказати, який IP-трафік має бути дозволений або заборонений. Вони використовують числа 100-199 і 2000-2699.

Порівняння Linux ACL та Windows ACL

Linux забезпечує гнучкість для внесення змін до ядра, що неможливо зробити з Windows. Однак, оскільки ви можете вносити зміни до ядра Linux, вам можуть знадобитися спеціальні знання для підтримки робочого середовища.

Windows пропонує перевагу стабільної платформи, але вона не така гнучка, як Linux. Що стосується інтеграції додатків, Windows легше, ніж Linux.

Користувач може налаштувати механізми контролю доступу в системі Windows без додавання програмного забезпечення.

З точки зору виправлень, Microsoft є єдиним джерелом для випуску виправлень Windows. З Linux ви можете зачекати, доки комерційний постачальник Linux випустить виправлення, або ви можете скористатися організацією з відкритим кодом для виправлень.

У Windows кожен дескриптор безпеки містить два види ACL – системні (system, SACL) та вибіркові (Discretionary, DACL)

Яка різниця між ACL, ACE, DACL і SACL?

Дескриптор безпеки містить два **списки керування доступом (ACL)**, які використовуються для призначення та відстеження інформації про безпеку для кожного об’єкта: **дискреційний список контролю доступу (DACL)** і **список контролю доступу до системи (SACL)**.

Дискреційні списки контролю доступу (DACL). DACL ідентифікують користувачів і групи, яким призначено або заборонено доступ до об’єкта. Якщо DACL явно не ідентифікує користувача або будь-які групи, членом яких є користувач, користувачеві буде відмовлено в доступі до цього об’єкта. За замовчуванням DACL контролюється власником об’єкта або особою, яка створила об’єкт, і містить **записи керування доступом (ACE)**, які визначають доступ користувача до об’єкта.

Списки контролю доступу до системи (SACL). SACL ідентифікують користувачів і групи, які потрібно перевірити, коли вони успішно отримують або не можуть отримати доступ до об’єкта. Аудит використовується для моніторингу подій, пов’язаних із системною або мережевою безпекою, для виявлення порушень безпеки, а також для визначення ступеня та місця будь-яких пошкоджень. За замовчуванням SACL контролюється власником об’єкта або особою, яка створила об’єкт. SACL містить **записи керування доступом (ACE)**, які визначають, чи реєструвати успішну чи невдалу спробу користувача отримати доступ до об’єкта за допомогою наданого дозволу, наприклад, Повний доступ і Читання.

Найкращі практики ACL

Налаштовуючи списки керування доступом, слід дотримуватися кількох найкращих практик, щоб переконатися, що безпека є жорсткою, а підозрілий трафік блокується:

1. Наскрізний ACL

ACL застосовуються на кожному інтерфейсі, майже в усіх засобах безпеки та маршрутизації. Це доречно, оскільки ви не можете мати однакові правила для зовнішніх інтерфейсів та інтерфейсів, які формують мережу вашого кампусу. Однак інтерфейси схожі, і ви не хочете, щоб деякі були захищені списками керування доступом, а інші – відкритими.

Практика ACL на всіх інтерфейсах є важливою для вхідних ACL, зокрема правил, які визначають, яка адреса може передавати дані у вашу мережу. Це правила, які роблять значну різницю.

2. ACL за порядком

Майже у всіх випадках механізм, що забезпечує дотримання ACL, починається зверху та рухається вниз у списку. Це має наслідки для розробки того, що ACL робитиме з певним потоком даних.

Одна з причин, чому організації використовують ACL, полягає в тому, що вони мають менші обчислювальні витрати, ніж брандмауери з підтримкою стану, і вони працюють на високій швидкості. Це важливо, коли ви намагаєтесь реалізувати безпеку для швидких мережевих інтерфейсів. Однак, чим довше пакет залишається в системі, поки він перевіряється на відповідність правилам у ACL, тим нижча продуктивність.

Фокус полягає в тому, щоб розмістити правила, які, як ви очікуєте, будуть активовані у верхній частині ACL. Працюйте від загального до конкретного, забезпечуючи логічне згрупування правил. Ви повинні знати, що на кожен пакет діятиме початкове правило, яке він запускає, ви можете в кінцевому підсумку передати пакет через одне правило, коли ви збираєтеся заблокувати його через інше. Подумайте, як ви хочете, щоб відбувався ланцюг подій, зокрема, додаючи нові правила.

3. Задокументуйте свою роботу

Коли ви додаєте правила ACL, задокументуйте, чому ви їх додаєте, для чого вони призначені та коли ви їх додали.

Вам не потрібно мати один коментар до правила. Ви можете зробити один коментар для блоку правил, складне пояснення для окремого правила або поєднати обидва підходи.

Розробники повинні переконатися, що поточні правила задокументовані, щоб нікому не доводилося здогадуватися, чому існує правило.

Порівняння RBAC й ACL

Розробники можуть використовувати системи **списків доступу на основі ролей (RBAC)** для контролю безпеки на детальному рівні. Замість того, щоб підкреслювати особу користувача та визначати, чи має він мати дозвіл переглядати щось у програмі, RBAC керує безпекою на основі ролі користувача в організації.

Наприклад, замість того, щоб надати дозвіл Джону Сміту, архітектору з Нью-Йорка, RBAC надасть дозвіл на роль для архітекторів США. Джон Сміт може бути одним із багатьох користувачів із цією роллю. Таким чином, RBAC гарантує контролюючим особам, що лише певні користувачі мають доступ до конфіденційної інформації, оскільки дає всі дозволи на основі ролей.

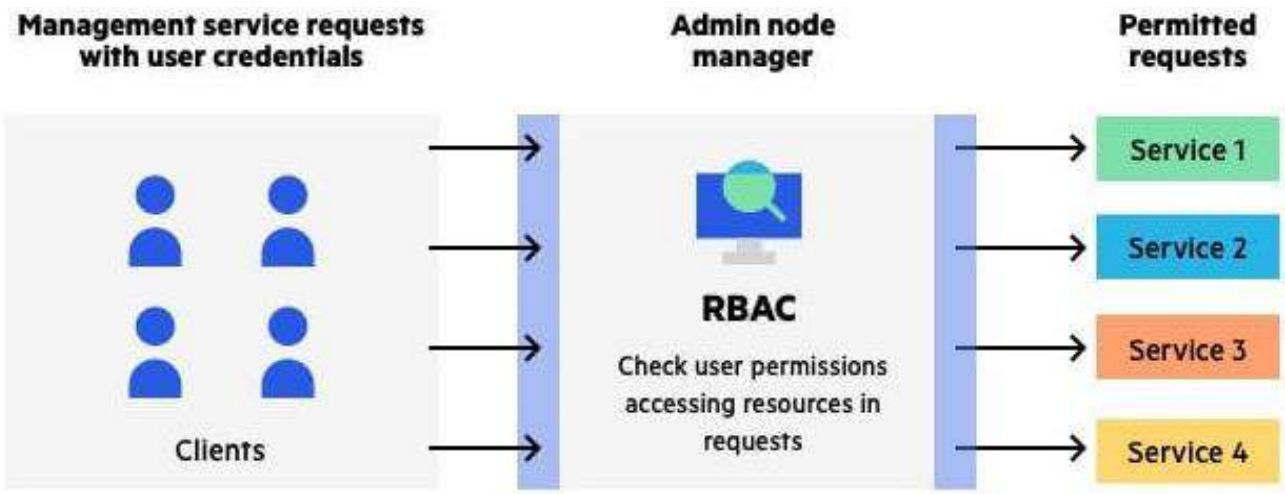


Рисунок 8.2 – Приклад системи керування доступом на основі ролей (RBAC)

RBAC зазвичай вважається кращим методом для бізнес-додатків. RBAC є більш ефективним, ніж ACL, щодо адміністративних витрат і безпеки. ACL найкраще використовувати для застосування безпеки на рівні окремого користувача. Ви можете використовувати RBAC для обслуговування системи безпеки всієї компанії, яку контролює адміністратор. Наприклад, ACL може надати доступ для запису до певного файлу, але він не може визначити, як користувач може змінювати файл.

8.5. Система контролю та управління доступом (СКУД)

Система контролю та управління доступом, **СКУД** (англ. *Physical Access Control System, PACS*) – сукупність програмно-апаратних технічних засобів контролю та засобів управління, що мають на меті обмеження та реєстрацію входу-виходу об'єктів (людей, транспорту) на заданій території через «точки проходу»: двері, ворота, КПП.

Основне завдання – управління доступом на задану територію (кого пускати, в який час і яку територію), включаючи:

– обмеження доступу на задану територію;
– ідентифікацію особи, яка має доступ на задану територію.

Додаткові завдання:

– облік робочого часу;

– розрахунок заробітної плати (при інтеграції із системами бухгалтерського обліку);

– ведення бази персоналу/відвідувачів;

– інтеграція із системою безпеки, наприклад:

- із системою відеоспостереження для поєднання архівів подій систем, передачі системі відеоспостереження сповіщень про необхідність стартувати запис, повернути камеру для запису наслідків зафіксованої підозрілої події;
- з системою охоронної сигналізації (СОС), наприклад, для обмеження доступу до приміщень, що стоять на охороні, або для автоматичного зняття та постановки приміщень на охорону.
- з системою пожежної сигналізації (СПС) для отримання інформації про стан пожежних сповіщувачів, автоматичне розблокування евакуаційних виходів та закриття протипожежних дверей у разі пожежної тривоги.

На особливо відповідальних об'єктах мережа пристроїв СКУД виконується фізично не пов'язаною з іншими інформаційними мережами.

Запобіжні пристрої

Встановлюються на двері:

– Електрозасувки – їх зазвичай встановлюють на внутрішні двері (внутрішньоофісні і т. п.) Електрозащілки, як і інші типи замків, бувають напругою, що відкриваються (тобто двері відкриваються при подачі напруги живлення на замок), і напругою, що закриваються (відчиняються, як тільки з них знімається напруга живлення, тому рекомендовано для використання пожежною інспекцією).

– Електромагнітні замки – практично всі замикаються напругою, тобто придатні для встановлення на шляхах евакуації під час пожежі.

– Електромеханічні замки – досить стійкі до злому (якщо міцний замок механічно), багато хто має механічний перевзвод (це означає, що якщо на замок подали відкриваючий імпульс, він буде розблокований до тих пір, поки двері не відчинять).

Встановлюються на проходах/проїздах:

Турнікет-трипод поясний із зчитувачем системи контролю доступу

– Турнікети використовуються на прохідних підприємствах, суспільно значущих об'єктах (стадіони, вокзали, метро, деякі держустанови) скрізь, де потрібно організувати контрольований прохід великої кількості людей. Турнікети поділяються на два основні типи: поясні та повноростові. Якщо поряд з турнікетом немає вільного проходу, що швидко відкривається (на випадок пожежі), поясний турнікет повинен бути обладнаний т.з. планками «антипаніка» – планками, що зламуються зусиллям нормальної людини (вимога пожежної інспекції).

– Шлюзові кабіни – використовуються в банках, на режимних об'єктах (на підприємствах із підвищеними вимогами до безпеки).

– Ворота та шлагбауми – переважно встановлюються на в'їздах на територію підприємства, на автомобільних парковках та автостоянках, на в'їздах на прибудинкову територію, у двори житлових будівель. Основна вимога – стійкість до кліматичних умов та можливість автоматизованого керування (за допомогою системи контролю доступу). Коли йдеться про організацію контролю доступу до проїзду, до системи пред'являються додаткові вимоги – підвищена дальність зчитування міток, розпізнавання автомобільних номерів (у разі інтеграції із системою відеоспостереження).

– Автоматичні дорожні бар'єри – використовуються для гарантованого запобігання несанкціонованому проїзду автотранспорту на територію, що захищається. Є заходами антитерористичного захисту, оскільки проїзд через піднятий бар'єр призводить до руйнування підвіски автомобіля.

Ідентифікатор

Основні типи виконання – картка, брелок, мітка. Є базовим елементом системи контролю доступу, оскільки зберігає код, який служить визначення прав («ідентифікації») власника. Це може бути Touch memory, безконтактна карта (наприклад, RFID-мітка), або застаріваючий тип карток з магнітною смугою. Як ідентифікатор можуть виступати також коди, що вводяться на клавіатурі, або окремі біометричні ознаки людини – відбиток пальця, малюнок сітківки або райдужної оболонки ока, тривимірне зображення обличчя.

Надійність (стійкість до злому) системи контролю доступу значною мірою визначається типом ідентифікатора, що використовується: наприклад, найбільш поширені безконтактні карти proximity можуть підроблятися в майстернях з виготовлення ключів на устаткуванні, наявному у вільному продажу. Тому для об'єктів, які потребують вищого рівня захисту, такі ідентифікатори не підходять. Принципово вищий рівень захищеності забезпечують RFID-мітки, у яких код карти зберігається у захищеній області й шифрується.

Крім безпосереднього використання в системах контролю доступу, RFID-мітки широко застосовуються і в інших областях. Наприклад, у локальних розрахункових системах (оплата обідів у їдальні та інших послуг), системах лояльності тощо.

Контролер

Автономний контролер – це «мозок» системи: саме контролер визначає, чи пропустити власника ідентифікатора у двері, оскільки зберігає коди ідентифікаторів зі списком прав доступу кожного з них у власній енергонезалежній пам'яті. Коли людина пред'являє (підносить до пристрою, що зчитує) ідентифікатор, лічений з нього код порівнюється з зберігається в базі, на підставі чого приймається рішення про відкриття дверей.

Мережевий контролер об'єднується в єдину систему з іншими контролерами та комп'ютером для можливості централізованого контролю та управління. У такому разі рішення про надання доступу може прийматись як

контролером, так і програмним забезпеченням головного комп'ютера. Найчастіше об'єднання контролерів мережу здійснюється за допомогою промислового інтерфейсу RS-485 або локальної мережі Ethernet.

У випадках, коли необхідно забезпечити роботу контролера при аваріях електромережі, блок контролера забезпечується власним акумулятором або зовнішнім блоком резервного живлення. Час роботи від акумулятора може становити від кількох годин до кількох діб.

Зчитувач

Це пристрій, який отримує («зчитує») код ідентифікатора та передає його в контролер. Варіанти виконання зчитувача залежать від типу ідентифікатора: для «таблетки» – це два електричні контакти (у вигляді «лузи»), для proximity-карти – це електронна плата з антеною в корпусі, а для зчитування, наприклад, малюнку райдужної оболонки ока до складу зчитувача має входити камера. Якщо зчитувач встановлюється на вулиці (ворота, зовнішні двері будівлі, проїзд на територію автостоянки), то він повинен витримувати кліматичні навантаження – перепади температур, опади – особливо якщо йдеться про об'єкти в районах із суворими кліматичними умовами. А якщо існує загроза вандалізму, потрібна ще й механічна міцність (сталевий корпус). Окремо можна виділити зчитувачі для дальньої ідентифікації об'єктів (з відстанню ідентифікації до 50 м). Такі системи зручні на автомобільних проїздах, парковках, на в'їздах на платні дороги тощо. Ідентифікатори для таких зчитувачів, як правило, активні (містять вбудовану батарейку).

Конвертери середовища

Служать для підключення апаратних модулів СКУД один до одного та до ПК. Наприклад, є популярними конвертори RS-485 ↔ RS-232 та RS-485 ↔ Ethernet. Деякі контролери СКУД вже мають інтегрований інтерфейс Ethernet, що дозволяє без використання будь-яких додаткових пристроїв підключатися до ПК і зв'язуватися один з одним.

Допоміжне обладнання

Блоки безперебійного живлення, дверні доводчики, датчики відчинення дверей, кнопки, дроти, відеоспостереження і т.д.

Програмне забезпечення

Не є обов'язковим елементом системи контролю доступу, використовується у разі, коли потрібна обробка інформації про проходи, побудова звітів, або коли для початкового програмування, управління та збору інформації в процесі роботи системи необхідне мережне програмне забезпечення, яке встановлюється на один або кілька ПК, з'єднаних у мережа.

Усі СКУД можна віднести до двох великих класів або категорій: мережеві системи та автономні системи.

Популярні компанії виробники програмного забезпечення систем контролю та управління доступу: ITV Group, ZkTeco, PERCo, ControlGate, Hikvision, Bosh, Parsec, Bolid, RusGuard, HID Global, IronLogic, OVISION.

Мережеві системи

У мережі всі контролери з'єднані з комп'ютером, що дає безліч переваг для великих підприємств, але зовсім не потрібно для «однодверної» СКУД. Мережеві системи зручні для великих об'єктів (офіси, виробничі підприємства), оскільки керувати навіть десятком дверей, на яких встановлені автономні системи, стає надзвичайно важко. Незамінні мережеві системи у таких випадках:

– якщо необхідно реалізувати складні алгоритми допуску груп співробітників з різними привілеями до різних зон підприємства та мати можливість оперативно їх змінювати;

– якщо необхідно вибірково видаляти або створювати перепустки (мітки) для великої кількості точок проходу або для великої кількості співробітників (велика текучка та втрати пропусків);

– якщо необхідна інформація про події (архів подій), що відбулися раніше, або потрібен додатковий контроль у реальному часі. Наприклад, у мережній системі існує функція фотоверифікації: на прохідній при піднесенні вхідною людиною ідентифікатора до зчитувача, службовець (вахтер, охоронець) може на екрані монітора бачити фотографію людини, якій у базі даних присвоєно даний ідентифікатор, і порівняти із зовнішністю проходить, що під передачі карток іншим;

– якщо необхідно організувати облік робочого дня та контроль трудової дисципліни;

– якщо необхідно забезпечити взаємодію (інтеграцію) з іншими підсистемами безпеки, наприклад, відеоспостереженням або пожежною сигналізацією).

У мережній системі з одного місця можна не тільки контролювати події на всій території, що охороняється, але і централізовано управляти правами користувачів, вести базу даних. Мережеві системи дозволяють організувати кілька робочих місць, розділивши функції управління між різними співробітниками та службами підприємства.

У мережевих системах контролю доступу можуть застосовуватися бездротові технології, звані радіоканали. Використання бездротових мереж часто визначається конкретними ситуаціями: складно чи неможливо прокласти провідні комунікації між об'єктами, скорочення фінансових витрат на монтаж точки проходу тощо. Існує велика кількість варіантів радіоканалів, однак у СКУД використовуються лише деякі з них.

– Bluetooth. Даний вид бездротового пристрою передачі даних є аналогом Ethernet. Його особливість полягає в тому, що відпадає необхідність прокладати паралельні комунікації для об'єднання компонентів під час використання інтерфейсу RS-485.

– Wi-Fi. Основна перевага даного радіоканалу полягає у великій дальності зв'язку, здатного досягати кількох сотень метрів. Це особливо необхідно для

з'єднання між собою об'єктів на великих відстанях (?). При цьому скорочуються як тимчасові, і фінансові витрати на прокладання вуличних комунікацій.

– ZigBee. Спочатку сферою застосування даного радіоканалу була система охоронної та пожежної сигналізації. Технології не стоять на місці та активно розвиваються, тому ZigBee може використовуватись і в системах контролю доступу. Ця бездротова технологія працює в діапазоні 2,45 ГГц, що не ліцензується.

– GSM. Перевага використання бездротового каналу зв'язку – практично суцільне покриття. До основних методів передачі інформації в мережі, що розглядається, відносяться GPRS, SMS і голосовий канал.

Непоодинокі ситуації, коли встановлення повноцінної системи безпеки може виявитися невиправдано дорогою для вирішення поставленого завдання. У таких ситуаціях оптимальним рішенням буде встановлення автономного контролера на кожну точку проходу, які необхідно обладнати доступом.

Автономні системи

Автономні системи дешевші, простіше в експлуатації, не вимагають прокладання сотень метрів кабелю, використання пристроїв сполучення з комп'ютером, самого комп'ютера. При цьому до мінусів таких систем відноситься неможливість створювати звіти, вести облік робочого часу, передавати та узагальнювати інформацію про події, керуватися дистанційно. При виборі автономної системи з високими вимогами безпеки рекомендується звернути увагу на наступне:

– Зчитувач повинен бути відокремлений від контролера, щоб дроти, якими можливе відкривання замка, були недоступні зовні.

– Контролер повинен мати резервне джерело живлення у разі відключення електроживлення.

– Переважно використовувати зчитувач у вандалозахищеному корпусі.

У складі автономної системи контролю доступу використовуються також електронні замки, що передають інформацію бездротовими каналами зв'язку: у двері встановлюється механічний замок з електронним управлінням і вбудованим зчитувачем. Замок по радіоканалу пов'язаний з хабом, який вже по дротах обмінюється інформацією з робочою станцією, де встановлено програмне забезпечення.

Для автономної системи можна використовувати «зворотний метод», коли на контрольних точках встановлюються ідентифікатори, а співробітники відзначаються зчитувачем-контролером, згодом дані передаються при першій нагоді – поява зв'язку у зчитувача. Цей метод зручно використовувати, наприклад, у місцях, де відсутня зв'язок, можливість прокладання електроживлення або інших комунікацій. Також «зворотний метод» може використовуватися для контролю патрулювання великих периметрів: після обходу території або після закінчення зміни охоронець здає на перевірку контролер, в якому записані всі контрольні точки, що пройшли, із зазначенням послідовності проходу і часу проходу кожної точки.

Додаткові можливості

– GSM модуль, який дозволяє надсилати SMS з інформацією про прохід (використовується, наприклад, у школах).

– для мережевий СКУД (також деякі автономні системи) – можливість віддаленого управління мережею Інтернет (наприклад, управління системою контролю доступу з центрального офісу, якщо підприємство має безліч філій).

– комплекс для персоналізації пластикових карток (принтер для друку на пластиковій картці даних власника, у тому числі фотографії).

– режим «антипасбек» – якщо людина вже пройшла на територію, що охороняється, то повторне пред'явлення її ідентифікатора на вхід буде заборонено (поки карта не буде пред'явлена на вихід), що виключить можливість проходу по одній карті двох і більше осіб. При цьому мережний СКУД дозволяє організувати такий режим на всіх точках проходу, об'єднаних у мережу, що забезпечує повнофункціональний захист по всьому периметру контрольованої території.

Застосування СКУД

Сфери застосування СКУД різноманітні:

– офіси компаній; бізнес-центри;
– банки;
– заклади освіти (школи, технікуми, виші);
– промислове підприємство;
– охоронювані території;
– автостоянки, паркування;
– місця проїзду автотранспорту;
– приватні будинки, житлові комплекси, котеджі;
– готелі;
– громадські установи (спорткомплекси, музеї, метрополітен та ін.).

Основні типи компаній на ринку

– Виробники.
– Дистриб'ютори.
– Проектувальники.
– Інтегратори.
– Торгові будинки.
– Монтажні організації.
– Кінцеві замовники.
– Великі кінцеві замовники (мають власну службу безпеки).

Розділ 9. Відновлення функціонування інформаційно-комунікаційних систем (ІКС) після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження

9.1. Організаційно-технічні заходи відновлення функціонування ІКС.
9.2. Журнал аудиту подій.
9.3. Політики резервного копіювання даних.

9.1. Організаційно-технічні заходи відновлення функціонування ІКС

Можливість повної втрати даних за відсутності програми післяаварійного відновлення ставить під загрозу діяльність організацій, які не мають коштів для відновлення працездатності після катастрофічних подій. У багатьох компаніях планування надзвичайних заходів фокусується вже насамперед на IT. Програма збереження безперервності бізнес-операцій та післяаварійного відновлення може стати одним із найцінніших вкладів відділу IT у успішну діяльність організації.

Шість етапів планування

У термінології планування дій у аварійних ситуаціях фігурують два загальні поняття: **планування збереження безперервності бізнесу (Business Continuity Planning, BCP)** та **планування післяаварійного відновлення (Disaster Recovery Planning, DRP**). Ці поняття, які часто використовуються як рівноцінні, представляють різні концепції.

BCP традиційно передбачає планування заходів, що забезпечують збереження ділової активності організації у надзвичайних ситуаціях.

Сфера відповідальності DRP, за суттю, є підмножиною BCP і стосується відновлення інформації та працездатності систем у разі аварії. Наприклад, вихід з ладу жорсткого диска на сервері бази даних потенційно загрожує цілісності бізнесу, але не є результатом катастрофічних подій. Розрив водопровідної труби з затопленням серверного приміщення і зануренням сервера бази даних у воду становить загрозу цілісності бізнесу, що розглядається в рамках плану післяаварійного відновлення (DRP).

Планування заходів BCP і DRP – справа непроста, і у великих організаціях цим часто займаються спеціальні групи. Однак навіть без детального аналізу ступенів ризику та вирішення інших складних питань у рамках BCP та DRP у великих компаніях можна створити програму збереження цілісності бізнесу та післяаварійного відновлення, якщо дотримуватись наведених нижче етапів.

Етап 1. Визначення критично важливих ділових операцій

Перший крок планування рамках BCP і DRP – визначення критично важливих ділових операцій, тобто. дій, які мають виконуватися у повсякденному режимі задля збереження працездатності організації.

Наприклад, центр прийому заявок клієнтів на виконання технічного обслуговування повинен зберігати здатність приймати та фіксувати заявки.

Юридична фірма повинна мати доступ до інформації про клієнтів, надсилати та приймати електронну пошту, користуватися інтерактивними довідниками з права, а також відповідати на телефонні дзвінки.

На даному етапі планування необхідно співпрацювати з головними відповідальними особами організації у визначенні видів діяльності, важливих для збереження її працездатності. У центрі планування заходів у межах BCP знаходиться збереження ділової активності організації з допомогою відновлення цих видів діяльності.

Етап 2. Упорядкування схеми інфраструктури інформаційних систем, які забезпечують виконання критично важливих ділових операцій.

Від визначення критично важливих ділових операцій переходимо до визначення інформаційних систем, що забезпечують їхнє виконання.

Зокрема, в центрі прийому заявок клієнтів на проведення технічного обслуговування можливість перегляду зареєстрованих та фіксації нових заявок залежить від працездатності серверів бази даних, де зберігаються ці записи, та програм, що забезпечують доступ до цих серверів. Крім того, має також функціонувати певна частина центральної мережної інфраструктури, щоб ці критично важливі ділові операції могли виконуватись. Наведені вище інформаційні системи необхідно підтримувати у працездатному стані за рахунок оперативного післяаварійного відновлення.

Етап 3. Моделі загроз у вигляді передбачуваних та ймовірних подій

Практично всі катастрофи та аварії, що загрожують цілісності бізнесу, є передбачуваними з певним ступенем ймовірності. Катастрофічні події можуть бути природними (землетрус, повінь) або механічними (несправність жорсткого диска, розрив водопровідної труби тощо). Наприклад, якщо служба приймання заявок клієнтів на технічне обслуговування розташована у м. Владивосток, цілком можливо, що інформаційні системи центру рано чи пізно виявляться на шляху шторму. Так само, у будь-якій компанії, що використовує результати технічного прогресу, завжди можлива відмова апаратних засобів.

Визначивши критично важливі системи, можна приступати до моделювання загроз передбачуваних і ймовірних подій. Моделювання дозволяє реалізувати структурний підхід до визначення потенційних загроз, що несуть у собі максимальну небезпеку для цілісності бізнесу, та послаблення їх негативних наслідків. Складіть список можливих сценаріїв порушення працездатності критично важливих інформаційних систем, а також подій, що передують реалізації кожної загрози. Наприклад, працездатність центру прийому заявок клієнтів може бути порушена через недоступність бази заявок, що реєструються. Попередньою подією може стати відмова апаратних засобів, перебій у харчуванні або щось серйозніше, наприклад, руйнування інформаційного центру через шторм.

Етап 4. Розробка планів та процедур збереження цілісності бізнесу

Після складання списку критично важливих ділових операцій, перерахування інформаційних систем, що забезпечують їх виконання, та визначення можливих і ймовірних подій, здатних порушити працездатність зазначених інформаційних систем, можна розпочати вироблення превентивних

заходів, які мають на меті збереження цілісності бізнесу, з використанням моделей загроз.

В рамках **BCP існують чотири категорії превентивних заходів**:

– відмовостійкість та відновлення після збою;

– резервне копіювання;

– «холодне» запасне обладнання та приміщення;

– «гаряче» запасне обладнання та приміщення.

Розглянемо ці категорії більш детально:

– Відмовостійкість та відновлення після збою. Ця категорія превентивних заходів передбачає використання резервних апаратних засобів, що зберігають працездатність при відмові окремих елементів. В IT для забезпечення стійкості до відмови найбільш широко використовуються масиви жорстких дисків, технології кластеризації, акумуляторні і генераторні джерела живлення.

– Резервне копіювання. Резервне копіювання з використанням внутрішньосистемних та позасистемних засобів займає центральне місце серед превентивних заходів у рамках DRP. У разі втрати даних резервне копіювання забезпечує можливість відновлення та реконструкції інформації за останніми даними, що відповідають працездатному стану систем.

– «Холодне» запасне обладнання та приміщення. "Холодне" запасне обладнання – це автономні пристрої, які можна швидко підготувати до виконання робочих функцій. Наприклад, можна тримати набір серверів без підключення до мережі, на яких встановлені операційні системи з налаштуваннями, прийнятими в компанії. У разі аварії можна завершити налаштування конфігурації та відновити або скопіювати дані, необхідні для відновлення роботи. «Холодне» приміщення містить автономне обладнання, яке можна використовувати для відновлення роботи у разі аварії на головному устаткуванні. Часто «холодне» приміщення є просто залом, здатним вмістити робочі столи та стільці. Для більшості організацій малого та середнього бізнесу (SMB) утримання «холодних» приміщень не є економічно вигідним.

– «Гаряче» запасне обладнання та приміщення. "Гаряче" запасне обладнання – це пристрої, готові до негайної роботи у надзвичайній ситуації. Наприклад, можна безперервно дублювати критично важливу інформацію із занесенням у віддалену базу даних та забезпечити можливість перенаправлення клієнтських додатків до цих копій даних у разі потреби. "Гаряче" обладнання дозволяє дуже швидко відновлювати виконання операцій. Швидкість приведення «гарячого» устаткування працездатний стан зазвичай визначається часом, необхідним співробітникам прибуття до місця зберігання запасного устаткування. «Гаряче» обладнання має в своєму розпорядженні точні копії даних в реальному часі (або майже в реальному часі) і завжди працездатне. Утримання «гарячого» запасного обладнання та приміщень обходиться дорого, тому цей варіант використовується тільки в організаціях, які повинні зберігати працездатність у надзвичайних ситуаціях, наприклад у відомствах державної безпеки.

Етап 5. Розробка планів та процедур післяаварійного відновлення

Не всі події є передбачуваними та ймовірними. Важко знайти більш вдалий приклад непередбачуваної катастрофи, ніж атака на всесвітній торговий центр 11 вересня 2001 р. Для надзвичайних обставин такого роду, а також інших серйозних катастроф, у яких можлива повна втрата даних і працездатності головних систем, необхідна розробка планів і процедур відновлення. Оскільки післяаварійне відновлення відноситься до стресових ситуацій, дуже важливо мати під рукою добре документовані, перевірені та випробувані на практиці процедури. Переконатися у працездатності даних, які зберігаються на резервних носіях, можна як імітації роботи процедур відновлення.

Необхідно подбати про засоби позасистемного зберігання копій процедур, які виконуються в рамках DRP, разом із перевіреними працездатними резервними копіями. Для більшості організацій найбільш ефективним, доступним та безпечним варіантом позасистемного зберігання перевірених резервних копій та планів DRP є депозитарні осередки та банківські сейфи.

Етап 6. Перевірка працездатності планів збереження цілісності бізнесу та випробування на практиці засобів післяаварійного відновлення

Сам характер обставин, що змушують складати плани BCP та DRP, передбачає необхідність гарантії працездатності планів, процедур та технологій, що використовуються для збереження цілісності бізнесу.

Проведіть плановані і спонтанні навчання для перевірки стану стратегій BCP і DRP. Можна щомісяця імітувати відмова кластерних вузлів, періодично виконувати відновлення «холодних» запасних серверів чи проводити повномасштабні імітації катастрофічних ситуацій із перевіркою працездатності «холодних» і «гарячих» засобів відновлення. Як мінімум, слід виконати відновлення критично важливих даних щодо резервних копій з носіїв, що зберігаються поза офісом. Носії резервних копій, що зберігаються поза офісом, – остання лінія захисту від повної втрати даних.

Шість етапів захисту від катастрофи

Виконуючи перелічені етапи, можна допомогти підприємству створити програму BCP та DRP, яка забезпечить захист від наслідків природних, механічних та обумовлених людським фактором катастроф. Коли стільниковий телефон дзвонить о другій годині ночі, найменше хочеться гарячково винаходити шляхи відновлення даних, що знаходяться на сервері та стрічках і пробули під водою протягом 30 годин, або, що ще гірше, після фізичного руйнування інформаційного центру внаслідок катастрофи.

9.2. Журнал аудиту подій

Для вирішення завдання обробки інцидентів інформаційної безпеки (ІБ) логічно міркувати, що чим більше даних (логів, подій безпеки) ми збираємо, зберігаємо та аналізуємо, тим простіше нам буде надалі не тільки оперативно зреагувати на інцидент, але й розслідувати обставини атак, що відбулися, для пошуку причин їх виникнення. При цьому велика кількість даних для обробки

має і очевидний мінус: нас може просто «засипати» повідомленнями, алеутами (попередженями), повідомленнями, тому необхідно обрати найзначніші з погляду ІБ події та налаштувати відповідні політики аудиту.

Microsoft пропонує використовувати безкоштовний набір утиліт та рекомендацій (Baselines) у своєму наборі Microsoft Security Compliance Toolkit, в якому в тому числі наведені та рекомендовані налаштування аудиту для контролерів домену, рядових серверів та робочих станцій.

Крім рекомендацій вендора можна звернутися ще до документів CIS Microsoft Windows Server Benchmark і CIS Microsoft Windows Desktop Benchmark, в яких, серед іншого, вказані рекомендовані експертами політики аудиту для серверних і десктопних версій ОС Windows.

Однак найчастіше виконання абсолютно всіх рекомендацій неефективне саме через потенційну появу великої кількості «шумлячих», малозначних з погляду ІБ подій, тому в цьому розділі наведемо список найбільш корисних і ефективних (на наш погляд) політик аудиту безпеки та відповідних типів подій безпеки Windows.

В ОС Microsoft Windows, починаючи з Microsoft Windows Server 2008 і Vista, використовується досить просунута система аудиту, яка настроюється за допомогою конфігурування розширених політик аудиту (Advanced Audit Policy Configuration). Не варто забувати про те, що як тільки на пристроях будуть включені політики розширеного аудиту, за замовчуванням старі «класичні» політики аудиту перестануть бути ефективними, хоча ця поведінка може бути перевизначена в груповій політиці. аудиту (Windows Vista або наступні версії))» (Audit: Force audit policy subcategory settings).

Політики аудиту Windows

Пройдемо послідовно за налаштуваннями, ефективними для вирішення завдань аудиту ІБ та вироблення цілісної політики аудиту безпеки.

Крім описаних у таблиці 9.1 налаштувань, має сенс контролювати появу в журналі безпеки події з EventID=1102, яке формується відразу після очищення журналу безпеки, що може говорити про шкідливу активність. Більше того, розумно буде включити в каталозі «Конфігурація комп'ютера – Конфігурація Windows – Параметри безпеки – Локальні політики – Параметри безпеки» політику «Мережева безпека: обмеження NTLM: вихідний трафік NTLM до віддалених серверів» у значення «Аудит всього». Після цього EventID=8001 у журналі Microsoft-Windows-NTLM/Operational міститиме інформацію про автоматичну автентифікацію на веб-ресурсах з обліковим записом користувача. Наступним кроком стане allow list із переліком веб-ресурсів, які легітимно можуть вимагати облікові записи, а вказану політику можна буде перевести в режим блокування. Це не дозволить шкідливим ресурсам отримувати NTLM-ґеші користувачів, які натиснули на посилання з фішингового листа.

Звернімо увагу і на те, що підсистема журналювання Windows дуже гнучка і дозволяє налаштувати аудит довільних папок і гілок реєстру – слід вибрати критичні для ІТ-інфраструктури об'єкти аудиту і включити дані опції.

Таблиця 9.1 – Політики аудиту Windows

Категорія аудиту	**Підкатегорія аудиту**	**Події аудиту**	**EventID**	**Коментарі**
Вхід облікового запису	Аудит перевірки облікових даних	Успіх, Відмова	4776	Доцільно контролювати на домен-контролерах під час використання NTLM-автентифікації.
	Аудит служби автентифікації Kerberos	Успіх, Відмова	4771	Неуспішна автентифікація облікового запису на контролері домену за допомогою Kerberos-автентифікації.
			4768	Запит квитка Kerberos, слід аналізувати коди відповіді сервера.
	Примітка: Даний тип аудиту слід включати на контролерах домену, при цьому для детального вивчення спроб підключення та отримання IP-адреси пристрою, що підключається на контролері домену, слід виконати команду nltest /dbflag:2080ffff і проводити аудит текстового лог-файлу %windir%\debug\netlogon. log			
Управління обліковими записами	Аудит керування обліковими записами комп'ютерів	Успіх	4741	Заведення пристрою до домену Active Directory; може використовуватися зловмисниками, оскільки будь-який користувач домену за замовчуванням може завести домен 10 пристроїв, на яких може бути встановлено неконтрольоване компанією ПЗ, у тому числі шкідливе.
	Аудит управління групами безпеки	Успіх, Відмова	4728	Додавання члена глобальної групи.
			4732	Додавання члена локальної групи.
			4756	Додавання члена універсальної групи.

	Аудит керування обліковими записами користувачів	Успіх, Відмова	4720	Створення облікового запису.
			4725	Вимкнення облікового запису.
			4740	Блокування облікового запису.
			4723	Зміна пароля.
			4724	Скидання пароля.
Детальне відстеження	Аудит створення процесів	Успіх	4688	Під час створення процесу.
			4689	Після завершення процесу.
	Примітка: Щоб для командного інтерпретатора вівся запис введених команд, слід включити політику «Конфігурація комп'ютера – Конфігурація Windows – Адміністративні шаблони – Система – Аудит створення процесів –> Включати командний рядок у події створення процесів». Примітка: Щоб вести запис виконуваних PowerShell-команд і завантажених PowerShell-модулів, слід увімкнути в каталозі «Конфігурація комп'ютера – Конфігурація Windows – Адміністративні шаблони – Компоненти Windows – Windows PowerShell» політики «Увімкнути ведення журналу модулів» (у налаштуваннях політики вказати всі модулі символом «* ») та «Включити реєстрацію блоків сценаріїв PowerShell» (у налаштуваннях політики відзначити check-box «Реєстрація початку або зупинення виклику блоків сценаріїв»). Робота скриптів PowerShell реєструється з EventID=4104,4105,4106 у журналі Microsoft-Windows-PowerShell/Operational, а завантаження PowerShell-модулів реєструється з EventID=800 у журналі Windows PowerShell.			
Вхід вихід	Аудит виходу із системи	Успіх	4634	Для неінтерактивних сесій.
			4647	Для інтерактивних сесій та RDP-підключень.
	Примітка: При цьому слід звертати увагу на код Logon Type, який показує тип підключення (інтерактивне, мережне, із закешованими обліковими даними, з наданням облікових даних у відкритому вигляді тощо).			

	Аудит входу до системи	Успіх, Відмова	4624	При успішній спробі автентифікації створюється на локальному ПК і на домен-контролері при використанні NTLM і Kerberos-автентифікації.
			4625	При неуспішній спробі автентифікації створюється на локальному ПК і на домен-контролері при використанні NTLM автентифікації; при Kerberos-автентифікації на контролері домену створюється EventID=4771.
			4648	При спробі входу з явною вказівкою облікових даних, наприклад, при виконанні команди runas, а також при роботі хакерської утиліти Mimikatz.
	Примітка: При цьому слід звертати увагу на код входу (Logon Type), який показує тип підключення (інтерактивне, мережне, із закешованими обліковими даними, з наданням облікових даних у відкритому вигляді тощо). Доцільно також звертати увагу на код помилки (Status/SubStatus), який також зберігається у події аудиту та характеризує причину неуспішного входу – неіснуюче ім'я облікового запису, недійсний пароль, спроба входу із заблокованим обліковим записом тощо.			
	Аудит інших подій входу та виходу	Успіх, Відмова	4778	RDP підключення було встановлено.
			4779	RDP-підключення було розірвано.
	Аудит спеціального входу	Успіх	4672	На вході з адміністративними повноваженнями.

Доступ до об'єктів	Аудит відомостей про загальний файловий ресурс	Успіх, Відмова	5145	При доступі до системних мережних ресурсів, таких як \C$\. Ця подія буде створюватися під час роботи ransomware, націленого на горизонтальне переміщення по мережі.
	Аудит інших подій доступу до об'єктів	Успіх, Відмова	4698	Під час створення завдання у «Планувальнику завдань», що часто використовується зловмисниками як метод закріплення та приховування активності в атакованій системі.
Зміна політики	Аудит зміни політики аудиту	Успіх	4719	Зміна політики аудиту.
			4906	Зміна налаштування CrashOnAuditFail.
	Примітка: Змінити реакцію ОС на неможливість вести журнал аудиту безпеки (налаштування CrashOnAuditFail) можна в каталозі «Конфігурація комп'ютера – Конфігурація Windows – Параметри безпеки – Локальні політики – Параметри безпеки» у політиці «Аудит: негайне відключення системи, якщо неможливо внести в журнал запису про аудит безпеки ».			
Система	Аудит розширення системи безпеки	Успіх	4610 4614 4622	З появою у системі нових пакетів автентифікації, що має відбуватися несанкціоновано.
			4697	При створенні нового сервісу, який часто використовується зловмисниками як метод закріплення та приховування активності в атакованій системі.

Утиліта Sysmon

Окрім залучення штатного функціоналу підсистеми журналювання, можна скористатися і офіційною безкоштовною утилітою Sysmon із пакета Microsoft

Windows Sysinternals, яка суттєво розширює та доповнює можливості моніторингу ОС. Дана утиліта дає можливість проводити аудит створення файлів, ключів реєстру, процесів та потоків, а також здійснювати моніторинг завантаження драйверів та бібліотек, мережевих підключень, WMI-подій та іменованих каналів. З особливо корисних функцій відзначимо можливість утиліти показувати батьківський процес та командний рядок процесу, відображати значення ґеш-сум при подіях створення процесу та завантаження драйверів та бібліотек із зазначенням наявності та дійсності цифрового підпису. Нескладним шляхом можна автоматизувати порівняння отриманих ґеш-сум з індикаторами компрометації (IoCs, Indicator of Compromise) з даних фідів CyberThreat Intelligence, а також використовувати додаток QVTI для IBM QRadar, за допомогою якого ґеші файлів, що запускаються, автоматично перевіряються через сервіс VirusTotal. Ще однією приємною опцією є можливість створення XML-конфігурацій, в яких можна чітко вказати об'єкти контролю та налаштування роботи Sysmon. Одними з найбільш розвинених і детальних варіантів XML-конфігурацій, на наш погляд, є конфіги https://github.com/ion-storm/sysmon-config і https://github.com/SwiftOnSecurity/sysmon-config.

9.3. Політики резервного копіювання даних

9.3.1 Політика резервного копіювання даних

Резервне копіювання або бекап – створення копій всіх файлів, наявних на пристрої, жорсткого диска на інших пристроях або передача їх для зберігання в хмарі на випадок втрати або пошкодження комп'ютера.

Виділяють два види резервного копіювання:

1. Повне, при якому копіюються всі важливі файли, що зберігаються на комп'ютері або знаходяться на корпоративному сервері або в хмарі.
2. Диференціальне, коли спочатку на носій копіюються всі файли, а потім згідно з встановленим заздалегідь графіком копіюються дані, які були змінені.

Другий варіант вважається найбільш продуктивним. Але, тим не менш, не всі програми на даний момент підтримують резервне копіювання даних.

Причини втрати даних

До найбільш частих причин, через які відбувається втрата даних, можна віднести:

– Помилки власника, коли потрібні і важливі документи і файли видаляються через неуважність або помилок.

– Збій системи. В такому випадку файл може бути, як видалений, так і пошкоджений, що унеможливлює роботу з цим файлом.

– Вірус. Занесений в систему вірус або шкідлива програма може стати як причиною пошкодження або видалення файлів з жорсткого диска, так і зміни даних в ньому.

– Шифрувальник. Останнім часом в компаніях дуже гостро постала проблема з вірусами шифрувальниками, вони повністю зашифровують жорсткий

диск, а якщо комп'ютер включений в локальну мережу, то і всі комп'ютери в локальній мережі і сервери компанії. Після такого шифрування ви не зможете користуватися комп'ютерами і серверами до тих пір, поки ви не сплатите хакерам їх вимогу за розшифровку даних. Але навіть якщо ви оплатили, з великою ймовірності вам все одно нічого не розшифрують і дані будуть назавжди загублені, а гроші витрачені.

– Хакерська атака може пошкодити файли, що зберігаються на сервері компанії або бухгалтерські бази даних.

– Вихід з ладу жорсткого диска або комп'ютера в цілому.

Періодичність виконання резервного копіювання

Резервне копіювання даних необхідно виконувати з тією частотою, з якою відбувається оновлення документів. Наприклад, якщо компанія щодня вносить зміни в свої файли, формує звіти – то виконувати резервну копію необхідно щодня, в кінці робочого дня. Якщо фірма невелика, і файли зі звітністю оновлюються раз на тиждень – то дані необхідно копіювати щотижня.

Копіювання обов'язково необхідно виконувати і перед перевстановленням операційної системи або при оновленні програмного забезпечення.

Для того щоб не забувати вчасно робити бекап, слід встановити спеціальну програму для резервного копіювання даних. Як налаштувати резервне копіювання для тієї чи іншої програми, можна дізнатися з інструкції до неї або звернеться до обслуговуючого системного адміністратора.

Програмне забезпечення буде або нагадувати власнику про необхідність чергового бекапа, або ж виконувати його самостійно, якщо мова йде про копіювання документів в хмарне сховище.

Вибір програми для створення резервної копії

При виборі програми необхідно звернути увагу на кілька основних параметрів:

– Можливість налаштування розкладу копіювання даних. Важливо, щоб програма заздалегідь нагадувала вам про необхідність виконати резервне копіювання.

– Управління розміщенням і копіями даних. Програма повинна підтримувати можливість резервного копіювання даних на кілька носіїв. Більш того, аналізувати всі файли і вибирати для копіювання ті, в які були внесені зміни з дати останнього резервного копіювання.

– Програма повинна підходити співробітникам і бути проста в управлінні. Чим простіше інтерфейс і чим швидше ваші співробітники навчаться користуватися програмою, тим краще.

Носії для зберігання резервних копій

Серед найбільш популярних фізичних носіїв для зберігання інформації виділимо:

1. SSD і HDD диски. Це жорсткі диски з великим об'ємом вбудованої пам'яті. Незважаючи на високу вартість, вважаються одними з найбільш надійних. Проте, їх необхідно берегти від ударів і падінь, в іншому випадку, накопичувач може вийти з ладу.

2. USB-накопичувачі з великим об'ємом пам'яті. З переваг можна виділити порівняно невелику вартість пристрою, компактність і зручність підключення до будь-якого пристрою. З мінусів-обмежена кількість записів і менший обсяг пам'яті.

3. Оптичні диски CD, DVD або Blu-ray. Бюджетний варіант, у якого є маса недоліків. В першу чергу, невеликий обсяг вільної пам'яті. По-друге, це нетривалий час служби. Диски необхідно оберігати від перепадів температури, впливу ультрафіолету, механічних пошкоджень.

4. Мережеві сховища NAS. Це спеціальні пристрої невеликого розміру, в яких встановлені жорсткі диски. Мережеве сховище підключається в локальну мережу організації після чого всі комп'ютери і сервери компанії можуть централізовано здійснювати резервне копіювання даних на цей тип носія інформації. Це найбільш дорогий спосіб організації резервного копіювання даних, але і найефективніший і не вимагають будь-яких дій від користувача. Система резервного копіювання на мережеве сховище налаштовується системним адміністратором один раз і потім працює довгий час без збоїв.

Хмарні сервіси зі створення та зберігання резервних копій

Створення резервної копії в хмарі на iCloud або Google Drive є одним з популярних варіантів. Більшість сервісів надають клієнтам можливість самостійно вибирати необхідний обсяг сховища і оплачувати тільки використовуване місце. Крім того, деякі фірми і зовсім надають своїм користувачам кілька гігабайт в хмарі безкоштовно, що ідеально підходить для невеликих фірм і компаній.

Незважаючи на свою простоту і порівняно невисоку вартість, використання хмарного сервісу для зберігання інформації має і свої недоліки.

В першу чергу, це передача корпоративної інформації на чужий сервер. При неналежному рівні захисту, вона в будь-який момент може стати надбанням громадськості.

Крім того, провайдери, що надають хмарні технології та їх розробники не несуть відповідальності за збої в мережі і тим більше не відповідають за видалення даних. Тобто, при збої в роботі сервера, зникнення важливої інформації компанія може зазнати збитків, які їй ніхто не відшкодує.

Крім того після закінчення підписки дані клієнтів і їх файли видаляються з хмарного сервісу. Звичайно, цей процес не буде запущений відразу після закінчення терміну підписки, але як мінімум протягом місяця ваші дані будуть видалені. Хорошим варіантом є наявність власного сервера або мережевого сховища для резервного копіювання даних.

Дані, які підлягають резервуванню

І все ж, які документи потребують резервного копіювання?

– В першу чергу, це робочі документи: бланки договорів, статутні документи підприємства, анкети співробітників та інша документація, яка не особливо бере участь в роботі підприємства, але в той же час повинна завжди бути під рукою на випадок перевірки.

– Звіт. Наприклад, резервне копіювання бухгалтерських програм і всіх створених в програмі звітів.

– База даних. Бухгалтерська база та інші важливі бази даних обов'язково повинні резервуватися.

– Закладки браузера. Чи не найнеобхідніше, але в деяких ситуаціях не буде зайвим мати копії адрес відвідуваних вами і корисних для компанії сайтів.

– Файли налаштувань програм, які часто використовуються на підприємстві.

– Контакти. Всі важливі контакти, зокрема, дані Ваших партерів, їх номери телефонів, адреси електронної пошти повинні бути продубльовані.

Бажано робити не одну, а кілька резервних копій, щоб уникнути неприємних ситуацій, коли інформація втрачена, а флешка або диск з резервною копією був загублений. Найкраще зробити кілька резервних копій на різних носіях і зберігати їх в різних місцях.

Порядок створення резервної копії

Резервне копіювання серверів або даних комп'ютера повинно проходити в кілька основних етапів.

1. На першому етапі підключається зовнішній накопичувач або ж відбувається підключення до хмари або мережевого сховища.
2. На другому етапі відбувається безпосередньо копіювання всіх необхідних даних.
3. На третьому етапі важливо перевірити дані, поміщені в резервне сховище: чи всі вони були передані, коректно відкриваються, чи не пошкоджені архіви.
4. Останній етап – відключення накопичувача.

Попередньо можна використовувати програми-архіватори, щоб файли займали менше місця.

Резервне копіювання даних – це не модна тенденція, а необхідність. Вчасно збережені дані не потрібно відновлювати, витрачаючи час і гроші. Незважаючи на те, що дані можна відновити навіть після того, як вони були видалені з кошика, все ж резервне копіювання залишається єдиним надійним варіантом зберігання даних. Це пов'язано з тим, що для відновлення видалених файлів знадобитися установка спеціальних програм, а в деяких випадках, допомогти зможе тільки фахівець з сервісного центру.

9.3.2 Політика резервного копіювання сайту

Резервні копії потрібні, коли основні файли сайту втрачені або пошкоджені. Статися це може в різних ситуаціях, ось розповсюдженіші з них:

– **Несвоєчасна оплата послуг**. По завершенні сплаченого періоду хостингу доступ до нього блокується. Зазвичай провайдери залишають клієнту можливість продовжити термін послуги ще якийсь час. Наприклад, ми зберігаємо клієнтські файли ще 95 днів.

– **Зараження сайту вірусом**. Для створення сайту багато хто використовує відкриті системи управління контентом на зразок Joomla або WordPress. Це зручно, швидко й безкоштовно. При цьому в таких систем є мінус – відкритий код, що дозволяє зловмисникам знаходити «дірки» і зламувати проекти. Резервне копіювання допоможе відновити сайт таким, яким він був до

зламу. Але тут важливо розуміти, що резервна копія не закриє «дірок» у сайті, їх повинні виправляти розробники.

– **Помилкове видалення файлів**. Усі ми робимо помилки. Іноді такі помилки можуть коштувати дуже дорого. Наприклад, якщо ви випадково видалите файли власного сайту, то без наявності резервної копії відновити їх не зможете.

– **Зникнення розробника або системного адміністратора**. Наймані фахівці не завжди якісно виконують роботу, а іноді й зовсім зникають безслідно. Особливо це актуально для людей, найнятих на біржах фрилансу. Наприклад, ви замовили розробку сайту, оплатили роботу, зробили сайт, але в якийсь момент розробник зник. Не бере слухавку і не відповідає на повідомлення. Що робити? Діставати резервну копію, звичайно! Якщо вона є. Рекомендую всім реєструвати хостинг і домен одразу на свої особисті дані. У такому випадку ви зможете відновити послуги, звернувшись до провайдера.

– **Переїзд з одного хостингу на інший.** Якщо поточний хостинг-провайдер вас не влаштовує, його потрібно змінювати. Суть переїзду в тому, щоб взяти копію сайту і завантажити її на новий сервер. Створюючи копію перед переїздом, перевірте, щоб вона містила всі файли та бази даних.

Як створювати резервні копії та де зберігати бекап

Щоб мати можливість у будь-який час дня і ночі розгорнути бекап, потрібно перш за все зробити копію і вибрати правильне місце для її зберігання.

Якщо ми говоримо про стандартну послугу з розміщення сайту – хостинг, то зазвичай провайдери самі роблять копії файлів раз на якийсь період. Знайти таку копію можна в панелі керування послугою.

Існує так звана «ротація» копій, коли старіша копія змінюється новою. Купуючи простий віртуальний хостинг для свого сайту, ви можете як зберігати копії на сервері провайдера, так і завантажувати їх на особистий комп’ютер або сторонній сервіс.

Резервне копіювання можна зробити й примусово, наприклад, перед внесенням глобальних змін у сайт. Якщо щось піде не так, ви зможете «відкотитися» до попередньої версії, просто розгорнувши резервну копію.

Якщо ж мова йде про віртуальні та виділені сервери, то найчастіше резервне копіювання – це завдання розробників, системних адміністраторів або тих, хто підтримує проект. Оскільки подібні послуги вимагають передачу клієнту сервера в повне керування, провайдер просто не має доступу до налаштувань і файлів.

Для створення резервних копій необхідно розробити і правильно налаштувати систему. Для цього можна використовувати вже готові скрипти і програмне забезпечення або створити їх самостійно. Також важливо вибрати й місце для зберігання створених копій.

В ідеалі це має бути ще один сервер, розташований в іншому дата-центрі (центрі зберігання й обробки даних), щоб мінімізувати ризики.

Ось три конкретні рекомендації, як не втратити сайт:

– Перевірте, чи налаштована функція створення резервних копій на вашому хостингу, віртуальному або виділеному сервері.

– Дізнайтеся, де зберігаються резервні копії.

– Зберігайте копію раз на певний час (залежить від частоти внесення змін на сайті) в альтернативному сховищі.

Розділ 10. Моніторинг процесів функціонування інформаційно-комунікаційних систем (ІКС)

10.1. Джерела інформації про події та типи подій, що аналізуються в системах моніторінгу.

10.2. Система візуалізації та управління подіями (SIEM).

10.3. Аналіз подій

10.1. Джерела інформації про події та типи подій, що аналізуються в системах моніторінгу

До джерел інформації про події та типи подій, що аналізуються в системах моніторингу відносяться наступні:

– Журнали подій серверів та робочих станцій. Застосовуються для контролю доступу, забезпечення безперервності, дотримання політик інформаційної безпеки. Записуються тонкими і товстими клієнтами.

– Антивірусні програми. Генерують події про працездатність ПЗ, бази даних, зміну конфігурацій і політик, шкідливий код. Повідомляють про знаходження шкідливого програмного забезпечення або коду.

– Засоби антиексплойт захисту дозволяють виявляти та запобігати шкідливому впливу експлойтів, тобто. програм або набору команд, які використовують вразливість встановленого прикладного чи системного програмного забезпечення.

– «Пісочниці», або, по-науковому, засоби ізольованого виконання програм дозволяють запускати підозрілий файл в ізольованому віртуальному середовищі, яке спеціально призначене для пошуку аномалій або потенційно шкідливої поведінки досліджуваного файлу.

– DLP системи. Системи запобігання витоку (англ. Data Leak Prevention, DLP) – технології запобігання витоку конфіденційної інформації з інформаційної системи зовні, а також технічні пристрої (програмні або програмно-апаратні) для запобігання витоку. DLP-системи будуються на аналізі потоків даних, що перетинають периметр інформаційної системи, що захищається. При детектуванні в цьому потоці конфіденційної інформації спрацьовує активний компонент системи, і передача повідомлення (пакету, потоку, сесії) блокується. Відомості про спроби інсайдерських витоків, порушення прав доступу. Контролюють і не допускають несанкціоноване переміщення інформації за межі мережі.

– Системи контролю доступу, Access Control, Authentication. Застосовуються для моніторингу контролю доступу до інформаційних систем та використання привілеїв.

– IDS/IPS-системи. Система запобігання вторгнень (англ. Intrusion Prevention System, IPS) – програмна або апаратна система мережевої та комп'ютерної безпеки, що виявляє вторгнення або порушення безпеки і автоматично захищає від них. Системи IPS можна як розширення Систем

виявлення вторгнень (IDS), оскільки завдання відстеження атак залишається однаковою. Однак, вони відрізняються в тому, що IPS повинна відстежувати активність у реальному часі та швидко реалізовувати дії щодо запобігання атакам. Надають відомості про мережеві атаки, зміни конфігурації та доступ до пристроїв.

– Міжмережеві екрани. Відомості про атаки, шкідливе ПЗ, інциденти безпеки та інше.

– Мережеве активне обладнання. Використовується для контролю доступу, обліку мережевого трафіку.

– Системи веб-фільтрації. Надають дані про відвідування співробітниками підозрілих або заборонених веб-сайтів, контролює доступ до шкідливих сайтів.

– Сканери вразливостей. Дані про інвентаризацію активів, сервісів, програмного забезпечення, уразливостей, постачання інвентаризаційних даних та топологічної структури.

– Системи інвентаризації та asset-management. Поставляють дані для контролю активів в інфраструктурі та виявлення нових.

– Системи ресурсів-приманок для зловмисників (англ. honeypots і honeynets) є заздалегідь створеними «муляжами» інформаційних систем, схожими на реальні системи компанії, але не містять жодних цінних даних. Атакуючі, потрапивши в таку пастку, спробують застосувати свій інструментарій для проведення атаки, а в цей момент їхні дії ретельно журналюватимуться і потім вивчатимуть фахівці захисту інформації.

– Засоби управління портативними пристроями (MDM – Mobile Device Management) є програмами контролю та захисту портативних пристроїв співробітників організації. Встановивши такий засіб на свій пристрій, співробітник може отримати контрольований та безпечний віддалений доступ до IT-ресурсів організації, наприклад, підключивши собі на смартфон робочу пошту.

10.2. Система візуалізації та управління подіями (SIEM)

SIEM (Security information and event management) – об'єднання двох термінів, що позначають область застосування ПЗ: SIM (Security information management) – управління інформацією про безпеку, і SEM (Security event management) – управління подіями безпеки. Технологія SIEM забезпечує аналіз у реальному часі подій (тривог) безпеки, що виходять від мережевих пристроїв та додатків, і дозволяє реагувати на них до настання істотних збитків.

З зростаючим обсягом інформації, що обробляється та передається між різними інформаційними системами (ІС), організації та окремі користувачі все більше залежать від безперервності та коректності виконання цих процесів. Для реагування на загрози безпеці в ІС необхідно мати інструменти, що дозволяють **аналізувати в реальному часі події**, кількість яких тільки зростає. Одним із рішень даної проблеми є використання SIEM-систем.

Основним принципом системи SIEM є те, що дані про безпеку інформаційної системи збираються з різних джерел, і результат їх обробки надається в єдиному інтерфейсі, доступному для аналітиків безпеки, що полегшує вивчення характерних особливостей, що відповідають інцидентам безпеки.

SIEM є об'єднанням систем управління інформаційною безпекою(SIM) та управління подіями безпеки (SEM) в єдину систему управління безпекою. Сегмент SIM в основному відповідає за аналіз історичних даних, намагаючись покращити довгострокову ефективність системи та оптимізувати зберігання історичних даних. Сегмент SEM, навпаки, наголошує на вивантаженні з наявних даних певного обсягу інформації, за допомогою якого можуть бути негайно виявлені інциденти безпеки. У міру зростання потреб у додаткових можливостях безперервно розширюється та доповнюється функціональність цієї категорії продуктів.

Однією з головних цілей використання SIEM-систем є підвищення рівня інформаційної безпеки в існуючій архітектурі за рахунок забезпечення можливості маніпулювати інформацією про безпеку та здійснювати попереджувальне управління інцидентами та подіями безпеки в близькому до реального часу режимі.

Випереджальне управління інцидентами та подіями безпеки полягає у ухваленні рішень ще до того, як ситуація стане критичною. Таке управління може здійснюватися з використанням автоматичних механізмів, які прогнозують майбутні події на основі історичних даних, а також автоматичне підстроювання параметрів моніторингу подій до конкретного стану системи.

SIEM представлено програмами, приладами або послугами, і використовується також для журналування даних та генерації звітів з метою сумісності з іншими бізнес-даними.

Поняття *управління подіями інформаційної безпеки* (SIEM), введене Марком Ніколеттом та Амрітом Вільямсом з компанії Gartner у 2005 р., описує функціональність збору, аналізу та подання інформації від мережевих пристроїв та пристроїв безпеки, додатків ідентифікації (управління обліковими даними) та управління доступом, інструментів підтримки політики безпеки та відстеження вразливостей, операційних систем, баз даних та журналів додатків, а також відомостей про зовнішні загрози. Основна увага приділяється управлінню привілеями користувачів та служб, службами каталогів та іншим змінам конфігурації, а також забезпеченню аудиту та огляду журналів, реакціям на інциденти.

Розв'язувані завдання:

– збір, обробка та аналіз подій безпеки, що надходять до системи з багатьох джерел;

– виявлення в режимі реального часу атак та порушень критеріїв та політик безпеки ;

– оперативна оцінка захищеності інформаційних, телекомунікаційних та інших критично важливих ресурсів;

– аналіз та управління ризиками безпеки;
– проведення розслідувань інцидентів;
– прийняття ефективних рішень щодо захисту інформації;
– формування звітних документів

Архітектура

Зазвичай, SIEM-система розгортається над інформаційною системою, що захищається, і має архітектуру «джерела даних» – «сховище даних» – «сервер додатків».

SIEM-рішення являють собою інтегровані пристрої (all-in-one) або двотрикомпонентні комплекси. Розподілена архітектура найчастіше передбачає велику продуктивність і кращі можливості масштабування, а також дозволяє розгорнути SIEM-рішення в IT-інфраструктурах з кількома майданчиками.

Агенти виконують початкову обробку та фільтрацію, а також збирання подій безпеки.

Передача інформації від джерел даних може здійснюватися кількома способами:

– джерело ініціює передачу подій (наприклад, відправляє по syslog-протоколу);
– події з джерела забираються пасивно.

Розглянемо використання цих методів практично.

З першим варіантом все досить просто: на джерелі вказується IP-адреса пристрою, що здійснює збір подій (колектора), і події відправляються адресату.

Другий варіант включає агентний або безагентний збір інформації, причому в деяких SIEM-системах частини джерел доступні обидва способи.

Агентний спосіб передбачає використання спеціальної програми-агента, безагентний – налаштування джерела подій, такі як створення додаткових облікових записів, дозвіл віддаленого доступу та використання додаткових протоколів.

Зібрана та відфільтрована інформація про події безпеки надходить до сховища даних, де вона зберігається у внутрішньому форматі подання з метою подальшого використання та аналізу сервером додатків.

Сервер програм реалізує основні функції захисту інформації. Він аналізує інформацію, що зберігається в репозиторії, і перетворює її для вироблення попереджень або управлінських рішень щодо захисту інформації.

Виходячи з цього, в SIEM-системі виділяються такі **рівні її побудови**:

– збирання даних: здійснюється від джерел різних типів, наприклад, файлових серверів, міжмережевих екранів, антивірусних програм;
– керування даними: дані, що зберігаються в репозиторії, видаються за запитами моделей аналізу даних;
– аналіз даних: результатом є звіти у визначеній і довільній формі, оперативна кореляція даних про події, а також попередження, що видаються.

Функціонування SIEM

Для вирішення поставлених завдань SIEM-системи першого покоління застосовують нормалізацію, фільтрацію, класифікацію, агрегацію, кореляцію та пріоритезацію подій, а також генерацію звітів та попереджень.

У SIEM-системах нового покоління до них слід додати також аналіз подій, інцидентів та їх наслідків, а також прийняття рішень та візуалізацію.

Нормалізація наводить формати записів журналів, зібраних із різних джерел, до єдиного внутрішнього формату, який потім буде використовуватися для їх зберігання та подальшої обробки.

Фільтрація подій безпеки полягає у видаленні надлишкових подій з потоків, що надходять в систему.

Класифікація дозволяє для атрибутів подій безпеки визначити їхню належність певним класам.

Агрегація поєднує події, схожі за певними ознаками.

Кореляція виявляє взаємозв'язок між різнорідними подіями.

Пріоритезація визначає значущість та критичність подій безпеки на підставі правил, визначених у системі.

Аналіз подій, інцидентів та їх наслідків включає процедури моделювання подій, атак та їх наслідків, аналізу вразливостей та захищеності системи, визначення параметрів порушників, оцінки ризику, прогнозування подій та інцидентів.

Генерація звітів та попереджень означає формування, передачу, відображення чи друк результатів функціонування.

Візуалізація передбачає подання у графічному вигляді даних, що характеризують результати аналізу подій безпеки та стан системи, що захищається, та її елементів.

Функціональність:

- **Агрегація даних:** керування журналами даних; дані збираються з різних джерел: мережеві пристрої та послуги, датчики систем безпеки, сервери, бази даних, додатки; забезпечується консолідація даних із метою пошуку критичних подій.
- **Кореляція:** пошук загальних атрибутів, зв'язування подій у значні кластери. Технологія забезпечує застосування різних технічних прийомів для інтеграції даних із різних джерел перетворення вихідних даних на значну інформацію. Кореляція є типовою функцією підмножини Security Event Management.
- **Оповіщення:** автоматизований аналіз корелюючих подій та генерація сповіщень (тривог) про поточні проблеми. Оповіщення може виводитися на «приладову» панель самої програми, так і бути направлено в інші канали: e-mail, GSM-шлюз і т.п.
- **Засоби відображення** (інформаційні панелі): відображення діаграм, які допомагають ідентифікувати патерни, відмінні від стандартної поведінки.
- **Сумісність (трансформованість):** застосування додатків для автоматизації збору даних, формування звітності для адаптації даних, що

агрегуються, до існуючих процесів управління інформаційною безпекою та аудиту.

– **Зберігання даних:** застосування довгострокового сховища даних в історичному порядку для кореляції даних за часом та забезпечення трансформації. Довготривале зберігання даних є критичним для проведення комп'ютерно-технічних експертиз, оскільки розслідування мережного інциденту навряд чи проводитиметься в момент порушення.

– **Експертний аналіз:** можливість пошуку за безліччю журналів на різних вузлах; може виконуватися у межах програмно-технічної експертизи.

10.3. Аналіз подій SIEM

Перше завдання SIEM – отримати дані від джерела. Це може бути як «активне» джерело, яке вміє передавати дані в SIEM і йому достатньо вказати мережеву адресу приймача, так і «пасивний», до якого SIEM-система повинна звернутися сама.

Отримавши від джерела дані, SIEM-система перетворює їх на одноманітний, придатний для подальшого використання формат – це називається нормалізацією. Порівняємо це з великою компанією людей з різних країн: усі говорять своїми мовами, а SIEM-система всіх слухає і нормалізує, тобто. перекладає все англійською, щоб потім можна було переглянути всю розмову єдиною, зрозумілою мовою.

Далі SIEM-система виконує таксономію, тобто. класифікує вже нормалізовані повідомлення в залежності від їх змісту: яка подія говорить про успішну мережеву комунікацію, яка – про вхід користувача на ПК, а яка – про спрацювання антивіруса. Таким чином, ми отримуємо вже не просто набір записів, а послідовність подій з певним змістом та часом настання. Отже, ми вже можемо зрозуміти, в якій послідовності йшли події і який може бути зв'язок між ними.

Тут у гру входить основний механізм SIEM-систем: кореляція. Кореляція в SIEM – це співвідношення між собою подій, які відповідають тим чи іншим умовам (правилам кореляції). Приклад правила кореляції: якщо на двох і більше ПК протягом 5 хвилин спрацював антивірус, то це може свідчити про вірусну атаку на компанію. Більш складне правило: якщо протягом 24 годин були зафіксовані чиїсь спроби віддалено зайти на сервер, які зрештою увінчалися успіхом, а потім з цього сервера почалося копіювання даних на зовнішній файлообмінник, це може свідчити про те, що зловмисники підібрали пароль до облікового запису, зайшли всередину сервера та крадуть важливі дані. За підсумками спрацьовування правил кореляції у SIEM-системі формується інцидент інформаційної безпеки (у деяких системах, наприклад, у SIEM IBM QRadar інцидент називається Offense). При цьому фахівець з ІБ при роботі з SIEM повинен мати можливість швидкого пошуку по попереднім інцидентам і подіям, що зберігаються в SIEM-системі, на випадок, якщо йому знадобиться будь-які додаткові технічні подробиці для розслідування атаки.

Отже, **основні завдання SIEM-систем** такі:

1. Отримання журналів із різноманітних засобів захисту
2. Нормалізація отриманих даних
3. Таксономія нормалізованих даних
4. Кореляція класифікованих подій
5. Створення інциденту, надання інструментів щодо розслідування
6. Зберігання інформації про події та інциденти протягом тривалого часу (від 6 місяців)
7. Швидкий пошук за даними, що зберігаються в SIEM даних

Крім зазначеного функціоналу, SIEM-системи можуть також оснащуватися додатковими функціями, такими як управління ризиками та вразливістю, інвентаризація IT-активів, побудова звітів та діаграм тощо. Автоматизоване реагування на інцидент також можна налаштувати, для цього використовують системи IRP (Incident Response Platform, платформи реагування на інциденти інформаційної безпеки), які можуть без участі людини, наприклад, заблокувати зламаний обліковий запис або відключити інфікований ПК від мережі.

Підсумовуючи, ми можемо сказати, що системи SIEM необхідні компаніям для роботи з великим потоком різноманітних даних від різних джерел з метою виявлення потенційних інцидентів інформаційної безпеки та своєчасного реагування на них.

Користь від впровадження та застосування SIEM-системи полягає в тому, що вона значно прискорює процес обробки інцидентів ІБ та отримання необхідної інформації про події ІБ: аналітику не потрібно підключатися до кожного засобу захисту інформації, він бачить усі дані в єдиному консолідованому вигляді в одному зручному інтерфейс.

Якщо у компанії відповідно до законодавства є вимоги до зберігання всіх журналів аудиту (тобто логів) засобів захисту за певний часовий період, наприклад, не менше ніж за рік, використання SIEM-систем дозволяє виконати цю вимогу. Таким чином є можливість реалізувати SOC (Security Operations Center, або Центр забезпечення безпеки), ядром якого стане SIEM-система.

Зрозуміло, при впровадженні та налаштуванні SIEM-систем існують очевидні **труднощі** як організаційного, так і технічного характеру: крім купівлі самої SIEM-системи доведеться ще:

– налаштувати всі джерела даних на відправку даних у SIEM;
– створювати правила кореляції;
– усувати причини хибно-позитивних спрацьовувань;
– підтримувати SIEM-систему в актуальному стані;
– оперативно розслідувати інциденти інформаційної безпеки що згенеровані SIEM.

Але це є прийнятним, оскільки забезпечує безпеку даних, а значить – найціннішого, що часом є у компанії.

Перспективи розвитку SIEM-систем

Найбільш перспективними напрямками, які допоможуть SIEM-системам краще виявляти кіберінциденти та запобігати їх наслідкам, експерти назвали:

– розвиток експертизи в галузі управління системою;

– автоматизацію реагування на інциденти;

– розширення можливостей SIEM за рахунок технологій аналізу трафіку, аналізу того, що відбувається на кінцевих вузлах, моніторингу користувачів та сутностей;

– хмарних обчислень як джерела даних та надання SIEM за сервісною (as a service) моделлю.

Серед технологій, що впливають на розвиток SIEM-систем, фахівці відзначили розвиток експертизи в галузі управління системою. Останні 15 років про SIEM прийнято говорити як засіб для збору логів з різних систем і засобів кореляції, а аналіз зібраних масивів даних обмежується мапінгом правил кореляції по матриці MITRE ATT & CK.

Для підвищення якості моніторингу подій безпеки SIEM цього недостатньо, потрібні:

– правила нормалізації;

– способи налаштування джерел;

– пакети з правилами виявлення загроз;

– інструкції з активації джерел;

– опис правил детектування;

– рекомендації про те, що робити, якщо спрацювало правило.

Частка покриття цієї технології (глибина проникнення) становить 50-60%, якість реалізації – середня (3 бали).

Ще один тренд розвитку SIEM-систем – це автоматизація реагування на інциденти. Згідно з опитуванням, проведеним, 25% фахівців з ІБ проводять у SIEM-системі від двох до чотирьох годин щодня. До найбільш трудомістких завдань учасники опитування віднесли роботу з помилковими спрацьовуваннями (доналагодження правил кореляції) та розбір інцидентів: їх відзначили 58% та 52% респондентів відповідно. У 30% фахівців з ІБ багато часу забирають налаштування джерел даних та відстеження їх працездатності. Цей тренд дає поштовх розвитку SIEM-систем в область іншого класу продуктів – SOAR. Частка покриття технології становить 60-70%, а якість реалізації – 3.

Третій тренд пов'язаний з конвергенцією технологій аналізу трафіку (NTA-систем), логів (SIEM) і того, що відбувається на кінцевих вузлах (EDR). Без глибокого аналізу мережі та можливостей EDR моніторинг не буде повним. У найближчі три роки аналіз трафіку розглядатиметься як обов'язкова умова майбутнього SIEM, а аналіз подій на кінцевих вузлах – як функціональна можливість, що доповнює. Покриття технології 60-70%, якість реалізації – 2 бали.

Прагнення отримати на одному екрані єдину картину того, що відбувається в інфраструктурі, сприятиме додаванню до можливостей SIEM інструментів UEBA – поведінкового аналізу користувачів та сутностей (процесів, вузлів

мережі, мережевих активностей). Головна відмінність SIEM від UEBA в тому, що SIEM-система виступає як свого роду конструктор для збору логів, а рішення UEBA будує поведінкові моделі. Алгоритми пошуку та обробки аномалій можуть включати різні методи: статистичний аналіз, машинне навчання(machine learning), глибоке навчання (deep learning) та ін., які підказують оператору, які користувачі та сутності в мережі стали вести себе нетипово і чому ця поведінка для них нетипова. Це четверта технологія, покриття якої оцінюється в 70-80%, а якість реалізації на 4 бали.

П'яте напрямок розвитку SIEM-систем пов'язані з хмарами. Згідно з дослідженням, приблизно дві третини (64%) підприємств планують збільшити витрати на публічні хмарні платформи порівняно з попереднім роком. Такий підхід, з одного боку, змушує вендорів додавати найпопулярніші хмарні сервіси (AWS, Google Cloud Platform, Microsoft Azure) до списку підтримуваних SIEM джерел – за рахунок підключення конекторів до хмар а з іншого, навчитися і самим надавати SIEM за моделлю as a service – за допомогою додавання специфічних для хмарної інфраструктури способів розгортання, конфігурування та диригування SIEM (віртуальних, хмарних аплайнсів). За експертними оцінками, частка покриття цієї технології становить 60-70%, а якість реалізації – 3 бали.

Розділ 11. Механізми безпеки комп'ютерних мереж

11.1. Віртуальні приватні мережі (VPN).
11.2. Протоколи автентифікації RADIUS.
11.3. Протоколи SSL/TLS.

11.1. Віртуальні приватні мережі (VPN)

VPN (англ. Virtual Private Network «Віртуальна приватна мережа») – узагальнена назва технологій, що дозволяють забезпечити одне або кілька мережевих з'єднань поверх іншої мережі, наприклад Інтернет.

Незважаючи на те, що для комунікації використовуються мережі з меншим або невідомим рівнем довіри (наприклад, публічні мережі), рівень довіри до побудованої логічної мережі не залежить від рівня довіри до базових мереж завдяки використанню засобів криптографії (шифрування, автентифікації, інфраструктури відкритих ключів, засобів захисту від повторів і змін повідомлень, що передаються по логічній мережі).

Залежно від застосовуваних протоколів та призначення VPN може забезпечувати з'єднання трьох видів: вузол-вузол, вузол-мережа та мережа-мережа.

Рівні реалізації

Зазвичай VPN розгортають рівнях не вище мережевого, оскільки застосування криптографії цих рівнях дозволяє використовувати у незмінному вигляді транспортні протоколи (такі як TCP, UDP).

Користувачі Microsoft Windows позначають терміном VPN одну з реалізацій віртуальної мережі – **PPTP**, причому використовується часто не для створення приватних мереж.

Найчастіше для створення віртуальної мережі використовується інкапсуляція протоколу **PPP** в будь-який інший протокол – **IP** (такий спосіб використовує реалізація **PPTP** – Point-to-Point Tunneling Protocol) або Ethernet (**PPPoE**) (хоча вони мають відмінності).

Технологія VPN останнім часом використовується не лише для створення власне приватних мереж, а й деякими провайдерами « останньої милі » на пострадянському просторі для надання виходу до Інтернету.

При належному рівні реалізації та використання спеціального програмного забезпечення мережа VPN може забезпечити високий рівень шифрування інформації, що передається.

Структура VPN

VPN складається з двох частин: «внутрішня» (підконтрольна) мережа, яких може бути кілька, і «зовнішня» мережа, через яку проходить інкапсульоване з'єднання (зазвичай використовується Інтернет).

Можливе також підключення до віртуальної мережі окремого комп'ютера.

Підключення віддаленого користувача до VPN здійснюється за допомогою сервера доступу, який підключений як до внутрішньої, так і зовнішньої (загальнодоступної) мережі. При підключенні віддаленого користувача (або під час встановлення з'єднання з іншою захищеною мережею) сервер доступу вимагає проходження процесу ідентифікації, а потім процесу автентифікації. Після успішного проходження обох процесів віддалений користувач (віддалена мережа) наділяється повноваженнями для роботи в мережі, тобто відбувається процес авторизації.

Класифікація VPN

Класифікувати рішення VPN можна за кількома основними параметрами:

За рівнем захищеності використовуваного середовища:

– Захищені. Найпоширеніший варіант віртуальних приватних мереж. З його допомогою можна створити надійну та захищену мережу на основі ненадійної мережі, як правило, Інтернету. Прикладом захищених VPN є: IPSec, OpenVPN та PPTP.

– Довірчі. Використовуються у випадках, коли середовище, що передає, можна вважати надійним і необхідно вирішити лише завдання створення віртуальної підмережі в рамках більшої мережі. Проблеми безпеки стають неактуальними. Прикладами подібних рішень VPN є: Multi-protocol label switching (MPLS) і L2TP (Layer 2 Tunnelling Protocol) (точніше буде сказати, що ці протоколи перекладають завдання безпеки на інші, наприклад L2TP, як правило, використовується в парі з IPSec).

За способом реалізації:

– У вигляді спеціального програмно-апаратного забезпечення. Реалізація мережі VPN здійснюється за допомогою спеціального комплексу програмно-апаратних засобів. Така реалізація забезпечує високу продуктивність і, зазвичай, високий рівень захищеності.

– У вигляді програмного рішення. Використовується персональний комп'ютер із спеціальним програмним забезпеченням, що забезпечує функціональність VPN.

– Інтегроване рішення. Функціональність VPN забезпечує комплекс, що вирішує також завдання фільтрації мережевого трафіку, організації мережевого екрана та забезпечення якості обслуговування.

За призначенням:

– Intranet VPN. Використовується для об'єднання в єдину захищену мережу кількох розподілених філій однієї організації, які обмінюються даними відкритими каналами зв'язку.

– Remote-access VPN. Використовується для створення захищеного каналу між сегментом корпоративної мережі (центральним офісом або філією) та одиночним користувачем, який, працюючи вдома, підключається до корпоративних ресурсів із домашнього комп'ютера, корпоративного ноутбука, смартфона або інтернет-кіоску.

– Extranet VPN. Використовується для мереж, до яких підключаються «зовнішні» користувачі (наприклад, замовники або клієнти). Рівень довіри до

них набагато нижчий, ніж до співробітників компанії, тому потрібне забезпечення спеціальних «рубежів» захисту, які запобігають чи обмежують доступ останніх до особливо цінної, конфіденційної інформації.

– Internet VPN. Використовується провайдерами для надання доступу до інтернету, зазвичай, якщо по одному фізичному каналу підключаються декілька користувачів. Протокол **PPPoE** став стандартом **ADSL** – підключення. **L2TP** був широко поширений у середині 2000-х років у будинкових мережах: на той час внутрішньомережевий трафік не оплачувався, а зовнішній коштував дорого. Це дозволяло контролювати витрати: коли VPN-з'єднання вимкнено, користувач нічого не платить. В даний час (2012) дротовий інтернет – дешевий або безлімітний, а на стороні користувача найчастіше є маршрутизатор, на якому вмикати-вимикати інтернет не так зручно, як на комп'ютері. Тому L2TP-доступ відходить у минуле.

– Client/server VPN. Цей варіант забезпечує захист даних між двома вузлами (не мережами) корпоративної мережі. Особливість цього варіанта в тому, що VPN будується між вузлами, що знаходяться, як правило, в одному сегменті мережі, наприклад, між робочою станцією та сервером. Така необхідність часто виникає у тому випадку, як у однієї фізичної мережі необхідно створити кілька логічних мереж. Наприклад, коли треба розділити трафік між фінансовим департаментом та відділом кадрів, які звертаються до серверів, що знаходяться в одному фізичному сегменті. Цей варіант схожий на технологію VLAN, але замість поділу трафіку використовується його шифрування.

За типом протоколу:

– Існують реалізації віртуальних приватних мереж під TCP/IP, IPX та AppleTalk. Але на сьогоднішній день спостерігається тенденція до загального переходу на протокол TCP/IP, і більшість рішень VPN підтримує саме його. Адресація в ньому найчастіше вибирається відповідно до стандарту RFC5735, з діапазону Приватних мереж TCP/IP.

За рівнем мережевого протоколу:

– За рівнем мережевого протоколу з урахуванням зіставлення з рівнями еталонної мережевої моделі ISO/OSI.

VPN-з'єднання на маршрутизаторах

Зі зростанням популярності VPN-технологій багато користувачів стали активно налаштовувати VPN-з'єднання на маршрутизаторах задля підвищення безпеки в мережі. VPN-з'єднання, налаштоване на маршрутизаторі, шифрує мережевий трафік всіх під'єднаних пристроїв, у тому числі і тих, які не підтримують технології VPN.

Багато маршрутизаторів підтримують VPN-з'єднання та мають вбудований VPN-клієнт. Існують маршрутизатори, для яких потрібне програмне забезпечення з відкритим вихідним кодом, таке як DD-WRT, OpenWrt і Tomato для того, щоб підтримувати протокол OpenVPN.

Вразливості

Використання технології **WebRTC**, яка за замовчуванням включена в кожному браузері, дозволяє третій стороні визначити реальну публічну IP-адресу пристрою, що працює через VPN. Це є прямою загрозою для конфіденційності, оскільки, знаючи справжню IP-адресу користувача, можна однозначно ідентифікувати її в мережі. Для запобігання витоку адреси рекомендується або повністю відключити WebRTC в налаштуваннях браузера, або встановити спеціальний додаток.

VPN вразливі для атаки, яка називається дактилоскопією трафіку веб-сайту. Дуже коротко: це пасивна атака перехоплення; хоча супротивник тільки спостерігає зашифрований трафік з VPN, він все ще може здогадатися, який сайт відвідується, тому що всі веб-сайти мають певні шаблони трафіку. Зміст передачі, як і раніше, приховано, але до якого веб-сайту він підключається, більше не є секретом.

Приклади VPN

–IPSec (IP security) – часто використовується поверх IPv4.

–PPTP (point-to-point tunneling protocol) – розроблявся спільними зусиллями кількох компаній, включаючи Microsoft.

–PPPoE (PPP (Point-to-Point Protocol) over Ethernet)

–L2TP (Layer 2 Tunnelling Protocol) – використовується в продуктах компаній Microsoft та Cisco.

–L2TPv3 (Layer 2 Tunnelling Protocol version 3).

–OpenVPN SSL – VPN з відкритим вихідним кодом, підтримує режими PPP, bridge, point-to-point, multi-client server.

–freelan SSL P2P – VPN з відкритим вихідним кодом.

–Hamachi – програма для створення однорангової VPN-мережі.

–NeoRouter – zeroconf (не потребує налаштування) програма для забезпечення прямого з'єднання комп'ютерів за NAT, є можливість вибрати свій сервер.

Багато великих провайдерів пропонують свої послуги з організації VPN-мереж для бізнес-клієнтів.

OpenVPN

OpenVPN – вільна реалізація технології віртуальної приватної мережі (VPN) з відкритим вихідним кодом для створення зашифрованих каналів типу точка або сервер-клієнти між комп'ютерами. Вона дозволяє встановлювати з'єднання між комп'ютерами, що знаходяться за NAT і мережевим екраном без необхідності зміни їх налаштувань. OpenVPN була створена Джеймсом Йонаном (James Yonan) і поширюється під ліцензією GNU GPL.

Для забезпечення безпеки керуючого каналу та потоку даних OpenVPN використовує бібліотеку OpenSSL. Це дозволяє використовувати весь набір алгоритмів шифрування, доступних у цій бібліотеці. Також може використовуватися пакетна автентифікація HMAC для забезпечення більшої безпеки та апаратне прискорення для покращення продуктивності шифрування. Ця бібліотека використовує OpenSSL, а точніше протоколи SSLv 3/ TLSv 1.2.

OpenVPN використовується в операційних системах Solaris, OpenBSD, FreeBSD, NetBSD, GNU/ Linux, Apple Mac OS X, QNX, Microsoft Windows, Android, iOS.

Автентифікація

OpenVPN пропонує користувачеві кілька видів автентифікації.

– Передвстановлений ключ – найпростіший метод.

– Сертифікатна автентифікація – найбільш гнучкий метод налаштування.

– За допомогою логіну та пароля може використовуватися без створення клієнтського сертифікату (серверний сертифікат все одно потрібен).

Мережа

OpenVPN проводить усі мережеві операції через TCP- або UDP-транспорт. У загальному випадку переважним є UDP з тієї причини, що через тунель проходить трафік мережевого рівня і вище OSI, якщо використовується TUN-з'єднання, або трафік канального рівня і вище, якщо використовується TAP. Це означає, що OpenVPN для клієнта виступає протоколом канального або навіть фізичного рівня, а значить, надійність передачі даних може забезпечуватися вищими за рівнями OSI, якщо це необхідно. Саме тому протокол UDP за своєю концепцією найбільш близький до OpenVPN, тому що він, як і протоколи канального та фізичного рівнів, не забезпечує надійності з'єднання, передаючи цю ініціативу вищим рівням. Якщо ж налаштувати тунель на роботу з TCP, сервер у типовому випадку отримуватиме TCP-сегменти OpenVPN, які містять інші TCP-сегменти від клієнта. Також можлива робота через більшу частину проксі-серверів, включаючи HTTP, SOCKS, через NAT та мережеві фільтри. Сервер може бути налаштований на призначення мережевих установок клієнту. Наприклад: IP-адреса, налаштування маршрутизації та параметри з'єднання. OpenVPN пропонує два різні варіанти мережевих інтерфейсів, використовуючи драйвер TUN/TAP. Можливо створити тунель мережевого рівня, званий TUN, і канального рівня – TAP, здатний передавати Ethernet -трафік. Також можливе використання бібліотеки компресії LZO для стиснення потоку даних. Використовуваний порт 1194 виділено Internet Assigned Numbers Authority для роботи цієї програми. Версія 2.0 дозволяє одночасно керувати кількома тунелями на відміну від версії 1.0, що дозволяла створювати лише 1 тунель на 1 процес.

Використання в OpenVPN стандартних протоколів TCP та UDP дозволяє йому стати альтернативою IPsec у ситуаціях, коли Інтернет-провайдер блокує деякі VPN-протоколи.

11.2. Протоколи автентифікації RADIUS

RADIUS (англ. Remote Authentication in Dial-In User Service) – протокол для реалізації автентифікації, авторизації та збору відомостей про використані ресурси, розроблений для передачі відомостей між центральною платформою та обладнанням. Цей протокол застосовувався для системи тарифікації використаних ресурсів конкретним користувачем/абонентом. Центральна платформа та обладнання Dial-Up доступу (Network Access Server (NAS, не

плутати зі сховищем) із системою автоматизованого обліку послуг (білінгу)), RADIUS використовується як протокол **AAA**:

– англ. Authentication – процес, що дозволяє автентифікувати (перевірити справжність) суб'єкта за його ідентифікаційними даними, наприклад, за логіном (ім'я користувача, номер телефону тощо) та паролем.

– англ. Authorization – процес, що визначає повноваження ідентифікованого суб'єкта на доступ до певних об'єктів або сервісів.

– англ. Accounting – процес, що дозволяє вести збір відомостей (облікових даних) про використані ресурси. Первинними даними (тобто традиційно передаються за протоколом RADIUS) є величини вхідного та вихідного трафіку: в байтах/октетах (з недавніх пір в гігабайтах). Однак протокол передбачає передачу даних будь-якого типу, що реалізується за допомогою **VSA** (**V** endor **S** pecific **A** ttributes).

Протокол RADIUS був розроблений Карлом Рігні (англ. Carl Rigney) у фірмі Livingston Enterprises для їх серверів доступу (Network Access Server) серії PortMaster до мережі інтернет, і пізніше, в 1997, був опублікований як **RFC 2058** і **RFC 2059** (поточні версії **RFC 2865** та **RFC 2866**).

На даний момент існує кілька комерційних і RADIUS-серверів, що вільно розповсюджуються. Вони дещо відрізняються один від одного за своїми можливостями, але більшість підтримує списки користувачів у текстових файлах, **LDAP**, різних баз даних.

Облікові записи користувачів можуть зберігатися в текстових файлах, різних базах даних або зовнішніх серверах.

Часто для віддаленого моніторингу використовується **SNMP**.

Існують проксі-сервери для RADIUS, які спрощують централізоване адміністрування та/або дозволяють реалізувати концепцію інтернет-роумінгу. Вони можуть змінювати вміст RADIUS-пакету на льоту (з метою безпеки або для перетворення між діалектами).

Популярність RADIUS-протоколу багато в чому пояснюється:

– відкритістю до наповнення новою функціональністю при збереженні працездатності зі застарілим обладнанням;

– надзвичайно високою реактивністю при обробці запитів через використання UDP як транспорт пакетів;

– добре паралелізується алгоритмом обробки запитів;

– здатністю функціонувати в кластерних (Cluster) архітектурах (наприклад OpenVMS) і мультипроцесорних (SMP) платформах (DEC Alpha, HP Integrity) – як для підвищення продуктивності, так і для реалізації відмовостійкості.

Існує протокол DIAMETER (поточні версії RFC 3588 та RFC 3589), який покликаний замінити RADIUS, надаючи механізм міграції.

Можливості

Будучи частиною білінгової системи, RADIUS-сервер є інтерфейсом взаємодії з телекомунікаційною системою або сервером (наприклад, маршрутизатором або комутатором) і може реалізовувати для такої системи такі сервіси:

Загальні

– Створення та зберігання облікових записів користувачів (абонентів).

– Керування обліковим записом користувача (абонента) з персонального інтерфейсу (наприклад, веб-кабінету).

– Створення карток доступу (логін або PIN-код) для надання послуг, з деяким лімітом дії (Dial-Up доступу до Інтернету та карткової IP-телефонії).

– Ручне та автоматичне блокування облікового запису абонента після досягнення заданого критерію або ліміту.

– Збір та аналіз статистичної інформації про сесії користувача та всієї системи, що обслуговується (у тому числі CDR).

– Створення звітів з різних статистичних параметрів.

– Створення, друк та відправка рахунків до оплати.

– Автентифікація всіх запитів у RADIUS-сервер з системи, що обслуговується (поле Secret).

Автентифікація

– Перевірка облікових даних користувача (у тому числі шифрованих) на запит системи, що обслуговується.

Авторизація

– Видача стану блокування облікового запису користувача.

– Видача дозволу на ту чи іншу послугу.

– Сортування даних на основі аналізу статистичної інформації (наприклад, динамічна маршрутизація) та видача результату сортування на на запит.

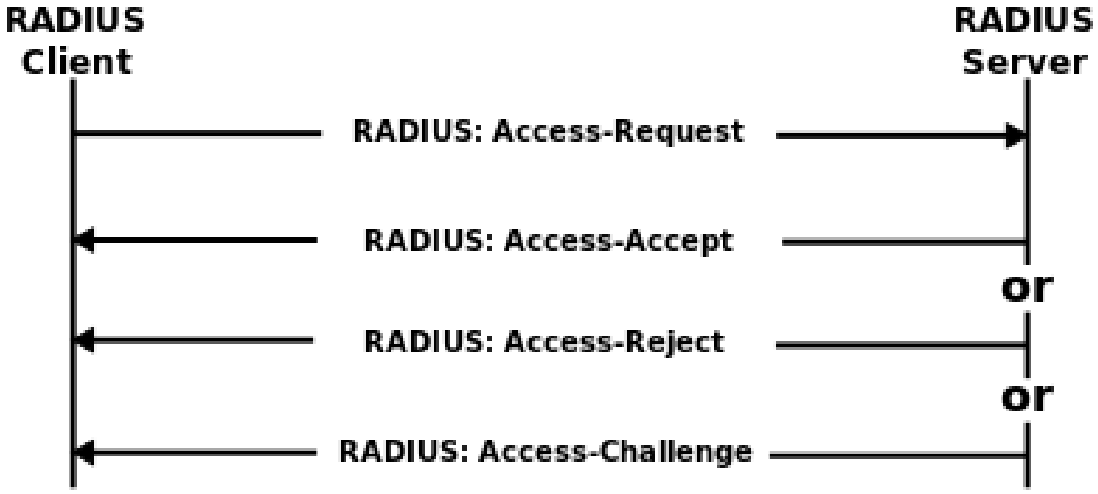


Рисунок 11.1 – Автентифікація та авторизація через RADIUS-сервер

Облік (Accounting)

– Онлайн-облік засобів абонента: повідомлення про початок і кінець сесії з боку системи, що обслуговується.

– Проміжні повідомлення про продовження сесії (Interim-пакети).

– Автоматичне примусове завершення дії сесії на системі, що обслуговується в рамках послуги (packet of disconnection).

– BOOT message – спеціальний пакет, який відправляється телекомунікаційною системою на RADIUS-сервер під час запуску (перезапуску) системи з метою примусового завершення всіх сесій.

В даний час протокол RADIUS використовується для доступу до віртуальних приватних мереж (VPN), точок бездротового (Wi-Fi) доступу, Ethernet-комутаторів, DSL та інших типів мережевого доступу. Завдяки відкритості, простоті впровадження, постійному вдосконаленню протокол RADIUS зараз є фактично стандартом для віддаленої автентифікації.

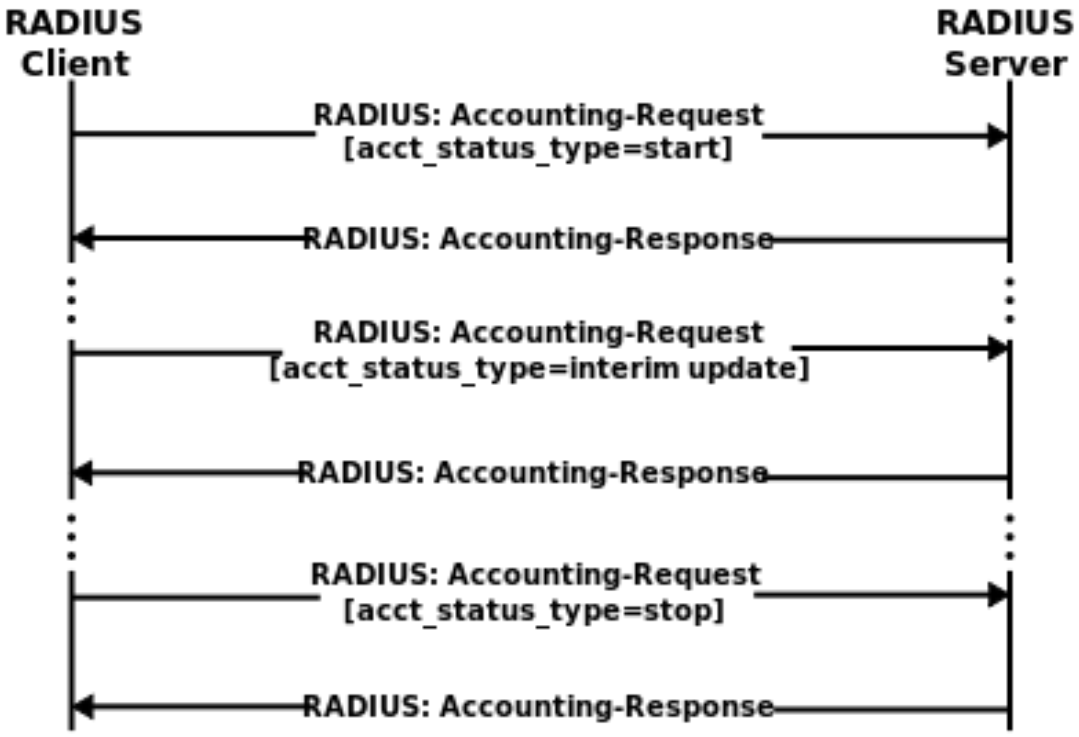


Рисунок 11.2 – Онлайн облік через RADIUS-сервер

Процес автентифікації та авторизації

Для визначення принципу роботи протоколу RADIUS необхідно розглянути наступне.

Ноутбуки та IP-телефон представляють пристрої користувача, з яких необхідно виконати автентифікацію та авторизацію на мережевих серверах доступу (NAS): точці Wi-Fi доступу, маршрутизаторі, VPN-сервері та IP АТС.

RADIUS реалізується у вигляді інтерфейсу між NAS (RADIUS-клієнт) та RADIUS-сервером – програмним забезпеченням, що встановлюється на

комп'ютері (сервері) або іншому спеціалізованому пристрої. Сервер взаємодіє з пристроєм користувача безпосередньо, а лише через мережевий сервер доступу.

Користувач надсилає запит на мережевий сервер для отримання доступу до певного мережевого ресурсу за допомогою сертифікату доступу. Сертифікат надсилається на сервер через мережевий протокол канального рівня (наприклад, PPP у разі комутованого доступу, DSL у разі використання відповідних модемів тощо). NAS, своєю чергою, посилає повідомлення запиту доступу на RADIUS-сервер (RADIUS Access Request). Запит включає сертифікати доступу, представлені у вигляді імені користувача та пароля або сертифікату безпеки, отримані від користувача. Запит може містити додаткові параметри: мережеву адресу пристрою користувача, телефонний номер, інформацію про фізичну адресу, з якою користувач взаємодіє з NAS.

Сервер **перевіряє інформацію на коректність**, використовуючи схеми **автентифікації**:

– **PAP** (Password Authentication Protocol) (RFC 1334) – простий автентифікаційний протокол, який використовується для автентифікації користувача стосовно мережевого сервера доступу (NAS). PAP використовується протоколом PPP. Майже всі сервери доступу підтримують PAP. PAP передає зашифрований пароль через мережу і, отже, при перехопленні трафіку пароль може бути схильний до атаки перебору. Тому PAP зазвичай використовується в тому випадку, коли сервер не підтримує захищені протоколи, такі як CHAP, EAP і т.п.

– **CHAP** (Challenge Handshake Authentication Protocol) (RFC 1994) – широко поширений алгоритм автентифікації, що передбачає передачу не самого пароля користувача, а непрямих відомостей про нього. У разі використання CHAP сервер віддаленого доступу надсилає клієнтові рядок запиту. На основі цього рядка та пароля користувача клієнт обчислює ґеш-код MD5 та передає його серверу. Ґеш-функція є алгоритмом одностороннього (необоротного) шифрування, оскільки значення ґеш-функції для блоку даних легко обчислити, а визначити вихідний блок з ґеш-коду з математичної точки зору неможливо за прийнятний час. Сервер, якому доступний пароль користувача, виконує ті ж обчислення і порівнює результат з ґеш-кодом, отриманим від клієнта. У разі збігу облікові дані клієнта віддаленого доступу вважаються справжніми.

– **MD5** (Message-Digest algorithm 5) (RFC 1321) – широко використовується криптографічна функція з 128 бітовим ґешем. В алгоритмі знайдено низку вразливостей, внаслідок чого Міністерство внутрішньої безпеки США не рекомендує використання MD5 у майбутньому.

– **EAP** (розширюваний протокол автентифікації) (RFC 3748) дозволяє перевіряти справжність при підключеннях віддаленого доступу за допомогою різних механізмів автентифікації. Точна схема автентифікації узгоджується клієнтом віддаленого доступу та сервером, що виконує автентифікацію (ним може бути сервер віддаленого доступу або RADIUS сервер). За промовчанням у маршрутизацію та віддалений доступ включена підтримка протоколів EAP-TLS та MD5-Challenge (MD5-завдання). Підключення інших модулів EAP до сервера,

що використовує маршрутизацію та віддалений доступ, забезпечує підтримку інших методів EAP. Протокол EAP дозволяє вести вільний діалог між клієнтом віддаленого доступу та системою автентифікації. Такий діалог складається із запитів системи автентифікації на необхідну їй інформацію та відповідей клієнта віддаленого доступу. Наприклад, Коли протокол EAP використовується з генераторами кодів доступу, сервер, що виконує автентифікацію, може окремо запитувати у клієнта віддаленого доступу ім'я користувача, ідентифікатор і код доступу. Після відповіді на кожен запит клієнт віддаленого доступу проходить певний рівень перевірки автентичності. Коли на всі запити будуть отримані відповіді, перевірка справжності клієнта віддаленого доступу успішно завершується.

Схеми автентифікації, що використовують протокол EAP, називаються типами EAP. Для успішної автентифікації клієнт віддаленого доступу та сервер, що виконує автентифікацію, повинні підтримувати один і той же тип EAP.

Тепер повернемося до RADIUS сервера, який перевіряє інформацію, отриману від NAS. Сервер перевіряє ідентичність користувача, а також коректність додаткової інформації, яка може міститися у запиті: мережева адреса пристрою користувача, телефонний номер, стан рахунку, його привілеї при доступі до запитуваного мережевого ресурсу. За результатами перевірки RADIUS сервер надсилає NAS один із трьох типів відгуків:

– **Access-Reject** показує, що цей запит користувача неправильний. За бажання сервер може включити текстове повідомлення в Access-Reject, яке може бути передано клієнтом користувачеві. Ніякі інші атрибути (крім Proxy-State) не дозволені у Access-Reject.

– **Access-Challenge**. Запит додаткової інформації від користувача, наприклад, другий пароль, пін-код, номер картки тощо. Цей відгук також використовується для більш повного автентифікаційного діалогу, де захисний тунель виконується між пристроєм користувача та сервером RADIUS, так що сертифікати доступу ховаються від NAS.

– **Access Accept**. Користувачеві дозволено доступ. Оскільки користувач автентифікований, RADIUS сервер перевіряє авторизацію на використання запитаних користувачем ресурсів. Наприклад, користувачеві може бути дозволений доступ через бездротову мережу, але заборонено доступ до мережі VPN.

Стандарти

Визначений у:

– RFC 2865 Remote Authentication Dial In User Service (RADIUS).
– RFC 2866 Облік RADIUS.

Також має відношення до:

– RFC 2548 Специфічні атрибути RADIUS Microsoft від постачальника.
– RFC 2607 З’єднання проксі та впровадження політики в роумінгу.
– RFC 2618 MIB клієнта автентифікації RADIUS.
– RFC 2619 Сервер автентифікації RADIUS MIB.
– RFC 2620 RADIUS Accounting Client MIB.
– RFC 2621 RADIUS обліковий сервер MIB.

– RFC 2809 Реалізація примусового тунелювання L2TP через RADIUS.

– RFC 2867 Модифікації обліку RADIUS для підтримки тунельного протоколу.

– RFC 2868 Атрибути RADIUS для підтримки тунельного протоколу.

– RFC 2869 Розширення RADIUS.

– Вимоги до серверів доступу до мережі RFC 2882: розширені практики RADIUS.

– RFC 3162 RADIUS і IPv6.

– RFC 3575 IANA, міркування щодо RADIUS.

– RFC 3576 Розширення динамічної авторизації для RADIUS.

– RFC 4672 MIB клієнта динамічної авторизації RADIUS.

– RFC 4673 MIB сервера динамічної авторизації RADIUS.

– RFC 3579 Підтримка RADIUS для EAP.

– RFC 3580 Інструкції з використання RADIUS IEEE 802.1X.

– RFC 4014 Підпараметр атрибутів RADIUS для параметра інформації агента ретрансляції DHCP.

DIAMETER

DIAMETER – сеансовий протокол, створений, частково, для подолання деяких обмежень протоколу RADIUS. Забезпечує взаємодію між клієнтами з метою автентифікації, авторизації та обліку різних сервісів (AAA, англ. authentication, authorization, accounting). Є основним протоколом архітектури IMS.

В основі протоколу DIAMETER лежить концепція створення базового протоколу з можливістю його розширення для надання сервісів AAA з появою нових технологій доступу.

Опис наведено у стандартах: RFC 6733 (Diameter Base Protocol), RFC 3589 (Diameter Command Codes for 3GPP), RFC 4006 (Diameter Credit-Control Application).

Порівняння з протоколом RADIUS

Назва DIAMETER – гра слів, що відображає перевагу нового протоколу над попередником RADIUS (діаметр – подвоєний радіус). Diameter не має зворотної сумісності до RADIUS, але надає механізми міграції. Серед відмінностей між протоколами особливо вирізняють:

– Підтримка транспортних протоколів з гарантованою доставкою (TCP або SCTP замість UDP). TCP транспорт для RADIUS ще у процесі стандартизації IETF.

– Захист даних на мережевому та транспортному рівнях (IPsec або TLS). Transport Layer Security for RADIUS ще в процесі стандартизації IETF.

– Підтримка переходу з RADIUS, незважаючи на те, що Diameter не повністю сумісний з RADIUS.

– Збільшений адресний простір для пар атрибут-значення (AVP) та ідентифікаторів (32 bit замість 8 bit).

– Модель клієнт-сервер. Як виняток, тим не менш, підтримуються деякі повідомлення, що ініціюються сервером.

– Підтримка stateful та stateless моделей використання.

– Динамічне виявлення вузлів (використовуючи DNS SRV та NAPTR).

– Можливість узгодження функціональних можливостей вузлів.

– Підтримка механізмів надійної доставки на рівні додатків, описані механізми відмовостійкості та state machine (RFC 3539).

– Повідомлення про помилки.

– Поліпшена підтримка мобільності.

– Поліпшена розширюваність; можливість використання команд і атрибутів користувача.

11.3. Протоколи SSL/TLS

SSL (Secure Sockets Layer) та **TLS (Transport Level Security)** – криптографічні протоколи, що забезпечують захищену передачу даних у комп'ютерній мережі. Вони широко використовуються у веб-браузерах, а також під час роботи з електронною поштою, обміну миттєвими повідомленнями та в IP-телефонії. Існує **SSL 1.0, 2.0 і 3.0**, на **підставі протоколу SSL 3.0 було розроблено та прийнято TLS 1.0.** Його також часто називають **SSL 3.1**. **SSL 1.0, 2.0, 3.0 і TLS**

Версія SSL 1.0 ніколи не була оприлюднена. Версія 2.0 була випущена в лютому 1995 року, але містила багато недоліків безпеки, які призвели до розробки SSL 3.0 версії.

Як тільки різні компанії (Microsoft) почали робити спроби розробки власних безпечних протоколів транспортування, IETF вирішило втрутитися і визначити стандарт протоколу шифрування. Згодом, за підтримки безлічі компаній, на підставі протоколу **SSL 3.0** було розроблено та прийнято стандарт RFC, який отримав ім'я **TLS 1.0**. Його також часто називають **SSL 3.1**.

Хоча TLS і SSL мають суттєві відмінності у реалізації, розробники зазвичай помічають лише деякі з них, а кінцеві користувачі їх зовсім не розрізняють. Проте **TLS 1.0 та SSL 3.0 несумісні**. Значна відмінність у тому, що **TLS вимагає певні алгоритми шифрування, які SSL не підтримує**. Таким чином, TLS сервер повинен "відкотитися" (downgrade) до SSL 3.0 для роботи з клієнтами, що використовують SSL 3.0.

З'єднання, захищене протоколом TLS, має одну або кілька наступних **властивостей**:

– Безпека: симетричне шифрування захищає передану інформацію від прочитання сторонніми особами.

– Автентифікація: "особистість" учасника з'єднання можна перевірити за допомогою асиметричного шифрування.

– Цілісність: кожне повідомлення містить код (**Message Authentication Code, MAC**), за допомогою якого можна перевірити, що дані не були змінені або втрачені в процесі передачі.

Так як більшість протоколів зв'язку можуть бути використані як з TLS/SSL, так і без нього, при встановленні з'єднання необхідно явно вказати серверу, чи клієнт встановлюватиме TLS. Один спосіб досягти цього – використовувати порт, яким з'єднання завжди встановлюється з допомогою TLS (наприклад, 443 для HTTPS). Інший спосіб – використовувати спеціальну команду серверу від клієнта переключити з'єднання на TLS (наприклад, STARTTLS для протоколів електронної пошти).

Версії SSL/TLS

SSL 1.0, 2.0 і 3.0

Протокол SSL був спочатку розроблений компанією Netscape Communications. Версія 1.0 ніколи не була оприлюднена. Версії 2.0 була випущена в лютому 1995 року, але містила багато недоліків безпеки, які призвели до розробки SSL версії 3.0. **SSL версії 3.0, випущений у 1996 році, послужив основою для створення протоколу TLS 1.0,** стандарту протоколу Internet Engineering Task Force (IETF), який вперше був визначений у RFC 2246 у січні 1999 року. Visa, Master Card, American Expressта багато інших організацій мають ліцензію на використання протоколу SSL для комерційних цілей у мережі Інтернет. Тим самим SSL розширюється відповідно до проекту про підтримку прямої та зворотної сумісності та переговорів між з'єднаннями в одноранговій мережі. З березня 2011 року, згідно з RFC 6176, TLS-клієнти не повинні використовувати протокол SSL 2.0 при запиті підключення до сервера, і сервери повинні відхиляти такі запити.

TLS 1.0

TLS 1.0 вперше був визначений в RFC 2246 у січні 1999 як оновлення версії SSL 3.0. Як зазначено в RFC, «відмінності між цим протоколом і SSL 3.0 не є критичними, але вони значні для появи несумісності при взаємодії TLS 1.0 і SSL 3.0». TLS 1.0 дійсно включає засоби, за допомогою яких реалізація підключення TLS до SSL 3.0 послабить безпеку.

TLS 1.1

TLS 1.1 презентували в RFC 4346 у квітні 2006 року. Це оновлення TLS версії 1.0. Значні зміни в цій версії включають:

– додано захист від атак, що використовують режим зчеплення блоків шифротексту (Cipher Block Chaining);

- неявний вектор ініціалізації (IV) був замінений на явний IV;
- було проведено зміну обробки помилок;

– введено підтримку IANA реєстрації параметрів.

TLS 1.2

TLS 1.2 був анонсований у RFC 5246 у серпні 2008 року. Він ґрунтується на раніше запропонованій версії TLS 1.1.

TLS 1.3

TLS 1.3 був визнаний стандартом у RFC 8446 у серпні 2018 року.

SSL

Надамо опис протоколу SSL**.**

SSL спочатку розроблений компанією Netscape для додавання протоколу – HTTPS до свого веб-браузера Netscape Navigator, тому що компанія вважала, що безпечне з'єднання між клієнтом і сервером в першу чергу послужить успіхом розвитку Інтернету як інструменту бізнесу.

Через неможливість гарантувати безпеку мережі, через яку передається інформація найкращим способом захистити її було вибрано шифрування та дешифрування на кінцях з'єднання, що встановлюється відповідно. Netscape могли б вбудувати цей підхід безпосередньо у свій браузер, але це не надало б єдиного рішення, яке інші програми могли б використовувати. Потрібно отримати більш загальний, незалежний від застосування підхід.

У результаті Netscape розробив протокол SSL, що працює поверх TCP, а також надає TCP-подібний інтерфейс для додатків вищого рівня. Теоретично, однією з переваг SSL для розробників була можливість замінити всі традиційні TCP виклики на нові SSL виклики. Специфічні деталі того, як SSL шифрує та дешифрує дані були відносно прозорі.

Опис протоколу SSL

Протокол SSL розміщується між двома протоколами: **протоколом, який використовує програма-клієнт** (HTTP, FTP, LDAP, TELNET тощо) і **транспортним протоколом TCP/IP.** SSL захищає дані, виступаючи як фільтр для обох сторін і передає їх далі на транспортний рівень.

Роботу протоколу можна розділити на два рівні:

– Шар протоколу підтвердження підключення (Handshake Protocol Layer).

– Шар протоколу запису.

Перший шар: протокол підтвердження підключення

Перший шар, у свою чергу, складається з трьох підпротоколів:

– Протокол підтвердження підключення (Handshake Protocol).

– Протокол зміни параметрів шифру (Cipher Spec Protocol).

– Попереджувальний протокол (Alert Protocol).

Протокол підтвердження підключення здійснює ланцюжок обміну даними, що в свою чергу починає автентифікацію сторін і погоджує шифрування, ґешування та стиснення. Наступний етап – автентифікація учасників, що здійснюється також протоколом підтвердження підключення.

Протокол зміни параметрів шифру використовується зміни даних ключа (keying material) – інформації, що використовується створення ключів шифрування. Протокол складається з одного повідомлення, в якому сервер говорить, що відправник хоче змінити набір ключів.

Попереджувальний протокол містить повідомлення, яке показує сторонам зміну статусу або повідомляє про можливу помилку. Зазвичай попередження надсилається тоді, коли підключення закрито та отримано неправильне повідомлення, повідомлення неможливо розшифрувати або користувач скасовує операцію.

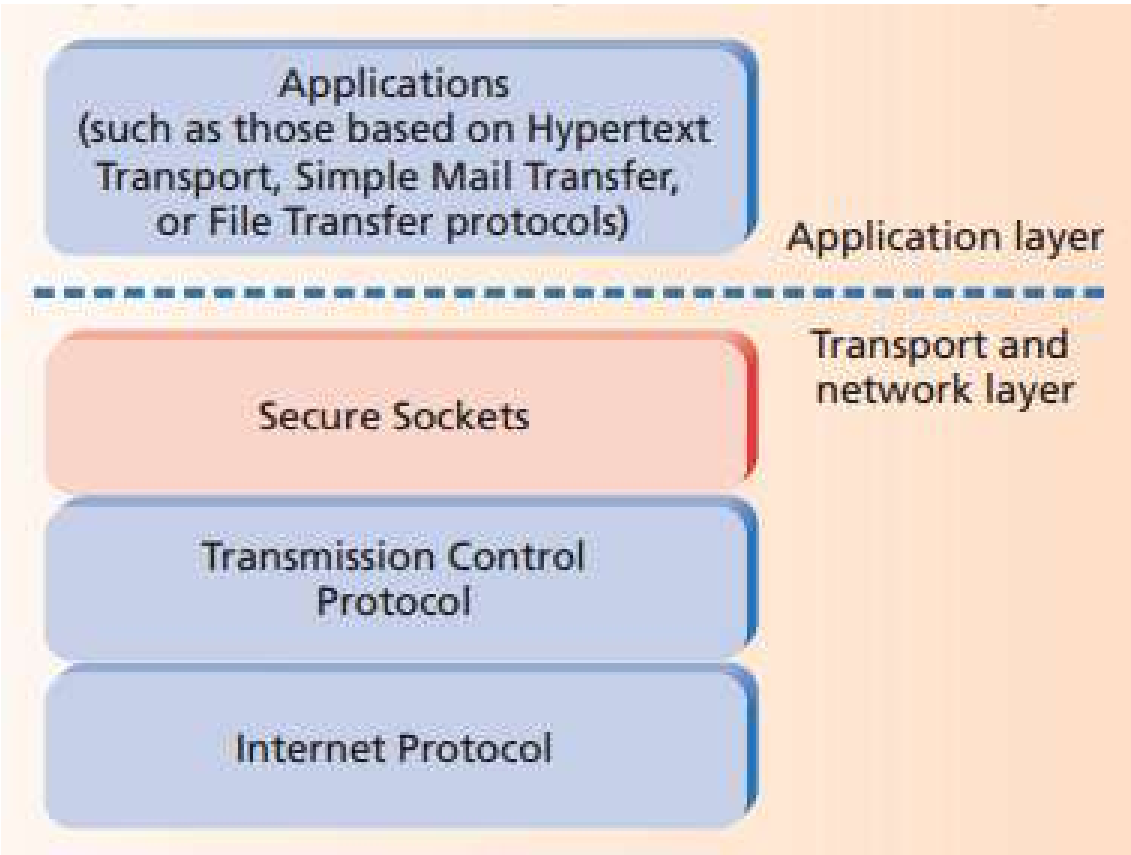


Рисунок 11.3 – Опис протоколу SSL

Другий шар: Протокол запису

Протокол запису (Record Layer) – це рівневий протокол. На кожному рівні повідомлення включають поля для довжини, опису та перевірки. Протокол запису приймає повідомлення, які потрібно передати, фрагментує дані в керовані блоки, розумно стискає дані, застосовуючи MAC (message authentication code), шифрує та передає результат. Отримані дані він розшифровує, перевіряє, розпаковує, збирає та доставляє до верхніх рівнів клієнта.

Існує чотири протоколи запису:

– Протокол рукостискання (handshake protocol).
– Протокол тривоги (alert protocol).
– Протокол зміни шифру (the change cipher spec protocol).
– Протокол програми (application data protocol);

Принцип роботи SSL

Принцип роботи SSL і двох фаз: **фаза рукостискання** і **фаза передачі**. Під час фази рукостискання клієнт та сервер використовують шифрування відкритим ключем для того, щоб визначити параметри секретного ключа, що використовується клієнтом та сервером для шифрування під час фази передачі даних.

Клієнт ініціює рукостискання посилаючи "hello"-повідомлення серверу. Таке повідомлення містить перелік алгоритмів симетричного шифрування (cipher specs), що підтримуються клієнтом. Сервер відповідає схожим

"hello"-повідомленням, вибравши при цьому найбільш підходящий алгоритм шифрування з отриманого списку. Далі сервер відправляє сертифікат, який містить його **публічний ключ**.

Сертифікат – це набір даних, що підтверджує справжність. Підтверджена третя сторона, відома як **центр сертифікації** (CA), генерує сертифікат та перевіряє його справжність. Щоб отримати сертифікат, сервер повинен використовувати безпечні канали для відправлення свого публічного ключа до центру сертифікації. Він генерує **сертифікат, який містить**:

– власний ID;

– ID сервера;

– публічний ключ сервера та іншу інформацію.

А **також центр сертифікації створює відбиток (digest) сертифікату**, який є контрольною сумою. Далі **центр сертифікації створює підпис сертифікату (certificate signature**), який формується шляхом шифрування відбитка сертифікату приватним ключем центру сертифікації.

Для **перевірки сертифікату сервера** клієнт використовує публічний ключ центру сертифікації для розшифровування підпису.

Потім клієнт самостійно зчитує відбиток сертифікату сервера та звіряє з розшифрованим. Якщо вони не збігаються, то сертифікат було підроблено. Природно, для розшифровки підпису клієнт повинен мати публічний ключ центру авторизації. Тому клієнт зберігає список публічних ключів підтверджених центрів сертифікації. За фактом, багато браузерних програм мають подібний список, що знаходиться безпосередньо в їх коді.

Коли клієнт встановив справжність сервера (сервер також може запросити сертифікат клієнта), сервер використовує шифрування відкритим ключем для визначення **секретного ключа** для обміну інформацією.

Фаза рукостискання завершується відправкою "finished"-повідомлень, як тільки обидві сторони готові розпочати використання секретного ключа. Починається фаза передачі даних, під час якої кожна сторона розбиває вихідні повідомлення фрагменти і прикріплює до них коди авторизації повідомлень **MAC** (message authentication code). **Код авторизації повідомлення** – це зашифрований відбиток, обчислений на основі вмісту повідомлень. З міркувань безпеки, він не збігається із секретним ключем та обчислюється разом із секретним ключем на стадії рукостискання. Для отримання повноцінного пакета SSL кожна зі сторін об'єднує дані фрагмента, код авторизації повідомлення, заголовки повідомлення і шифрують з використанням секретного. При отриманні пакета кожна зі сторін розшифровує його і звіряє отриманий код авторизації повідомлення зі своїм. Якщо вони не збігаються, то пакет було підроблено.

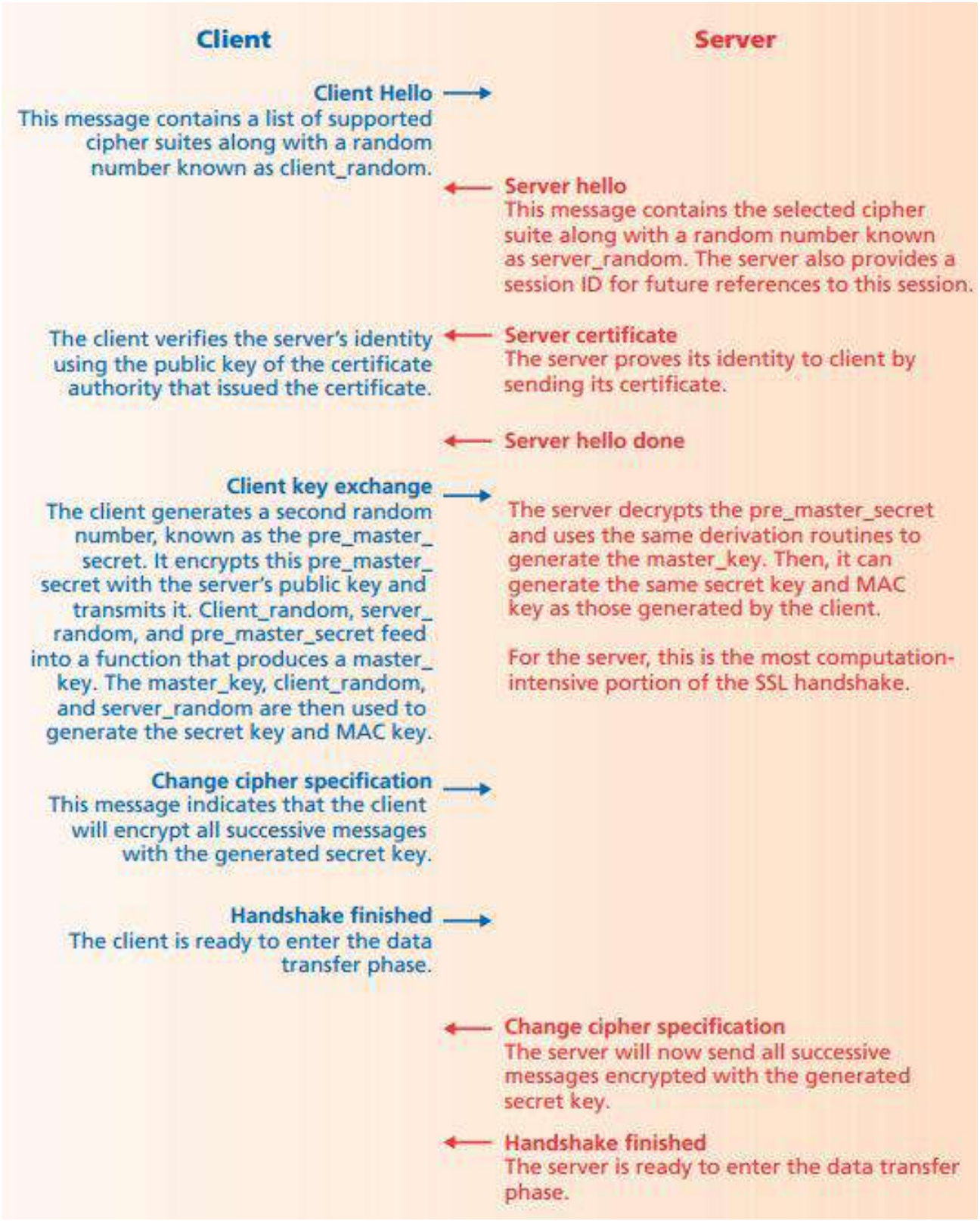


Рисунок 11.4 – Принцип роботи SSL

Цифрові сертифікати

Протокол SSL використовує сертифікати для перевірки з'єднання. Сертифікати розміщені на безпечному сервері та використовуються для шифрування даних та ідентифікації веб-сайту.

Способи отримання SSL-сертифікату:

– Використовувати сертифікат, виданий центром сертифікації (Certification authority).

– Використати самопідписаний сертифікат.

– Використовувати "порожній" сертифікат.

Самопідписаний сертифікат – сертифікат, створений самим користувачем, – у цьому випадку видавець сертифікату збігається з власником сертифікату.

«Порожній» сертифікат – сертифікат, що містить фіктивну інформацію, що використовується як тимчасова для налаштування SSL і перевірки його функціональності в даному середовищі.

Ґешування

Ґеш-значення є ідентифікатором повідомлення, його розмір менший за розмір оригінального повідомлення. Найвідомішими ґеш-алгоритмами є **MD5 (Message Digest 5)**, який створює 128-бітове ґеш-значення, **SHA-1 (Standard Hash Algorithm)**, що створює 160-бітове ґеш-значення, **SHA-2** та **SHA-3**. Результат роботи алгоритму ґешування – значення, яке використовується для перевірки цілісності передачі даних.

Шифрування

Існує два основні способи шифрування даних:

– симетричний ключ (загальний секретний ключ);

– асиметричний ключ (відкритий ключ).

Відкритий ключ

Суть асиметричного шифрування у тому, що використовується пара ключів. Один з них використовується як відкритий (як правило, він публікується в самому сертифікаті власника), другий ключ називається секретним – він тримається в таємниці і ніколи нікому не відкривається. Обидва ключі працюють у парі: один використовується для запуску протилежних функцій іншого ключа. Якщо відкритий ключ використовується для того, щоб зашифрувати дані, розшифрувати їх можна тільки секретним ключем і навпаки. Такий взаємозв'язок дозволяє робити дві важливі речі.

Будь-який користувач може отримати відкритий ключ за призначенням і використовувати його для шифрування даних, які може розшифрувати тільки користувач, який володіє секретним ключем. (RSA)

Якщо заголовок шифрує дані, використовуючи секретний ключ, кожен може розшифрувати дані, використовуючи відповідний відкритий ключ. Саме це є основою цифрових підписів. (DSA)

RSA – найпоширеніший алгоритм шифрування з використанням асиметричних ключів.

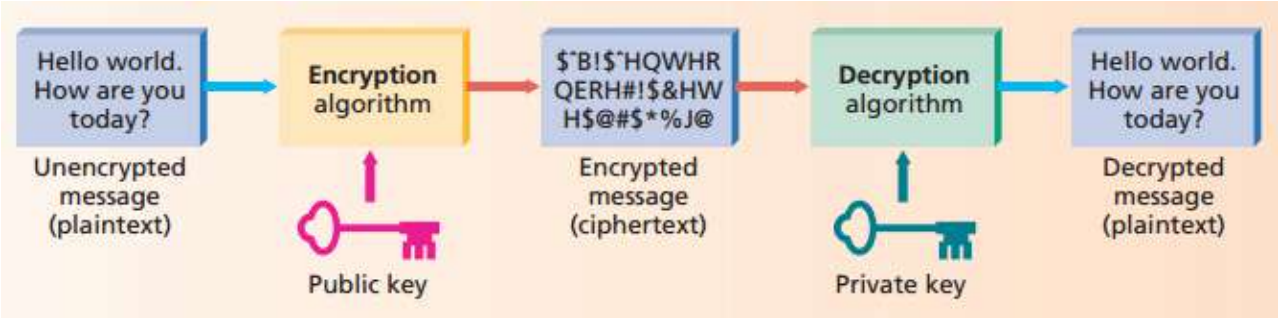


Рисунок 11.5 – Шифрування з використанням асиметричних (несиметричних, з відкритим ключем) алгоритмів

Секретний ключ

При шифруванні секретним ключем використовується той самий ключ для шифрованих даних. Якщо сторони хочуть обмінятися зашифрованими повідомленнями в безпечному режимі, то обидві сторони повинні мати однакові симетричні ключі. Такий тип шифрування використовується великого обсягу даних. Зазвичай використовуються алгоритми DES, 3-DES, RC2, RC4 та AES.

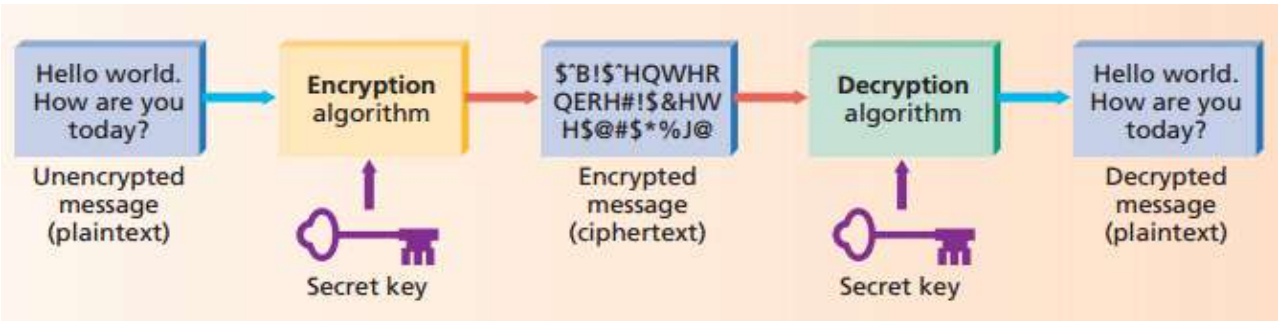


Рисунок 11.6 – Шифрування з використанням симетричних алгоритмів

Комбінований підхід

Алгоритми симетричного шифрування часто включають встановлену кількість добавок та зсувів. Такі алгоритми часто використовують ключ для допомоги при бітових маніпуляціях або для того, щоб дані, що шифруються, стали більш випадковими. Іншими словами, при збільшенні розміру секретного ключа може збільшитися випадковість даних, що шифруються, але не обов'язково зросте складність обчислень при розшифровці. Однак, шифрування відкритим ключем використовує ключ як експоненту, тому значне збільшення ключа сильно збільшує кількість обчислень, потрібних для шифрування/дешифрування даних.

Таким чином, хоча алгоритми шифрування відкритим ключем не стикаються з проблемою розподілу, з якою стикаються алгоритми шифрування секретним ключем, вони потребують значно більше обчислювальної потужності.

Для використання сильних сторін обох типів алгоритмів протоколи безпеки зазвичай використовують шифрування відкритим ключем передачі секретних ключів. Як тільки секретний ключ доставлено, починається передача даних з використанням симетричного шифрування.

Існує ще один підхід, який використовує відкритий ключ як угоду, а не спосіб доставки секретного ключа іншим. Обидві сторони обмінюються публічними ключами та незалежно генерують секретний ключ.

Найпоширенішою формою такої угоди є протокол **Діффі-Хеллмана**. Хоча SSL підтримує протокол Діффі-Хеллмана, більшість транзакцій SSL не використовують його. Натомість використовується алгоритм RSA, який вирішує проблему розподілу секретних ключів.

Застосування

При проектуванні програм **SSL** реалізується "під" будь-яким іншим протоколом прикладного рівня, таким як **HTTP, FTP, SMTP, NNTP і XMPP**, таким чином забезпечуючи "прозорість" його використання.

Історично SSL був використаний насамперед з надійними транспортними протоколами, такими як **Transmission Control Protocol (TCP)**. Проте він також був реалізований з датаграмними транспортними протоколами, такими як **User Datagram Protocol (UDP)** та **Datagram Control Protocol (DCCP)**, використання якого було стандартизовано, що призвело до появи терміну **Datagram Transport Layer Security (DTLS)**.

Веб-сайти

Часте використання протоколу SSL призвело до формування протоколу **HTTPS (Hypertext Transfer Protocol Secure),** який підтримує шифрування. Дані, які передаються за протоколом HTTPS, «упаковуються» в криптографічний протокол SSL або TLS, забезпечуючи тим самим захист цих даних. Такий спосіб захисту широко використовується у світі Веб для додатків, у яких важлива безпека з'єднання, наприклад, у платіжних системах. На відміну від HTTP, для HTTPS за замовчуванням використовується TCP-порт 443.

Використання та реалізація

Спочатку віртуальні приватні мережі (VPN) на основі SSL розроблялися як додаткова та альтернативна технологія віддаленого доступу на основі IPsec VPN. Однак такі фактори, як достатня надійність та дешевизна, зробили цю технологію привабливою для організації VPN. Також SSL набув широкого застосування в електронній пошті.

Найбільш поширена реалізація SSL – криптографічний пакет з відкритим вихідним кодом OpenSSL, заснований на **SSLeay**, написаної Еріком Янгом. Остання версія OpenSSL підтримує SSLv3. Пакет призначений для створення та управління різного роду сертифікатами. Також до його складу входить бібліотека підтримки SSL різними програмами. Бібліотека використовується, наприклад, модулем SSL у поширеному HTTP-сервері Apache.

Специфікація протоколу записів SSL

Формат заголовка записів SSL

Всі дані в SSL пересилаються у вигляді записів (рекордів) – об'єктів, які складаються із заголовка та деякої кількості даних. Кожен заголовок рекорду містить 2 або 3 байти коду довжини. Якщо старший біт у першому байті коду довжини рекорду дорівнює 1, тоді рекорд немає заповнювача і повна довжина заголовка дорівнює 2 байтам, інакше рекорд містить заповнювач, і повна довжина заголовка дорівнює 3 байтам. У разі довгого (3 байти) заголовка другий за старшинством біт першого байти має спеціальне значення. Якщо він дорівнює 0 – рекорд є інформаційним, якщо він дорівнює 1 – рекорд є security escape. Код довжини рекорду не включає число байт заголовка. Для 2-байтового заголовка його довжина обчислюється так:

RECORD-LENGTH = ((byte[0] & 0x7F) << 8) | byte[1];

Тут byte[0] перший отриманий байт, а byte[1] другий отриманий байт.

Для 3-байтового заголовка довжина рекорду обчислюється так:

RECORD-LENGTH = ((byte[0] & 0x3F) <<8) | byte[1];

IS-ESCAPE = (byte[0] & 0x40)! = 0;

PADDING = byte [2];

Значення **PADDING** специфікує кількість байтів, доданих відправником до вихідного рекорду. Дані заповнювача використовуються для того, щоб зробити довжину рекорду кратною розміру блоку шифру. Відправник додає **PADDING** після наявних даних, а потім шифрує все це, так як довжина цього масиву кратна розміру блоку використовуваного шифру. Оскільки відомий обсяг даних, що передаються, заголовок повідомлення може бути сформований з урахуванням обсягу **PADDING**. Отримувач повідомлення дешифрує все поле даних і отримує вихідну інформацію, потім обчислює справжнє значення **RECORD-LENGTH**, при цьому **PADDING** з поля дані видаляється.

Формат інформаційних записів SSL

Частина даних рекорду SSL складається з трьох компонентів:

1. **MAC-DATA[MAC-SIZE]**
2. **ACTUAL-DATA[N]**
3. **PADDING-DATA[PADDING]**

Де:

– **MAC-DATA** – код автентифікації повідомлення;

– **MAC-SIZE** – функція алгоритму обчислення ґеш-суми, що використовується;

– **ACTUAL-DATA** – реально передані дані або поле даних повідомлення;

– **PADDING-DATA** – дані **PADDING** (при блоковому шифруванні);

MAC-DATA = **HASH** [**SECRET**, **ACTUAL-DATA**, **PADDING-DATA**, **SEQUENCE-NUMBER**]

Тут **SECRET** передається ґеш-функції першим, потім слідує **ACTUAL-DATA** і **PADDING-DATA**, за якими передається **SEQUENCE-NUMBER** – порядковий номер.

Значення **SECRET** залежить від того, хто надсилає повідомлення. Якщо це робить клієнт, **SECRET** дорівнює **CLIENT-WRITE-KEY**. Якщо клієнт отримує повідомлення, **SECRET** дорівнює **CLIENT-READ-KEY**.

Порядковий номер є 32-бітовим кодом, який передається ґеш-функції у вигляді 4 байт, використовуючи мережевий порядок передачі «від старшого до молодшого». Порядковий номер – лічильник для сервера чи клієнта. Для кожного напряму передачі використовується пара лічильників – для відправника та для одержувача; щоразу, коли надсилається повідомлення, лічильник збільшує своє значення на 1.

Отримувач повідомлення використовує очікуване значення порядкового номера передачі **MAC** (тип ґеш-функції визначається параметром **CIPHER-CHOICE**). Обчислене значення **MAC-DATA** має збігатися з переданим значенням. Якщо порівняння не пройшло, повідомлення вважається пошкодженим, що призводить до виникнення помилки, яка спричиняє закриття з'єднання.

Остаточна перевірка відповідності виконується, коли використовується блоковий шифр. Обсяг даних у повідомленні (**RECORD-LENGTH**) повинен бути кратний розміру блоку шифру. Якщо ця умова не виконана, повідомлення вважається пошкодженим, що призводить до розриву з'єднання.

Для 2-байтового заголовка максимальна довжина повідомлення дорівнює 32767 байтів, для 3-байтового 16383 байтів. Повідомлення протоколу діалогу SSL повинні відповідати одиночним рекордам протоколу SSL, а повідомлення прикладного протоколу можуть займати кілька рекордів SSL.

Протокол діалогу SSL

Протокол діалогу SSL містить дві основні фази.

Фаза 1

Перша фаза використовується встановлення конфіденційного каналу комунікацій. Ця фаза ініціалізує з'єднання, коли обидва партнери обмінюються повідомленнями "hello". Клієнт надсилає повідомлення **CLIENT-HELLO**. Сервер отримує це повідомлення, обробляє його та посилає у відповідь повідомлення **SERVER-HELLO**.

У цей момент сервер і клієнт мають достатньо інформації, щоб знати, чи потрібен новий **master key.** Якщо ключ не потрібен, сервер і клієнт переходять у фазу 2.

Коли виникає необхідність створення нового **master key**, повідомлення сервера **SERVER-HELLO** вже містить достатньо даних для того, щоб клієнт міг згенерувати **master key**. Ці дані включають підписаний сертифікат сервера, список базових шифрів та ідентифікатор з'єднання (випадкове число, згенероване сервером, яке використовується протягом усієї сесії). Після генерації клієнтом **master key** він посилає серверу повідомлення **CLIENT-MASTER-KEY** або повідомлення про помилку, коли клієнт і сервер не можуть узгодити базовий шифр.

Після визначення **master key** сервер надсилає клієнту повідомлення **SERVER-VERIFY**, яке автентифікує сервер.

Фаза 2

Фаза 2 називається фазою автентифікації. Оскільки сервер вже автентифіковано першої фазі, то другої фазі здійснюється автентифікація клієнта. Сервер надсилає запит клієнту, і якщо клієнт має необхідну інформацію – він надсилає позитивний відгук, якщо ж ні – повідомлення про помилку. Коли один партнер виконав автентифікацію іншого партнера, він надсилає повідомлення **finished**. У разі клієнта повідомлення **CLIENT-FINISHED** містить зашифровану форму ідентифікатора **CONNECTION-ID**, яку повинен верифікувати сервер. Якщо вірифікація була невдалою, сервер надсилає повідомлення **ERROR**.

Коли один із партнерів надіслав повідомлення **finished –** він повинен приймати повідомлення до тих пір, поки не отримає повідомлення **finished** від іншого партнера, і тільки коли обидва партнери надіслали та отримали повідомлення **finished**, протокол діалогу SSL закінчить свою роботу. З цього моменту починає роботу прикладний протокол.

Типовий протокол обміну повідомленнями

Нижче наведено кілька варіантів обміну повідомленнями в рамках протоколу діалогу SSL. Клієнт – **C**, сервер – **S.** "{smth}key" означає що "smth" зашифровано за допомогою ключа.

Таблиця 11.1 – За відсутності ідентифікатора сесії

Client-hello	C ® S:	challenge, cipher_specs
Server-hello	S ® C:	connection-id,server_certificate,cipher_specs
Client-master-key	C ® S:	{master_key}server_public_key
Client-finish	C ® S:	{connection-id}client_write_key
Server-verify	S ® C:	{challenge}server_write_key
Server-finish	S ® C:	{new_session_id}server_write_key

Таблиця 11.2 – Ідентифікатор сесії знайдено клієнтом та сервером

Client-hello	C ® S:	challenge, session_id, cipher_specs
Server-hello	S ® C:	connection-id, session_id_hit
Client-finish	C ® S:	{connection-id}client_write_key
Server-verify	S ® C:	{challenge}server_write_key
Server-finish	S ® C:	{session_id}server_write_key

Таблиця 11.3 – Використаний ідентифікатор сесії та автентифікація клієнта

Client-hello	C ® S:	challenge, session_id, cipher_specs
Server-hello	S ® C:	connection-id, session_id_hit
Client-finish	C ® S:	{connection-id}client_write_key
Server-verify	S ® C:	{challenge}server_write_key
Request-certificate	S ® C:	{auth_type,challenge'}server_write_key
Client-certificate	C ® S:	{cert_type,client_cert, response_data}client_write_key

Server-finish	S ® C:	{new_session_id}server_write_key

Автентифікація та обмін ключами

SSL підтримує 3 типи автентифікації:

–автентифікація обох сторін (клієнт-сервер),

–автентифікація сервера з неавтентифікованим клієнтом,

–повна анонімність.

Зазвичай для автентифікації використовуються алгоритми: **RSA, DSA, ECDSA.**

Якщо сервер автентифікований, його повідомлення про сертифікацію має забезпечити правильний сертифікаційний ланцюжок, що веде до прийнятного центру сертифікації. Простіше кажучи, автентифікований сервер має надати допустимий сертифікат клієнту. Кожна сторона відповідає за перевірку того, що сертифікат іншої сторони ще не закінчився і не було скасовано. Щоразу, коли сервер автентифікується, канал стійкий (безпечний) до спроби перехоплення даних між веб-сервером і браузером, але повністю анонімна сесія за своєю суттю вразлива до такої атаки. Анонімний сервер не може автентифікувати клієнта.

Головна мета процесу обміну ключами – створення секрету клієнта (pre_master_secret), відомого тільки клієнту і серверу.

Секрет (pre_master_secret) використовується для створення загального секрету (master_secret).

Загальний секрет необхідний для того, щоб створити повідомлення для перевірки сертифікату, ключів шифрування, секрету MAC (message authentication code) та повідомлення "finished".

Відсилаючи повідомлення "finished", сторони вказують, що вони знають вірний секрет (pre_master_secret).

Анонімний обмін ключами

Повністю анонімна сесія може бути встановлена під час використання алгоритму RSA або Діффі-Хеллмана для створення ключів обміну. У разі використання RSA клієнт шифрує секрет (pre_master_secret) за допомогою відкритого ключа несертифікованого сервера. Відкритий ключ клієнт дізнається із повідомлення обміну ключами від сервера. Результат надсилається у повідомленні обміну ключами від клієнта. Оскільки перехоплювач не знає закритого ключа сервера, йому неможливо розшифрувати секрет (pre_master_secret). У разі використання алгоритму Діффі-Хеллмана відкриті параметри сервера містяться в повідомленні обміну ключами від сервера, і клієнту надсилають у повідомленні обміну ключами. Перехоплювач, який знає приватних значень, зможе знайти секрет (pre_master_secret).

Автентифікація та обмін ключами під час використання RSA

У цьому випадку обмін ключами та автентифікація сервера може бути скомбінована. Відкритий ключ також може міститись у сертифікаті сервера або може бути використаний тимчасовий ключ RSA, який надсилається у повідомленні обміну ключами від сервера. Коли використовується тимчасовий ключ RSA, повідомлення обміну підписуються сервером RSA або сертифікат

DSS. Сигнатура містить поточне значення повідомлення Client_Hello.random, таким чином, старі сигнатури та старі часові ключі не можуть повторюватися. Сервер може використовувати тимчасовий ключ RSA лише один раз для створення сесії. Після перевірки сертифікату сервера клієнт шифрує секрет (pre_master_secret) з допомогою відкритого ключа сервера. Після успішного декодування секрету (pre_master_secret) створюється повідомлення "finished", тим самим сервер демонструє, що він знає приватний ключ, який відповідає сертифікату сервера.

Коли RSA використовується для обміну ключами, для автентифікації клієнта використовується повідомлення для перевірки сертифікату клієнта. Клієнт підписується значенням, обчисленим з master_secret та всіх попередніх повідомлень протоколу рукостискання. Ці повідомлення рукостискання містять сертифікат сервера, який ставить у відповідність сигнатурі сервера повідомлення Server_Hello.random, якому ставить у відповідність сигнатуру поточному повідомленню рукостискання.

Автентифікація та обмін ключами під час використання протоколу Діффі-Хеллмана

У цьому випадку сервер може також підтримувати алгоритм Діффі-Хеллмана, що містить конкретні параметри, або може використовувати повідомлення обміну ключами від сервера для посилення набору тимчасових параметрів, підписаних сертифікатами DSS або RSA. Тимчасові параметри ґешуються з повідомленням hello.random перед підписанням, щоб зловмисник не зміг зробити повторення старих параметрів. У будь-якому випадку, клієнт може перевірити сертифікат або сигнатуру для впевненості, що параметри належать серверу.

Якщо клієнт має сертифікат, що містить параметри алгоритму Diffie-Hellman, то сертифікат також містить інформацію, потрібну для того, щоб завершити обмін ключами. У цьому випадку клієнт і сервер повинні будуть згенерувати однакові Diffie-Hellman результати (pre_master_secret) щоразу, коли вони встановлюють з'єднання. Для того, щоб запобігти збереженню секрету (pre_master_secret) в пам'яті комп'ютера на час довше, ніж необхідно, секрет повинен бути переведений в загальний секрет (master_secret) настільки швидко, наскільки це можливо. Параметри клієнта повинні бути сумісні з тими, що підтримує сервер для того, щоб працював обмін ключами.

Відновлення сесії

Творці SSL знали, що алгоритми шифрування відкритим ключем обчислювально складні, і клієнт, що створює кілька нових з'єднань до одного і того ж сервера протягом короткого проміжку часу може навантажити сервер, що призведе до помітних тимчасових затримок відповіді. Однак, якщо клієнт і сервер вже встановили з'єднання, йому відповідатиме унікальний ідентифікатор сесії, що дозволяє посилатися на нього і використовувати такий же секретний ключ при наступних з'єднаннях в рамках деякого часового відрізка. Безумовно, такий підхід привносить певний ризик у безпеку з'єднання. Тому, якщо

необхідно, клієнт може створити новий ідентифікатор і секретний ключ для даної сесії. Microsoft Internet Explorer, наприклад, роблять цю операцію кожні 2 хвилини.



Рисунок 11.7 – Відновлення сесії

Адміністрація

Обслуговування сертифікатів та ключів

Якщо клієнт планує звернутися до сервера, який вимагає клієнтської автентифікації, він повинен зберігати свій сертифікат та пов'язаний із ним приватний ключ. Сервер повинен зберігати свій сертифікат і пов'язаний з ним приватний ключ.

Сховище ідентифікаторів сесій

Клієнт та сервер зобов'язані зберігати ідентифікатори сесій та пов'язані з ними секретні ключі для використання під час відновлення з'єднання.

Протокол TLS

Принцип роботи TLS

Протокол TLS поділяється на два шари:

– TLS Record.

– TLS Handshake.

Підтвердження зв'язку (TLS Handshake)

1. Клієнт надсилає повідомлення **ClientHello**, що вказує версію SSL або TLS і методи шифрування, що підтримуються клієнтом (англ. CipherSuite). Це повідомлення містить випадкове число (набір байт), яке використовується в наступних обчисленнях. Протокол також дозволяє вказати методи стиснення даних, що підтримуються клієнтом.
2. Сервер відповідає повідомленням **ServerHello**, яке містить метод шифрування, вибраний сервером зі списку, запропонованого клієнтом, а також ідентифікатор сесії та ще одне випадкове число. Також сервер надсилає свій цифровий сертифікат. Якщо сервер потрібен сертифікат для автентифікації клієнта, на цьому кроці він може надіслати клієнту запит такого сертифікату.
3. Клієнт перевіряє сертифікат сервера.
4. Клієнт відправляє випадкове число, яке клієнт та сервер використовують для шифрування наступних повідомлень. Сам рядок із байт шифрується публічним ключем сервера.
5. Якщо сервер вимагає від клієнта сертифікат, клієнт надсилає набір байт, зашифрований його секретним ключем, і свій цифровий сертифікат, або оповіщення про відсутність сертифікату.
6. Сервер перевіряє сертифікат клієнта.
7. Клієнт та сервер надсилають одне одному повідомлення **ChangeCipherSpec**, оголошуючи про зміну режиму передачі даних із незахищеного на захищений.
8. Клієнт відправляє повідомлення **Finished**, зашифроване секретним ключем, і таким чином завершує підтвердження зв'язку зі свого боку.
9. Аналогічні дії здійснює сервер.
10. Протягом цієї сесії клієнт та сервер можуть обмінюватися повідомленнями, зашифрованими секретним ключем.

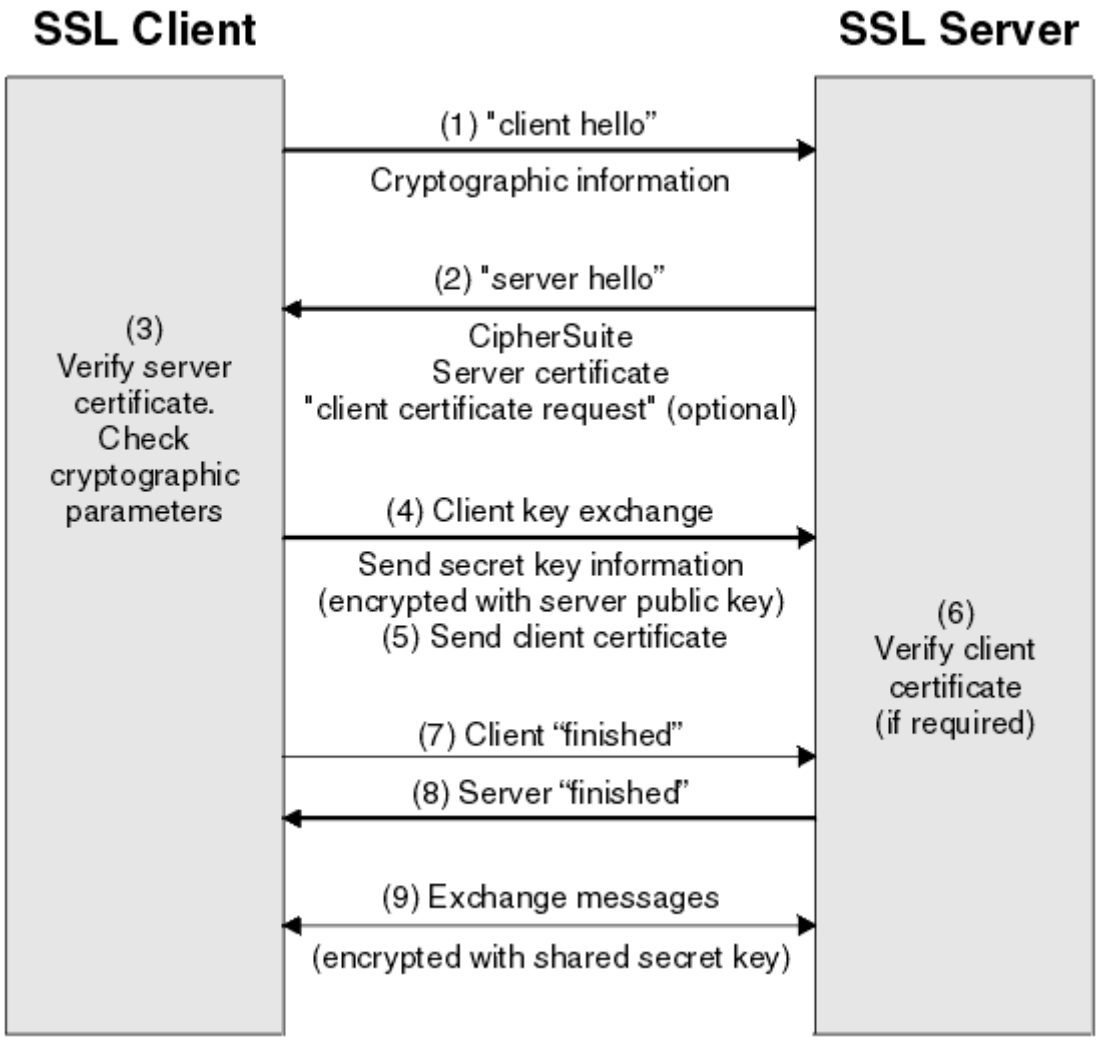


Рисунок 11.8 – Підтвердження зв'язку (handshake)

Відновлення сесії

1. Клієнт надсилає повідомлення **ClientHello за** допомогою ID сесії, яку потрібно відновити.

2. Сервер перевіряє, чи має він у кеші відповідний ідентифікатор. Якщо є і сервер здатний відновити сесію, він надсилає клієнтові повідомлення **ServerHello** з тим самим ID сесії. Якщо ні, сервер генерує новий ID сесії та виконує процедуру handshake з клієнтом.

3. Клієнт і сервер обмінюються повідомленнями **ChangeCipherSpec**, а потім **Finished**.

4. Передача даних захищеним каналом відновлюється.

Протокол запису (TLS Record)

Цей шар захищає дані за допомогою ключів, отриманих при підтвердженні зв'язку, та перевіряє цілісність та джерело вхідних повідомлень. Він виконує такі функції:

– Розбиття вихідних повідомлень на блоки потрібного розміру та "склеювання" вхідних повідомлень.

– Стиснення вихідних повідомлень та розпакування вхідних (використовується не завжди).

– Застосування коду автентифікації до вихідних повідомлень та перевірку вхідних за допомогою MAC.

– Шифрування вихідних повідомлень та дешифрування вхідних повідомлень.

Після обробки протоколом TLS Record зашифровані дані передаються на TCP для передачі.

Склад запису

– Content type: тип повідомлення – підтвердження зв'язку (22), звичайне повідомлення (23) або оповіщення (21).

– Version: версія SSL/TLS.

– Length: довжина частини повідомлення, що залишилася.

– Payload: власне зашифровані дані.

– MAC: код автентифікації.

– Padding: "відступ" для отримання потрібного розміру повідомлення.

Byte	+0	+1	+2	+3
0	Content type			
1..4	Version		Length	
5..n	*Payload*			
n..m	MAC			
m..p	Padding (block ciphers only)			

Рисунок 11.9 – Склад запису

Цифрові сертифікати (стандарт X.509)

– Зручний спосіб показати, що хтось володіє публічним ключем.

– Випускаються центрами сертифікації (**Certificate Authority, CA**): GlobalSign, Comodo та ін.

– **PKI (public key infrastructure)** – механізм, що регулює поширення та використання сертифікатів (включаючи створення, відгук та автентифікацію).

– Список довірених CA підтримується програмою (у браузерів свої списки).

– Сертифікати підписуються іншими сертифікатами, що підвищує надійність.

– Сертифікат може бути відкликаний. Система підтримує список таких сертифікатів (**Certificate Revocation List, CRL**). На стороні CA список оновлюється кожні кілька годин.

Отримання сертифікату

1. Користувач генерує ключ і надсилає запит серверу CA.
2. CA відповідає повідомленням зі своїм сертифікатом.
3. Користувач збирає дані, необхідні для видавання сертифікату (email, відбиток ключа тощо).
4. Користувач надсилає дані до CA, зашифрувавши їх публічним ключем CA.
5. CA перевіряє отримані дані та надсилає сертифікат користувачу.

Структура сертифікату

– Власне сертифікат:
  - Версія.
  - Серійний номер.
  - Емітент (той, хто випустив сертифікат).
  - Суб'єкт.
  - Публічний ключ суб'єкта.
  - Період дії.
  - Додаткові поля.
– Алгоритм підпису сертифікату.
– Значення підпису сертифікату.

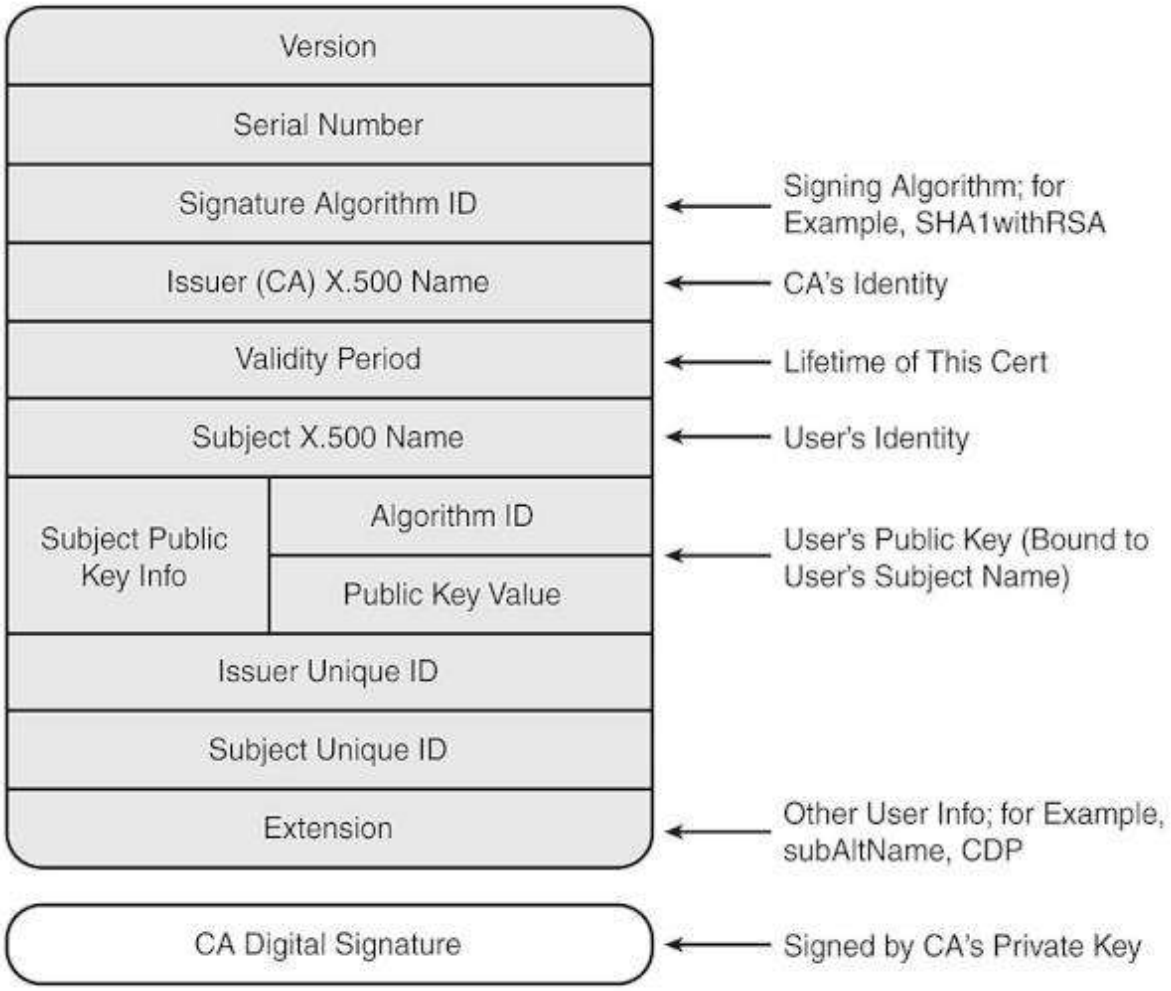


Рисунок 11.10 – Структура сертифікату X.509

Заходи безпеки в TLS

– Захист від downgrade-атаки – зниження версії протоколу до попередньої (менш захищеної) версії або менш надійного алгоритму шифрування.

– Нумерація послідовних записів програми та використання порядкового номера в коді автентифікації повідомлення (MAC).

– Використання ключа в ідентифікаторі повідомлення (тільки власник ключа може створити код автентифікації повідомлення).

– Повідомлення, яким закінчується підтвердження зв'язку («Finished»), містить ґеш всіх handshake-повідомлень, надісланих обома сторонами, що дозволяє перевірити автентичність вибраних параметрів TLS-з'єднання.

– Псевдовипадкова функція ділить подані їй на вхід дані навпіл, застосовує до половин різні ґеш-алгоритми (MD5 і SHA-1), а потім XOR'іт результати для отримання MAC. Це підвищує безпеку у випадку, якщо в одному з алгоритмів виявиться вразливість.

Ключові відмінності SSL та TLS

– Автентифікація повідомлень: в TLS використовується HMAC, що працює з будь-якою ґеш-функцією (а не тільки з MD5 або SHA, як у SSL).

– Генерація ключа: в TLS під час створення ключа використовується псевдовипадкова функція стандарту HMAC; в SSL – RSA, Diffie-Hellman або Fortezza / DMS.

– Перевірка сертифікату: SSL перевірка вимагає передачі складної послідовності повідомлень; у TLS інформація про перевірку повністю передається у повідомленнях під час handshake.

– Методи шифрування: SSL підтримує лише алгоритми RSA, Diffie-Hellman та Fortezza/DMS. У TLS відмовилися від підтримки Fortezza/DMS, але можливе додавання нових методів шифрування в наступних версіях.

Види можливих атак

– Атака за словником.
– Атака відображенням.
– Атака протоколу рукостискання.
– Зламування SSL-з'єднань усередині ЦОД.
– BEAST атака.
– Розкриття шифрів.
– Атака «зловмисник посередині».
– THC-SSL-DOS.
– SSLstrip.

Розділ 12. Проектування, створення, супровід комплексних систем захисту інформації (КСЗІ)

12.1. Дослідження середовищ функціонування ІС – середовища користувачів, обчислювальної системи, фізичного середовища, інформаційного середовища та побудова моделі загроз.

12.2. Проведення аудиту інформаційної безпеки (ІБ) та визначення її рівня на основі звіту з аудиту ризиків ІБ.

12.3. Вибір методів та засобів забезпечення необхідного рівня ІБ.

12.1. Дослідження середовищ функціонування інформаційної системи (ІС) – середовища користувачів, обчислювальної системи, фізичного середовища, інформаційного середовища та побудова моделі загроз

Розгляд даного питання зробимо, спираючись на поради (рекомендації) щодо створення **комплексних систем захисту інформації (КСЗІ)** в **інформаційно-телекомунікаційних системах (ІТС)**, які використовуються для надання послуг доступу до мережі Інтернет від Державної служби спеціального зв'язку та захисту інформації України, розроблених на основі **НД ТЗІ 3.7-003-05** «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі») (https://cip.gov.ua/ua/news/poradi-rekomendaciyi-shodo-stvorennya-kszi-v-its-yaki-vikoristovuyutsya-dlya-nadannya-poslug-dostupu-do-merezhi-internet)

Комплексна система захисту інформації (КСЗІ) – сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в ІТС.

До складу КСЗІ входять заходи та засоби, які реалізують методи, механізми захисту інформації від несанкціонованих дій та несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм, використання комп'ютерних вірусів та ін;

Для організації робіт зі створення КСЗІ в ІТС **створюється служба захисту інформації, порядок створення, завдання, функції, структура та повноваження якої визначено в НД 1.4-001-2000**.

Комплекс засобів захисту (КЗЗ) – сукупність програмно-апаратних засобів, які забезпечують реалізацію політики безпеки інформації.

Етапи створення КСЗІ

Дозволяється виключати окремі етапи робіт або поєднувати декілька етапів, а також включати нові етапи робіт. За необхідністю дозволяється змінювати послідовність виконання окремих етапів – виконувати одночасно

декілька етапів робіт, окремі етапи виконувати до завершення попередніх і т.п., якщо це не призводить до зниження якості робіт і не суперечить цілям їх виконання.

1 Формування загальних вимог до КСЗІ в ІТС

1.2 Обстеження середовищ функціонування ІТС

1.2.1 Під час виконання цих робіт ІТС розглядається як організаційно-технічна система, яка поєднує:

– обчислювальну систему;

– фізичне середовище;

– середовище користувачів;

– оброблювану інформацію і технологію її обробки (далі – середовища функціонування ІТС).

1.2.2 Метою обстеження є підготовка засадничих даних для формування вимог до КСЗІ у вигляді опису кожного середовища функціонування ІТС та виявлення в ньому елементів, які безпосередньо чи опосередковано можуть впливати на безпеку інформації, виявлення взаємного впливу елементів різних середовищ, документування результатів обстеження для використання на наступних етапах робіт.

Слід враховувати, що середовища функціонування є множинами, що перетинаються, окремі їхні елементи можуть входити одночасно до різних середовищ і мати в них різні якості. Наприклад, програмне забезпечення може розглядатись обчислювальною системою як об’єкт-процес, а в інформаційному середовищі – як пасивний об’єкт КС.

1.2.3 Обстеження виконується, коли розроблена концепція ІТС (основні принципи і підходи побудови), визначені основні завдання і характеристики ІТС, функціональних комплексів ІТС та існує варіант(и) їх реалізації.

1.2.4 **При обстеженні обчислювальної системи** ІТС повинні бути проаналізовані й описані:

– загальна структурна схема і склад (перелік і склад обладнання, технічних і програмних засобів, їхні зв'язки, особливості конфігурації, архітектури й топології, програмні і програмно-апаратні засоби захисту інформації, взаємне розміщення засобів тощо);

– види і характеристики каналів зв'язку;

– особливості взаємодії окремих компонентів, їх взаємний вплив один на одного;

– можливі обмеження щодо використання засобів та ін.

Мають бути виявлені компоненти обчислювальної системи, які містять і які не містять засобів і механізмів захисту інформації, потенційні можливості цих засобів і механізмів, їхні властивості і характеристики, в тому числі ті, що встановлюються за умовчанням та ін.

Метою такого аналізу є надання загального уявлення про наявність потенційних можливостей щодо забезпечення захисту інформації, виявлення компонентів ІТС, які вимагають підвищених вимог до захисту інформації і впровадження додаткових заходів захисту.

1.2.5 **При обстеженні інформаційного середовища** аналізу підлягає вся інформація, що обробляється, а також зберігається в ІТС (дані і програмне забезпечення). Під час аналізу інформація повинна бути класифікована за режимом доступу, за правовим режимом, визначені й описані види (в термінах об'єктів КС) її представлення в ІТС.

Для кожного виду інформації і типу об'єкта, в якому вона міститься, ставляться у відповідність властивості захищеності інформації (конфіденційність, цілісність, доступність) чи КС (спостережність), яким вони повинні задовольняти.

Аналіз технології обробки інформації повинен виявити особливості обігу електронних документів, мають бути визначені й описані інформаційні потоки і середовища, через які вони передаються, джерела утворення потоків та місця їх призначення, принципи та методи керування інформаційними потоками, складені структурні схеми потоків. Фіксуються види носіїв інформації та порядок їх використання під час функціонування ІТС.

Для кожного структурного елемента схеми інформаційних потоків фіксуються склад інформаційних об'єктів, режим доступу до них, можливий вплив на нього (елементу) елементів середовища користувачів, фізичного середовища з точки зору збереження властивостей інформації.

1.2.6 **При обстеженні фізичного середовища** здійснюється аналіз взаємного розміщення засобів обробки інформації ІТС на об'єктах інформаційної діяльності, комунікацій, систем життєзабезпечення і зв'язку, а також режим функціонування цих об'єктів.

Порядок проведення обстеження повинен відповідати ДСТУ 3391.

Аналізу підлягають такі **характеристики фізичного середовища**:

– територіальне розміщення компонентів ІТС (генеральний план, ситуаційний план);

– наявність охорони території та перепускний режим;

– наявність категорійованих приміщень, в яких мають розміщуватися компоненти ІТС;

– режим доступу до компонентів фізичного середовища ІТС;

– вплив чинників навколишнього середовища, захищеність від засобів технічної розвідки;

– наявність елементів комунікацій, систем життєзабезпечення і зв'язку, що мають вихід за межі контрольованої зони;

– наявність та технічні характеристики систем заземлення;

– умови зберігання магнітних, оптико-магнітних, паперових та інших носіїв інформації;

– наявність проектної та експлуатаційної документації на компоненти фізичного середовища.

1.2.7 **При обстеженні середовища користувачів** здійснюється аналіз:

– функціонального та кількісного складу користувачів, їхніх функціональних обов'язків та рівня кваліфікації;

– повноважень користувачів щодо допуску до відомостей, які обробляються в ІТС, доступу до ІТС та її окремих компонентів;

– повноважень користувачів щодо управління КСЗІ;

– рівня можливостей різних категорій користувачів, що надаються (можуть бути доступними) їм засобами ІТС.

– наявності СЗІ в ІТС.

1.2.8 Результати обстеження середовищ функціонування ІТС оформлюються у вигляді акту і включаються, у разі необхідності, до відповідних розділів плану захисту інформації в ІТС (далі – План захисту), який розробляється згідно з НД ТЗІ 1.4-001.

1.2.9 За результатами обстеження середовищ функціонування ІТС затверджується перелік об'єктів захисту (з урахуванням рекомендацій НД ТЗІ 1.4-001, НД ТЗІ 2.5-007, НД ТЗІ 2.5-008, НД ТЗІ 2.5-010 щодо класифікації об'єктів), а також визначаються потенційні загрози для інформації і розробляються **модель загроз** та **модель порушника**. **Побудова моделей** здійснюється відповідно до положень **НД ТЗІ 1.1-002, НД ТЗІ 1.4-001** та **НД ТЗІ 1.6-003**. **Модель загроз для інформації** та **модель порушника** рекомендується оформляти у вигляді окремих документів (або поєднаних в один документ) Плану захисту.

2 Розробка політики безпеки інформації в ІТС

2.1 На цьому етапі здійснюється вибір основних рішень з протидії всім суттєвим загрозам, формування загальних вимог, правил, обмежень, рекомендацій і т.п., які регламентують використання захищених технологій обробки інформації в ІТС, окремих заходів і засобів захисту інформації, діяльність користувачів всіх категорій;

2.2 Політика безпеки може розроблятись для ІТС в цілому або, якщо мають місце особливості функціонування окремих компонентів КСЗІ, для окремої компоненти, для окремої функціональної задачі, для окремої технології обробки інформації тощо.

2.3 Політика безпеки розробляється згідно з положеннями НД ТЗІ 1.1-002-99 та рекомендаціями НД ТЗІ 1.4-001-2000.

3 Розробка технічного завдання на створення КСЗІ

3.1 ТЗ на створення КСЗІ в ІТС є засадним організаційно-технічним документом, який визначає вимоги із захисту оброблюваної в ІТС інформації, порядок створення КСЗІ, порядок проведення всіх видів випробувань КСЗІ та введення її в експлуатацію в складі ІТС.

3.3 Для оформлення ТЗ на КСЗІ можуть бути використані такі варіанти:

– у вигляді окремого розділу ТЗ на створення ІТС;

– у вигляді окремого (часткового) ТЗ.

3.4 Перший варіант рекомендується застосовувати для вперше створюваних ІТС. Другий варіант рекомендується застосовувати у випадку модернізації КСЗІ, модернізації діючих ІТС, а також для ІТС, які вже мають затверджене ТЗ на створення, в якому не міститься окремого розділу із захисту інформації.

Вимоги в частині захисту від НСД мають бути викладені відповідно до НД ТЗІ 2.5-004-99 Згідно з цим документом в процесі оцінки захищеності ІТС розглядаються вимоги двох видів: вимоги до функцій (послуг) забезпечення безпеки і вимоги до рівня гарантій. Відповідно, в ТЗ на КСЗІ повинні бути зазначені вимоги обох видів.

3.7 Для будь-якого варіанту розроблення та оформлення ТЗ на КСЗІ його зміст, порядок погодження та затвердження повинен відповідати НД ТЗІ 3.7-001-99 та ГОСТ 34.602.

4 Розробка проекту КСЗІ

4.1.1 Проект КСЗІ розробляється на підставі та у відповідності до ТЗ на створення ІТС (доповнення до нього, окремого ТЗ на створення КСЗІ).

4.1.2 Під час розробки проекту КСЗІ обґрунтовуються і приймаються проектні рішення, які дають змогу реалізувати вимоги ТЗ, забезпечити сумісність і взаємодію різних заходів і способів захисту інформації.

4.1.3 Проект КСЗІ виконується на таких стадіях створення ІТС: ескізний проект, технічний проект, робочий проект.

Можливо вилучати етап “Ескізний проект КСЗІ”, а також поєднувати етапи “Технічний проект КСЗІ” і “Робочий проект КСЗІ” в один етап “Техноробочий проект КСЗІ”.

4.1.4 Для всіх стадій розробки проекту КСЗІ склад документації визначається ТЗ на КСЗІ, види та зміст – ГОСТ 34.201, НД ТЗІ 2.5-004-99. Документація на програмні засоби виконується згідно з комплексом стандартів ЄСПД, на технічні засоби – згідно з комплексом стандартів ЄСКД.

4.2 Ескізний проект КСЗІ

4.2.1 На цьому етапі здійснюється розробка попередніх проектних рішень КСЗІ та, у разі необхідності, її окремих складових частин, а також розроблення, оформлення, узгодження та затвердження документації на КСЗІ.

4.2.2 Визначаються: функції КСЗІ в цілому та функції її окремих складових частин; склад комплексу технічного захисту інформації від спеціальних впливів (за наявності); організаційних, правових та інших заходів захисту; склад КЗЗ; узагальнена структура КСЗІ та схема взаємодії складових частин.

4.3 Технічний проект КСЗІ

4.3.1 Розробка проектних рішень КСЗІ

Виконується розробка: загальних проектних рішень, необхідних для реалізації вимог ТЗ на КСЗІ; рішень щодо структури КСЗІ (організаційної структури, структури технічних і програмних засобів), алгоритмів функціонування та умов використання засобів захисту; рішень щодо архітектури КЗЗ та механізмів реалізації, визначених функціональним профілем послуг безпеки інформації.

4.3.2 Розробка документації на КСЗІ

Виконується розроблення, оформлення, узгодження та затвердження документації в обсязі, передбаченому ТЗ на КСЗІ.

4.4 Робочий проект КСЗІ

4.4.1 На цьому етапі здійснюється розроблення, оформлення та затвердження робочої та експлуатаційної документації КСЗІ та, у разі необхідності, її окремих складових частин.

Робоча документація містить детальні рішення щодо реалізації технічного проекту КСЗІ, щодо забезпечення управління КСЗІ і взаємодії її компонентів, а також документацію, необхідну для тестування, проведення пусконалагоджувальних робіт, проведення випробувань КСЗІ.

4.4.4 До складу робочої документації на КЗЗ повинні входити описи процедур інсталяції та ініціалізації комплексу, налагодження всіх механізмів розмежування доступу користувачів до інформації та апаратних ресурсів ІТС, контролю за діями користувачів, а також контролю цілісності програмного забезпечення

4.4.5 Експлуатаційна документація включає опис порядку функціонування КСЗІ та настанови (інструкції) щодо забезпечення цього порядку обслуговуючим персоналом і користувачами, порядку супроводження КСЗІ впродовж життєвого циклу ІТС.

5 Введення КСЗІ в дію та оцінка захищеності інформації в ІТС

5.1 Підготовка КСЗІ до введення в дію

5.1.1 Проводяться роботи з підготовки організаційної структури та розробки розпорядчих документів, що регламентують діяльність із забезпечення захисту інформації в ІТС.

5.1.2 Здійснюється створення СЗІ (призначаються відповідальні особи за захист інформації), якщо цього не було зроблено на попередніх етапах.

5.1.4 Створення СЗІ та розробка Плану захисту здійснюється згідно з НД ТЗІ 1.4-001-2000.

5.2 Навчання користувачів

Проводиться навчання користувачів ІТС всіх категорій (технічного обслуговуючого персоналу, звичайних користувачів та користувачів, які мають повноваження щодо управління засобами КСЗІ та ін.) в частині, що їх стосується, основним положенням документів Плану захисту, які необхідні їм для дотримання правил політики безпеки інформації, експлуатації засобів захисту інформації тощо, перевірка їх уміння користуватись впровадженими технологіями захисту інформації і реєстрація результатів навчання.

5.5 Пусконалагоджувальні роботи

5.5.2 Монтаж ОТЗ ІТС, кабельного обладнання, мереж живлення та заземлення здійснюється згідно з конструкторською документацією робочого проекту.

5.5.8 Здійснюється згідно з документацією робочого проекту інсталяція, ініціалізація та перевірка працездатності КЗЗ.

Під час інсталяції мають бути задіяні механізми розмежування доступу користувачів до інформації та апаратних ресурсів ІТС, контролю за діями користувачів, а також контролю цілісності програмного забезпечення.

5.6 Попередні випробування

5.1. Метою попередніх випробувань є перевірка працездатності КСЗІ та визначення можливості прийняття її у дослідну експлуатацію.

Під час випробувань перевіряються працездатність КСЗІ та відповідність її вимогам ТЗ.

5.6.2 Попередні випробування проводяться згідно з програмою та методиками випробувань. Програму й методики випробувань готує розробник КСЗІ, а узгоджує замовник ІТС. Програма та методики випробувань, протоколи випробувань розробляються та оформлюються згідно з вимогами РД 50-34.698.

5.6.3 Попередні випробування організовує замовник ІТС, а проводить розробник КСЗІ спільно із замовником. Для проведення попередніх випробувань замовником ІТС створюється комісія. Головою комісії призначається представник замовника.

5.6.4 Результати попередніх випробувань оформлюються “Протоколом випробувань”, де міститься висновок щодо можливості прийняття КСЗІ у дослідну експлуатацію, а також перелік виявлених недоліків, необхідних заходів з їх усунення, і рекомендовані терміни виконання цих робіт.

5.6.5 Після усунення недоліків у випадку їх наявності та коригування проектної, робочої, експлуатаційної документації КСЗІ оформлюється акт про приймання КСЗІ у дослідну експлуатацію.

5.7 Дослідна експлуатація

5.7.1 Під час дослідної експлуатації КСЗІ:

– відпрацьовуються технології оброблення інформації, обігу машинних носіїв інформації, керування засобами захисту, розмежування доступу користувачів до ресурсів ІТС та автоматизованого контролю за діями користувачів;

– співробітники СЗІ та користувачі ІТС набувають практичних навичок з використання технічних та програмно-апаратних засобів захисту інформації, засвоюють вимоги організаційних та розпорядчих документів з питань розмежування доступу до технічних засобів та інформаційних ресурсів;

– здійснюється (за необхідністю) доопрацювання програмного забезпечення, додаткове налагоджування та конфігурування КЗЗ;

– здійснюється (за необхідністю) коригування робочої та експлуатаційної документації.

5.7.2 За результатами робіт за довільною формою складається акт про завершення дослідної експлуатації, який містить висновок щодо можливості (неможливості) представлення КСЗІ на державну експертизу.

5.8 Державна експертиза КСЗІ

5.8.1 Державна експертиза КСЗІ є окремим етапом приймальних випробувань ІТС.

5.8.2 Державна експертиза проводиться з метою визначення відповідності КСЗІ технічному завданню, вимогам НД із захисту інформації та визначення можливості введення КСЗІ в складі ІТС в експлуатацію.

Державна експертиза КСЗІ в ІТС проводиться згідно з Положенням про державну експертизу в сфері технічного захисту інформації, яке затверджене наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України 16 травня 2007 року N 93 (у редакції наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 13 жовтня 2017 року N 565).

Надання послуг щодо проведення Державної експертизи КСЗІ (оцінювання захищеності інформації) підлягає ліцензуванню відповідно до Переліку послуг у галузі технічного захисту інформації, господарська діяльність щодо надання яких підлягає ліцензуванню.

5.8.3 Виявлені під час державної експертизи недоліки усуваються до її завершення, порядок усунення такий самий, як і для попередніх випробувань. Якщо в силу якихось причин усунути недоліки в ході експертизи неможливо, це оформлюється актом, до якого вноситься перелік необхідних доробок та рекомендації щодо їх виконання. Після завершення передбачених актом робіт проводиться повторна експертиза.

5.8.4 Для інтегрованих ІТС може проводитись державна експертиза кожної складової частини (модуля) КСЗІ окремо.

5.8.5 Якщо інтегрована КСЗІ має у своєму складі типові модулі, які створювались за єдиним ТЗ, то експертиза таких модулів КСЗІ виконується в два етапи: на першому проводиться у повному обсязі експертиза одного обраного типового модуля, а на другому – здійснюється перевірка відповідності умов експлуатації типовим на кожному конкретному об’єкті для всіх модулів КСЗІ цього типу.

5.8.6 Введення до складу діючої КСЗІ нового (оціненого) модуля здійснюється без проведення повторної експертизи всієї КСЗІ. Проводиться оцінювання взаємодії нового модуля зі складовими частинами КСЗІ, які вже знаходяться в експлуатації.

5.8.7 Допускається розпочинати і проводити державну експертизу КСЗІ паралельно з роботами етапів проектування.

12.2. Проведення аудиту інформаційної безпеки та визначення на основі звіту з аудиту ризиків ІБ

Мета процесу аудиту та аналізу ризиків полягає у визначенні рівня ризиків інформаційної системи.

Згідно **НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу** визначені наступні поняття щодо ризику інформаційної безпеки.

Створення КСЗІ має починатись з аналізу об'єкта захисту і можливих загроз. Передусім мають бути визначені ресурси АС, що підлягають захисту. Загрози мають бути визначені в термінах ймовірності їх реалізації і величини можливих збитків. На підставі аналізу загроз, існуючих в системі вразливостей,

ефективності вже реалізованих заходів захисту для всіх ресурсів, що підлягають захисту, мають бути оцінені ризики. **Ризик** являє собою функцію ймовірності реалізації певної загрози, виду і величини завданих збитків. **Величина ризику** може бути виражена в грошовому вимірі або у вигляді формальної оцінки (високий, низький і т. ін.). На підставі виконаної роботи мають бути вироблені заходи захисту, перетворення яких в життя дозволило б знизити рівень остаточного ризику до прийнятного рівня. Підсумком даного етапу робіт повинна стати сформульована або скоригована політика безпеки.

На підставі проведеного аналізу ризиків сформульованої політики безпеки розробляється план захисту, який включає в себе опис послідовності і змісту всіх стадій і етапів життєвого циклу КСЗІ, що мають відповідати стадіям і етапам життєвого циклу автоматизованої системи (АС). **Вартість заходів щодо захисту інформації має бути адекватною розміру можливих збитків.**

Згідно **НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі** визначені наступні поняття щодо **аналізу ризиків** інформаційної безпеки.

Основою для проведення аналізу ризиків і формування вимог до КСЗІ є розробка моделі загроз для інформації та моделі порушника.

Аналіз ризиків

Аналіз ризиків передбачає вивчення моделі загроз для інформації та моделі порушників, можливих наслідків від реалізації потенційних загроз (рівня можливої заподіяної ними шкоди) і формування на його підставі моделі захисту інформації в АС. Під час проведення аналізу ризиків необхідним є виконання наступних робіт.

1. Визначення компонентів і ресурсів АС, які необхідно враховувати при аналізі. Повинні бути визначені критичні з точки зору безпеки компоненти і ресурси АС, які можуть бути об'єктами атаки або самі є потенційним джерелом порушення безпеки інформації (об’єкти захисту). Для цього використовуються відомості п.3 додатку, одержані в результаті обстеження середовищ функціонування АС.

2. Ідентифікація загроз з об’єктами захисту. Встановлюється відповідність моделі загроз і об’єктів захисту, тобто складається матриця загрози/компоненти (ресурси) АС. Кожному елементу матриці повинен бути зіставлений опис можливого впливу загрози на відповідний компонент або ресурс АС. У процесі упорядкування матриці може уточнюватися список загроз і об’єктів захисту, внаслідок чого коригуватись модель загроз.

3. Оцінка ризиків. Повинні бути отримані оцінки гранично припустимого й існуючого (реального) ризику здійснення кожної загрози впродовж певного проміжку часу, тобто ймовірності її здійснення впродовж цього інтервалу. Для оцінки ймовірності реалізації загрози рекомендується вводити декілька дискретних ступенів (градацій). Оцінку слід робити за припущення, що кожна подія має найгірший, з точки зору власника інформації, що потребує захисту, закон розподілу, а також за умови відсутності заходів захисту інформації. На

практиці для більшості загроз неможливо одержати достатньо об’єктивні дані про ймовірність їхньої реалізації і доводиться обмежуватися якісними оцінками. У цьому випадку значення ймовірності реалізації загрози визначається в кожному конкретному випадку експертним методом або емпіричним шляхом, на підставі досвіду експлуатації подібних систем, шляхом реєстрації певних подій і визначення частоти їхнього повторення тощо. Оцінка може мати числове або смислове значення (наприклад, ймовірність реалізації загрози – незначна, низька, висока, неприпустимо висока). У будь-якому випадку існуючий ризик не повинен перевищувати гранично допустимий для кожної загрози. Перевищення свідчить про необхідність впровадження додаткових заходів захисту. Мають бути розроблені рекомендації щодо зниження ймовірності виникнення або реалізації загроз та величини ризиків.

4. Оцінювання величини можливих збитків, пов'язаних з реалізацією загроз. Виконується кількісна або якісна оцінка збитків, що можуть бути нанесені АС (організації) внаслідок реалізації загроз. Доцільно, щоб ця оцінка складалась з величин очікуваних збитків від втрати інформацією кожної з властивостей (конфіденційності, цілісності або доступності) або від втрати керованості АС внаслідок реалізації загрози. Для одержання оцінки можуть бути використані такі ж методи, як і при аналізі ризиків. Величина можливих збитків визначається розміром фінансових втрат або, у разі неможливості визначення цього, за якісною шкалою (наприклад, величина збитків – відсутня, низька, середня, висока, неприпустимо висока).

5. Вибір варіанту побудови КСЗІ. В залежності від конфіденційності інформації, яка обробляється в АС, рівня її критичності, величини можливих збитків від реалізації загроз, матеріальних, фінансових та інших ресурсів, які є у розпорядженні власника АС, а також інших чинників обґрунтовується пропозиція щодо доцільності застосування варіантів побудови КСЗІ. Можливі наступні варіанти:

– досягнення необхідного рівня захищеності інформації за мінімальних затрат і допустимого рівня обмежень на технологію її обробки в АС;

– досягнення необхідного рівня захищеності інформації за допустимих затрат і заданого рівня обмежень на технологію її обробки в АС;

– досягнення максимального рівня захищеності інформації за необхідних затрат і мінімального рівня обмежень на технологію її обробки в АС.

Якщо інформація становить державну таємницю, то необхідно застосовувати, як правило, третій варіант.

6 Оцінювання витрат на КСЗІ. Здійснюється первинне (попереднє) оцінювання допустимих витрат на блокування загроз, виходячи з вибраного варіанту побудови КСЗІ і виділених на це коштів. На етапі проектування КСЗІ, після формування пропозицій щодо складу заходів і засобів захисту, здійснюється оцінка залишкового ризику для кожної пропозиції (наприклад, за критерієм “ефективність/вартість”), вибирається найбільш оптимальна серед них і первинна оцінка уточнюється.

Якщо **залишковий ризик** перевищує гранично допустимий, вносяться відповідні зміни до складу заходів і засобів захисту, після чого всі процедури виконуються повторно до одержання прийнятного результату.

Основні підходи до аудиту та аналізу ризиків

Управління ризиками складається з трьох етапів:

– оцінка;

– зменшення;

– застосування заходів після оцінки ризику.

Управління ризиками – це процес, що дозволяє менеджерам здійснювати баланс між економічною та операційною вартістю ризику. Тому управління ними – це одне з головних завдань організації, оскільки воно дозволяє знайти баланс між вартістю засобів захисту інформації та вартістю ймовірної шкоди.

Основні компоненти управління ризиками

– Ресурси – інформація та підтримуючі засоби, які потрібні організації для ведення бізнесу. Це, наприклад, інформація/дані, паперові документи, програмне забезпечення, фізичне обладнання, служби, люди та їх знання, імідж та репутація організації. Кожному ресурсу інформаційної системи має бути присвоєно певне значення, що використовується визначення його важливості для бізнесу та необхідності тієї чи іншої рівня захисту. Значення можуть виражатися в термінах потенційного впливу на бізнес небажаних подій, що призводять до втрати конфіденційності, цілісності та доступності. Потенційний вплив включає фінансові втрати, падіння доходів та акцій на ринку або падіння престижу, що може призвести до фінансових втрат.

– Загроза – будь-які обставини чи події, які можуть спричинити порушення політики безпеки та/або заподіяння збитків автоматизованій системі. Загрози можуть бути ненавмисними (повінь, пожежа, землетрус), навмисними або випадковими. Результатом реалізації загрози можуть бути такі події, як руйнування, пошкодження чи модифікація, крадіжка, видалення чи втрата, розкриття об'єкта, використання чи впровадження нелегального об'єкта, переривання служби. Щоб загроза завдала шкоди, необхідна реалізація певної вразливості системи.

– Вразливість системи – неможливість системи протистояти реалізації певної загрози чи сукупності загроз. Як правило, вразливість виникає внаслідок погано відпрацьованих процедур, помилок некваліфікованого персоналу, внаслідок некоректної конфігурації системи. Щоб вразливість була використана, вона має бути відома чи реалізована загрозою.

– Ризик – функція ймовірності реалізації певної загрози, виду та величини зазнаних втрат. Рівень ризику безпеки визначається комбінацією значень ресурсів, оцінених рівнів відповідних загроз та асоційованих із нею вразливостей.

– Аналіз ризику – процес визначення загроз безпеки інформації та їх характеристик, слабких сторін комплексної системи захисту інформації (відомих та ймовірних), оцінки потенційних збитків від реалізації загроз та ступеня їхньої прийнятності для експлуатації автоматизованої системи.

– Базовий аналіз ризиків – аналіз ризиків, який проводиться відповідно до вимог базового рівня безпеки. Методи даного класу застосовуються у випадках, коли до інформаційної системи не висувається підвищених вимог у галузі ІБ.

– Повний аналіз ризиків – аналіз ризиків для інформаційних систем, які висувають підвищені вимоги до ІБ.

– Ризик порушення інформаційної безпеки – можливість реалізації загрози.

– Оцінка ризиків – ідентифікація ризиків, вибір параметрів для їх опису та отримання оцінок за цими параметрами.

– Управління ризиками – процес визначення контрзаходів відповідно до оцінки ризиків.

– Система управління інформаційною безпекою (СУІБ) або **Система менеджменту інформаційної безпеки (СМІБ)** – комплекс заходів, спрямованих на забезпечення режиму інформаційної безпеки на всіх стадіях життєвого циклу автоматизованих систем.

– Клас ризиків – безліч загроз ІХ, виділених за певною ознакою.

Процес оцінки ризиків

Оцінка ризику включає такі кроки:

1. Визначення характеристик системи.
2. Ідентифікація небезпек.
3. Ідентифікація вразливостей.
4. Аналіз контролю.
5. Визначення ймовірностей.
6. Аналіз впливу.
7. Визначення ризику.
8. Рекомендації щодо контролю.
9. Результуюча документація.

Крок 1. Визначення характеристик системи

На даному етапі збирається інформація, яка включає відомості про апаратуру; програмному забезпеченні, системних інтерфейсах (внутрішніх та зовнішніх з'єднаннях), даних, персоналі, що підтримує та використовує систему, призначенні системи (процесах, що виробляються системою), критичності системи та даних, їх чутливості.

Для збору цієї інформації можуть використовуватися запитальники, інтерв'ю, огляд документів, автоматичні пристрої сканування.

Крок 2. Ідентифікація загроз

Джерело загроз визначається як будь-яка обставина чи подія, які потенційно можуть завдати шкоди ІТ-системі. Спільними джерелами загроз можуть бути природа, люди та обладнання.

Крок 3. Аналіз вразливостей

Для визначення системних вразливостей використовуються джерела загроз та результати тестування системної безпеки. Потім слідує розробка контрольного списку вимог щодо безпеки. Необхідно відзначити, що типи вразливостей та методика їх визначення залежать від структури IT-інфраструктури.

Знаходження джерел вразливостей

Вразливості (як технічного, і нетехнічного характеру) ідентифікуються шляхом застосування технологій збору інформації. Іншим джерелом даних про вразливість є інтернет. Розробники часто публікують у Мережі відомі системні вразливості разом із засобами, призначеними для їх усунення або зменшення. Водночас можуть застосовуватись інші документовані джерела.

Тестування системної безпеки

Для оцінки дійсної наявності вразливостей можуть застосовуватись автоматичні засоби сканування, тести та оцінка безпеки, тести на проникнення. Автоматичні засоби сканування можуть бути використані для сканування мережі щодо наявності вразливих системних служб. Разом з тим слід зауважити, що не всі потенційні вразливості, визначені в такий спосіб, становлять реальну загрозу інформаційній безпеці організації.

Тест та оцінка безпеки включає розробку та виконання тестування. Призначення цього методу – протестувати ефективність контролю безпеки системи.

Тести проникнення використовуються з метою оцінки рівня контролю безпеки, здатності протистояти атакам на інформаційну систему.

Крок 4. Аналіз засобів захисту (контролю)

На цьому кроці проводиться аналіз засобів, що застосовуються або плануються до застосування засобів захисту інформації.

Крок 5. Ранжування частот появи

На цьому кроці необхідно визначити можливість реалізації потенційної вразливості. При цьому ймовірність описується як висока, середня та низька.

Крок 6. Аналіз впливу

На цьому кроці визначається величина впливу (висока, середня та низька), яку може зробити успішна реалізація загрози.

Крок 7. Визначення ризику

На цьому етапі оцінюється рівень ризику для системи. При цьому ризик виражається як функція від ймовірності того, що джерело загроз намагається реалізувати вразливість. Для вимірювання ризику розробляються шкали ризику та матриця рівнів ризику.

Визначення ризику одержують множенням класів (rating) ймовірностей загроз та впливу загроз.

Дана матриця (3x3) є матрицею оцінки загроз (високої, середньої, низької) та впливу загрози (висока, середня, низька). Залежно від вимог організації та кількості градацій бажаної оцінки ризику можна використовувати матриці 4x4 або 5x5.

Крок 8. Рекомендації щодо засобів захисту (контролю)

Метою цих рекомендацій є зменшення рівня ризику в інформаційній системі до допустимого рівня.

Виходом 8-го кроку є рекомендації щодо засобів захисту (контролю) та альтернативні рішення для зменшення ризику.

Крок 9. Результуюча документація

Після закінчення оцінки ризику результати подаються у вигляді звіту.

Зменшення ризиків

Процес зменшення ризику

Після того, як отримані результати оцінки ризиків, виникає завдання розділити ризики на прийнятні та неприйнятні. Для неприйнятних ризиків необхідно застосовувати процедури їхнього зменшення.

У загальному випадку зменшення ризику може бути досягнуто шляхом застосування однієї або комбінації наступних операцій, таких як прийняття ризику, ухилення від нього, обмеження, планування, дослідження та підтвердження, передача ризику.

Загальна схема процесу зменшення ризику ілюструє ці питання. Відповідні точки застосування дій засобів захисту малюнку позначені словом “так”.

Основним методом зниження ризику є застосування засобів захисту (контролю). Для зменшення ризику використовується наступна методологія, що описує підхід до застосування засобів захисту:

– Крок 1. Привласнення пріоритетів діям. Результат кроку 1 – ранжовані (від високого до низького) ризики.

– Крок 2.Оцінка рекомендованих варіантів захисту. Результат – перелік відповідних засобів захисту.

– Крок 3. Проведення аналізу витрат та результатів. Результат кроку 3 – аналіз витрат та результатів, що описує вартість та результати застосування засобів захисту.

– Крок 4. Вибір засобів захисту. Результат кроку 4 – список вибраних коштів.

– Крок 5. Призначення відповідальних. Результат – список відповідальних осіб.

– Крок 6. Розробка плану реалізації захисту. На цьому етапі розробляється план реалізації (застосування) засобів захисту (план дій). Результат кроку 6 – план застосування засобів захисту.

– Крок 7. Застосування вибраних засобів захисту. Результат – залишковий ризик.

При застосуванні рекомендованих засобів для зменшення ризику керівництво організації розглядає технічні, управлінські та операційні засоби захисту або їхню комбінацію, щоб максимізувати ефективність захисту для своєї ІТ-системи та організації.

Залишковий ризик

Застосування засобів захисту не гарантує знищення ризику. Тому завжди залишається певний рівень його, який називається залишковим ризиком. Загальна схема отримання залишкового ризику ілюструється малюнком.

Обчислення та оцінювання

Тенденції розвитку організацій показують, що з часом їх комп'ютерні мережі розширюватимуться та оновлюватимуться, компоненти мереж змінюватимуться та доповнюватимуться, прикладне та системне програмне забезпечення замінюватиметься чи оновлюватимуться новими версіями. Крім того, великі зміни зачіпають персонал організації та, відповідно, політику безпеки. Ці зміни означають, що з'являються нові ризики, і ризики, які раніше зазнали зменшення, знову стають значними. Тому процес управління ризиками має бути безперервним та еволюціонуючим

12.3. Вибір методів та засобів забезпечення необхідного рівня ІБ

Системний підхід до опису інформаційної безпеки пропонує виділити такі складові інформаційної безпеки:

1. Законодавча, нормативно-правова та наукова база.
2. Структура та завдання органів (підрозділів), що забезпечують безпеку ІТ.
3. Організаційно-технічні та режимні заходи та методи (Політика інформаційної безпеки).
4. Програмно-технічні способи та засоби забезпечення інформаційної безпеки.

Метою реалізації інформаційної безпеки будь-якого об'єкта є побудова **Системи забезпечення інформаційної безпеки** даного об'єкта (**СЗІБ**). Для побудови та ефективної експлуатації СЗІБ необхідно:

– виявити вимоги захисту інформації, специфічні для цього об'єкта захисту;

– врахувати вимоги національного та міжнародного Законодавства;

– використовувати напрацьовані практики (стандарти, методології) побудови подібних СЗІБ;

– визначити підрозділи, відповідальні за реалізацію та підтримку СЗІБ;

– розподілити між підрозділами відповідальності у здійсненні вимог СЗІБ;

– на базі управління ризиками інформаційної безпеки визначити загальні положення, технічні та організаційні вимоги, що становлять Політику інформаційної безпеки об'єкта захисту;

– реалізувати вимоги Політики інформаційної безпеки, запровадивши відповідні програмно-технічні способи та засоби захисту інформації;

– реалізувати **Систему менеджменту (управління) інформаційної безпеки (СМІБ)**;

– використовуючи СМІБ організувати регулярний контроль ефективності СЗІБ та за необхідності перегляд та коригування СЗІБ та СМІБ.

Як очевидно з останнього етапу робіт, процес реалізації СЗІБ безперервний і циклічно (після кожного перегляду) повертається до першого етапу, повторюючи послідовно й інші. Так СЗІБ коригується для ефективного виконання своїх завдань захисту інформації та відповідності новим вимогам інформаційної системи, що постійно оновлюється.

1. Організаційно-технічні та режимні заходи та методи

Для опису технології захисту інформації конкретної інформаційної системи зазвичай будується так звана **Політика інформаційної безпеки** або Політика безпеки інформаційної системи, що розглядається.

Політика безпеки (інформації в організації) (англ. Organizational security policy) – сукупність документованих правил, процедур, практичних прийомів або керівних принципів у сфері безпеки інформації, якими керується організація у своїй діяльності.

Політика безпеки інформаційно-телекомунікаційних технологій (англ. ICTsecurity policy) – правила, директиви, практика, що склалася, які визначають, як у межах організації та її інформаційно-телекомунікаційних технологій управляти, захищати та розподіляти активи, у тому числі критичну інформацію.

Для побудови Політики інформаційної безпеки рекомендується окремо розглядати такі напрямки захисту інформаційної системи:

– Захист об'єктів інформаційної системи.

– Захист процесів, процедур та програм обробки інформації.

– Захист каналів зв'язку (акустичні, інфрачервоні, дротові оптичні, радіоканали та ін.).

– Пригнічення побічних електромагнітних випромінювань та наведень (ПЕМВН).

– Управління системою захисту.

При цьому в кожному з перерахованих вище напрямків **Політика інформаційної безпеки має описувати такі етапи створення засобів захисту інформації**:

1. Визначення інформаційних та технічних ресурсів, що підлягають захисту.

2. Виявлення повної множини потенційно можливих загроз та каналів витоку інформації.

3. Проведення оцінки вразливості та ризиків інформації за наявної множини загроз та каналів витоку.

4. Визначення вимог до системи захисту.

5. Здійснення вибору засобів захисту інформації та їх характеристик.

6. Впровадження та організація використання обраних заходів, способів та засобів захисту.

7. Здійснення контролю цілісності та управління системою захисту.

Політика інформаційної безпеки оформляється як документованих вимог на інформаційну систему. Документи зазвичай поділяють за рівнями опису (деталізації) процесу захисту.

Документи верхнього рівня Політики інформаційної безпеки відображають позицію організації до діяльності в галузі захисту інформації, її прагнення відповідати державним, міжнародним вимогам та стандартам у цій галузі. Подібні документи можуть називатися «**Концепція ІБ**», «**Регламент управління ІБ**», «**Політика ІБ**», «**Технічний стандарт ІБ**» тощо. зовнішнього та внутрішнього використання.

Відповідно до стандарту **ISO/IEC 27002,** на **верхньому рівні Політики інформаційної безпеки** мають бути оформлені такі документи: «**Концепція забезпечення ІБ**», «**Правила допустимого використання ресурсів інформаційної системи**», «**План забезпечення безперервності бізнесу**».

До середнього рівня відносять документи щодо окремих аспектів інформаційної безпеки. Це вимоги на створення та експлуатацію засобів захисту інформації, організацію інформаційних та бізнес-процесів організації за конкретним напрямом захисту інформації. Наприклад: Безпека даних, Безпека комунікацій, Використання засобів криптографічного захисту, Контентна фільтрація тощо. Подібні документи зазвичай видаються у вигляді внутрішніх технічних та організаційних політик (стандартів) організації. Усі документи середнього рівня політики інформаційної безпеки є конфіденційними.

У політику інформаційної безпеки **нижнього рівня** входять регламенти робіт, посібники з адміністрування, інструкції з експлуатації окремих послуг інформаційної безпеки.

2. Організаційний захист об'єктів інформаційних систем

Організаційний захист – це регламентація виробничої діяльності та взаємовідносин виконавців на нормативно-правовій основі, що виключає або суттєво ускладнює неправомірне оволодіння конфіденційною інформацією та прояв внутрішніх та зовнішніх загроз. Організаційний захист забезпечує:

– організацію охорони, режиму, роботу з кадрами, документами;

– використання технічних засобів безпеки та інформаційно-аналітичну діяльність з виявлення внутрішніх та зовнішніх загроз підприємницької діяльності.

До основних організаційних заходів належать:

– організація режиму та охорони. Їхня мета – виключення можливості таємного проникнення на територію та у приміщення сторонніх осіб;

– організація роботи зі співробітниками, яка передбачає добір та розстановку персоналу, включаючи ознайомлення зі співробітниками, їх вивчення, навчання правил роботи з конфіденційною інформацією, ознайомлення із заходами відповідальності за порушення правил захисту інформації та ін.;

– організація роботи з документами та документованою інформацією, включаючи організацію розробки та використання документів та носіїв

конфіденційної інформації, їх облік, виконання, повернення, зберігання та знищення;

– організація використання технічних засобів збору, обробки, накопичення та зберігання конфіденційної інформації;

– організація роботи з аналізу внутрішніх та зовнішніх загроз конфіденційної інформації та вироблення заходів щодо забезпечення її захисту;

– організація роботи з проведення систематичного контролю за роботою персоналу з конфіденційною інформацією, порядком обліку, зберігання та знищення документів та технічних носіїв.

У кожному даному випадку організаційні заходи носять специфічну для цієї організації форму і зміст, створені задля забезпечення безпеки інформації у конкретних умовах.

3. Програмно-технічні способи та засоби забезпечення інформаційної безпеки.

Класифікація засобів захисту.

– Засоби захисту від несанкціонованого доступу (НСД):
  - Засоби авторизації.
  - Мандатне керування доступом.
  - Виборче керування доступом.
  - Управління доступом на основі ролей.
  - Журналювання (так само називається Аудит).
– Системи аналізу та моделювання інформаційних потоків (CASE-системи).
– Системи моніторингу мереж:
  - Системи виявлення та запобігання вторгненням (IDS/IPS).
  - Системи запобігання витоку конфіденційної інформації (DLP-системи).
– Аналізатори протоколів.
– Антивірусні засоби.
– Міжмережеві екрани.
– Криптографічні засоби:
  - Шифрування.
  - Цифровий підпис.
– Системи резервування:
  - Резервне копіювання.
  - Відмовостійкий кластер.
  - Резервний Центр обробки даних (ЦОД) для катастрофостійкої ІС.
– Системи безперебійного живлення:
  - Джерела безперебійного живлення.
  - Резервні лінії електроживлення.
  - Генератори електроживлення.

- Системи автентифікації на основі:
  - Паролі.
  - Ключі доступу (фізичного або електронного).
  - Сертифікат.
  - Біометричні дані.
- Засоби запобігання злому корпусів та крадіжок обладнання.
- Засоби контролю та управління доступом до приміщень.
- Інструментальні засоби аналізу систем захисту.
- Засоби захисту від ПЕМВН.

Розділ 13. Моделі загроз та моделі порушника

13.1. Загальні визначення й поняття моделі загроз та моделі порушника.
13.2. Загрози цілісності.
13.3. Загрози доступності.
13.4. Загрози конфіденційності.
13.5. Загрози автентичності.
13.6. Загрози через технічні канали.
13.7. Загрози через соціальну інженерію.

13.1. Загальні визначення й поняття моделі загроз та моделі порушника

Згідно **НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу**, визначені наступні поняття щодо **моделі загроз та моделі порушника**.

Основні загрози інформації

Інформація в комп'ютерних системах (КС) існує у вигляді даних, тобто представляється в формалізованому вигляді, придатному для обробки. Тут і далі під обробкою слід розуміти як власне обробку, так і введення, виведення, зберігання, передачу і т. ін. (ДСТУ 2226-93). Далі терміни «інформація» і «дані» використовуються як синоніми.

Інформація для свого існування завжди вимагає наявності носія. Як **носій** інформації може виступати поле або речовина. В деяких випадках у вигляді носія інформації може розглядатися людина. Втрата інформацією своєї цінності (порушення безпеки інформації) може статися внаслідок переміщення інформації або зміни фізичних властивостей носія.

При аналізі проблеми захисту від НСД інформації, яка може циркулювати в КС, як правило, розглядаються лише інформаційні об'єкти, що служать приймальниками/джерелами інформації, і інформаційні потоки (порції інформації, що пересилаються між об'єктами) безвідносно до фізичних характеристик їх носіїв.

Загрози оброблюваної в АС інформації залежать від характеристик ОС, фізичного середовища, персоналу і оброблюваної інформації. Загрози можуть мати або об'єктивну природу, наприклад, зміна умов фізичного середовища (пожежі, повені і т. і.) чи відмова елементів ОС, або суб'єктивну, наприклад, помилки персоналу чи дії зловмисника. Загрози, що мають суб'єктивну природу, можуть бути випадковими або навмисними. Спроба реалізації загрози називається атакою.

Із всієї множини способів класифікації загроз найпридатнішою для аналізу є **класифікація загроз за результатом їх впливу на інформацію, тобто порушення конфіденційності, цілісності і доступності інформації.**

Інформація зберігає **конфіденційність**, якщо дотримуються встановлені правила ознайомлення з нею.

Інформація зберігає **цілісність**, якщо дотримуються встановлені правила її модифікації (видалення).

Інформація зберігає **доступність**, якщо зберігається можливість ознайомлення з нею або її модифікації відповідно до встановлених правил упродовж будь-якого певного (малого) проміжку часу.

Загрози, реалізація яких призводить до втрати інформацією якої-небудь з названих властивостей, відповідно є **загрозами конфіденційності, цілісності або доступності інформації**. Загрози можуть впливати на інформацію не безпосередньо, а опосередковано. Наприклад, втрата КС керованості може призвести до нездатності КС забезпечувати захист інформації і, як результат, до втрати певних властивостей оброблюваної інформації.

Модель порушника

Як порушник розглядається особа, яка може одержати доступ до роботи з включеними до складу КС засобами. Порушники класифікуються за рівнем можливостей, що надаються їм штатними засобами КС. Виділяються **чотири рівні цих можливосте**й. Класифікація є ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього:

– **перший рівень** визначає найнижчий рівень можливостей проведення діалогу з КС – можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;

– **другий рівень** визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;

– **третій рівень** визначається можливістю управління функціонуванням КС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;

– **четвертий рівень** визначається всім обсягом можливостей осіб, що здійснюють проектування, реалізацію і ремонт апаратних компонентів КС, аж до включення до складу КС власних засобів з новими функціями обробки інформації. Припускається, що в своєму рівні порушник – це фахівець вищої кваліфікації, який має повну інформацію про КС і КЗЗ. Така класифікація порушників є корисною для використання в процесі оцінки ризиків, аналізу вразливості системи, ефективності існуючих і планових заходів захисту.

Згідно **НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі**, визначені наступні поняття щодо **моделі загроз та моделі порушника**.

Модель загроз

Загрози для інформації в АС

Основою для проведення аналізу ризиків і формування вимог до КСЗІ є розробка моделі загроз для інформації та моделі порушника.

Для створення **моделі загроз** необхідно скласти **перелік суттєвих загроз**, описати **методи** і **способи** їхнього **здійснення**.

Необхідно визначити, якими з можливих **способів** можуть здійснюватися загрози в АС:

– технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо- та радіотехнічні, хімічні та інші канали;

– каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;

– несанкціонованим доступом шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав’язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп’ютерних вірусів.

Загрози для інформації, що обробляється в АС, залежать від характеристик ОС, фізичного середовища, персоналу, технологій обробки та інших чинників і можуть мати об'єктивну або суб'єктивну природу. Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні.

Мають бути визначені **основні види загроз** для безпеки інформації, які можуть бути реалізовані стосовно АС і повинні враховуватись у моделі загроз, наприклад:

– зміна умов фізичного середовища (стихійні лиха і аварії, як землетрус, повінь, пожежа або інші випадкові події);

– збої і відмови у роботі обладнання та технічних засобів АС;

– наслідки помилок під час проектування та розробки компонентів АС (технічних засобів, технології обробки інформації, програмних засобів, засобів захисту, структур даних тощо);

– помилки персоналу (користувачів) АС під час експлуатації;

– навмисні дії (спроби) потенційних порушників. 4.2.3 Необхідно визначити перелік можливих загроз і класифікувати їх за результатом впливу на інформацію, тобто на порушення яких властивостей вони спрямовані (конфіденційності, цілісності та доступності інформації), а також порушення спостережності та керованості АС.

Випадковими загрозами суб’єктивної природи (дії, які здійснюються персоналом або користувачами по неуважності, недбалості, незнанню тощо, але без навмисного наміру) можуть бути:

– дії, що призводять до відмови АС (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв’язку, видалення даних, програм та ін.);

– ненавмисне пошкодження носіїв інформації;

– неправомірна зміна режимів роботи АС (окремих компонентів, обладнання, ПЗ тощо), ініціювання тестуючих або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації);

– неумисне зараження ПЗ комп'ютерними вірусами;

– невиконання вимог до організаційних заходів захисту чинних в АС розпорядчих документів;

– помилки під час введення даних в систему, виведення даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо;

– будь-які дії, що можуть призвести до розголошення конфіденційних відомостей, атрибутів розмежування доступу, втрати атрибутів тощо;

– неправомірне впровадження і використання забороненого політикою безпеки ПЗ (наприклад, навчальні та ігрові програми, системне і прикладне забезпечення та ін.);

– наслідки некомпетентного застосування засобів захисту;

– інші.

Навмисними загрозами суб'єктивної природи, спрямованими на дезорганізацію роботи АС (окремих компонентів) або виведення її з ладу, проникнення в систему і одержання можливості несанкціонованого доступу до її ресурсів, можуть бути:

– порушення фізичної цілісності АС (окремих компонентів, пристроїв, обладнання, носіїв інформації);

– порушення режимів функціонування (виведення з ладу) систем життєзабезпечення АС (електроживлення, уземлення, охоронної сигналізації, вентиляції та ін.);

– порушення режимів функціонування АС (обладнання і ПЗ);

– впровадження і використання комп'ютерних вірусів, закладних (апаратних і програмних) і підслуховуючих пристроїв, інших засобів розвідки;

– використання засобів перехоплення побічних електромагнітних випромінювань і наводів, акусто-електричних перетворень інформаційних сигналів;

– використання (шантаж, підкуп тощо) з корисливою метою персоналу АС;

– крадіжки носіїв інформації, виробничих відходів (роздруків, записів, тощо);

– несанкціоноване копіювання носіїв інформації;

– читання залишкової інформації з оперативної пам'яті ЕОМ, зовнішніх накопичувачів;

– одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача ("маскарад");

– неправомірне підключення до каналів зв'язку, перехоплення даних, що передаються, аналіз трафіку тощо;

– впровадження і використання забороненого політикою безпеки ПЗ або несанкціоноване використання ПЗ, за допомогою якого можна одержати доступ до критичної інформації (наприклад, аналізаторів безпеки мереж);

– інші.

Перелік суттєвих загроз має бути максимально повним і деталізованим. **Для кожної з загроз необхідно визначити**:

– на порушення яких властивостей інформації або АС вона спрямована (рекомендується користуватись чотирма основними градаціями – порушення конфіденційності, цілісності, доступності інформації, а також порушення спостережності та керованості АС);

– джерела виникнення (які суб'єкти АС або суб'єкти, зовнішні по відношенню до неї, можуть ініціювати загрозу);

– можливі способи здійснення загроз.

Модель порушника

У кожному конкретному випадку, виходячи з технології обробки інформації, необхідно розробити модель порушника, яка повинна бути адекватна реальному порушнику для даної АС. Модель порушника – абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії і т.ін. По відношенню до АС порушники можуть бути внутрішніми (з числа співробітників, користувачів системи) або зовнішніми (сторонні особи або будь-які особи, що знаходяться за межами контрольованої зони).

Модель порушника повинна визначати:

– можливу мету порушника та її градацію за ступенями небезпечності для АС;

– категорії осіб, з числа яких може бути порушник.;

– припущення про кваліфікацію порушника;

– припущення про характер його дій.

Метою порушника можуть бути:

– отримання необхідної інформації у потрібному обсязі та асортименті;

– мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами (інтересами, планами);

– нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

Рекомендується класифікувати порушників за рівнем можливостей, що надаються їм засобами АС, наприклад, поділити на чотири рівні цих можливостей.

Класифікація є ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього:

– **перший рівень** визначає найнижчий рівень можливостей ведення діалогу з АС – можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;

– **другий рівень** визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;

– **третій рівень** визначається можливістю управління функціонуванням АС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;

– **четвертий рівень** визначається повним обсягом можливостей осіб, що здійснюють проектування, реалізацію, впровадження, супроводження програмно-апаратного забезпечення АС, аж до включення до складу АС власних засобів з новими функціями обробки інформації.

За рівнем знань про АС усіх порушників можна класифікувати як таких, що:

– володіють інформацією про функціональні особливості АС, основні закономірності формування в ній масивів даних та потоків запитів до них, вміють користуватися штатними засобами;

– володіють високим рівнем знань та досвідом роботи з технічними засобами системи та їхнього обслуговування;

– володіють високим рівнем знань у галузі обчислювальної техніки та програмування, проектування та експлуатації АС;

– володіють інформацією про функції та механізм дії засобів захисту.

За використовуваними методами і способами порушників можна класифікувати як таких, що:

– використовують виключно агентурні методи одержання відомостей;

– використовують пасивні технічні засоби перехоплення інформаційних сигналів;

– використовують виключно штатні засоби АС або недоліки проектування КСЗІ для реалізації спроб НСД;

– використовують способи і засоби активного впливу на АС, що змінюють конфігурацію системи (підключення додаткових або модифікація штатних технічних засобів, підключення до каналів передачі даних, впровадження і використання спеціального ПЗ тощо).

За місцем здійснення дії можуть класифікуватись:

– без одержання доступу на контрольовану територію організації (АС);

– з одержанням доступу на контрольовану територію, але без доступу до технічних засобів АС;

– з одержанням доступу до робочих місць кінцевих (у тому числі віддалених) користувачів АС;

– з одержанням доступу до місць накопичення і зберігання даних (баз даних, архівів, АРМ відповідних адміністраторів тощо);

– з одержанням доступу до засобів адміністрування АС і засобів керування КСЗІ.

Далі більш детально розглянемо питання моделі загроз та моделі порушника. Наявна постійна еволюція як інформаційних технологій, так і сфери захисту інформації, а також самих атакуючих: якщо ще наприкінці 20-го століття питаннями злому комп'ютерних систем займалися, як правило, захоплені ентузіасти з академічних середовищ, які не мали на меті отримання незаконного прибутку та обман компаній та громадян, то останнім часом з кожним роком зростає кількість фінансово мотивованих зловмисників. Більше того, в сучасному кіберпросторі орудують справжні армії хакерів, які підтримують і спонсорують уряди різних країн. Вони здійснюють напади на ресурси та інфраструктуру інших держав та великих корпорацій з метою одержання

розвідувальної інформації та, найчастіше, виведення з ладу об'єктів критичної інфраструктури або навіть цілих галузей промисловості. Одночасно з цим наростає також державний регуляторний тиск: усвідомлюючи важливість захисту інформації та інформаційної інфраструктури, практично всі розвинуті держави приймають законодавчі норми, що відповідають сучасним викликам. Таким чином, сучасна інформаційна безпека знаходиться на лінії перехресного вогню наступних чинників:

– висококваліфікованих атакуючих;

– IT-потреб бізнесу та держави;

– правового регулювання.

Для перемоги в умовах передусім необхідний твердий фундамент, саме чітке розуміння основних явищ, термінів, і навіть самої концепції інформаційної безпеки.

Під **захистом інформації** в класичному розумінні мається на увазі забезпечення **цілісності, конфіденційності, доступності** інформаційних ресурсів. Крім цього, **додатковими властивостями інформації** у стані захищеності є **невідмовність, справжність, підзвітність**.

Під **загрозою безпеці** інформації розуміють потенційну причину виникнення небажаного інциденту інформаційної безпеки, який може завдати шкоди активам та порушити стан захищеності інформації; інциденту може передувати несанкціонована зміна стану активу, що називається подією інформаційної безпеки.

Моделювання загроз – це ідентифікація всіх загроз, які можуть завдати шкоди активам, та векторів атак, які можуть бути використані джерелами загроз для заподіяння шкоди.

Під **ризиком інформаційної безпеки** розуміють потенційну можливість використання вразливостей активів конкретною загрозою заподіяння шкоди організації. Як і в класичному **ризик-менеджменті**, є такі способи **обробки кіберризику**:

– ігнорувати;

– прийняти;

– уникнути;

– передати;

– мінімізувати.

Вибір саме останнього, найбільш оптимального у багатьох випадках способу обробки ризику передує розробці та впровадженню систем та засобів інформаційної безпеки. При цьому при виборі та реалізації конкретних заходів щодо забезпечення інформаційної безпеки активів слід керуватися доцільністю застосування цих заходів у контексті вирішуваного бізнес-завдання, вартості активу та величини прогнозованих збитків, а також потенційних витрат зловмисників. Відповідно до загальноприйнятого підходу,

Збитки від реалізації атаки можуть бути прямими чи непрямими. Прямий збиток – це безпосередні очевидні й легко прогнозовані втрати компанії, такі як втрати прав інтелектуальної власності, розголошення секретів виробництва, зниження вартості активів або їх часткове або повне руйнування, судові витрати

та виплата штрафів і компенсацій тощо. Непрямі збитки можуть означати якісні або непрямі втрати. Якісними втратами можуть бути призупинення або зниження ефективності діяльності компанії, втрата клієнтів, зниження якості вироблених товарів або послуг. Непрямі втрати – це недоотриманий прибуток, втрата ділової репутації, додатково понесені витрати.

Загроза безпеки інформації виникає за наявності наступних взаємопов'язаних **компонентів**:

– джерела загрози;
– уразливості активу;
– способу реалізації загрози;
– об'єкта впливу;
– шкідливого впливу.

Наведемо приклад: хакер (джерело загрози) атакує непропатчений веб-сервер компанії (уразливість активу) шляхом впровадження SQL-ін'єкції (спосіб реалізації загрози) в обслуговуючу цей веб-сервер СУБД (об'єкт впливу) і незаконно отримує конфіденційну інформацію (шкідливий вплив).

Далі ці компоненти загрози інформаційній безпеці будуть розглянуті докладніше.

1. Джерелом загрози можуть бути зовнішні або внутрішні (по відношенню до об'єкта захисту, що розглядається) порушники, треті особи, сили природи.

Зовнішні порушники не є співробітниками компанії, легітимними користувачами внутрішніх інформаційних систем, аутсорсерами, підрядниками, постачальниками, замовниками та іншими особами, пов'язаними юридичними відносинами з організацією, що розглядається. Такі порушники не мають легітимного доступу до об'єкта захисту (інформаційного активу) і класифікуються за їх навичками, можливостями та мотивацією.

Прикладами зовнішніх порушників можуть бути як проурядові хакери-експерти з державною фінансовою підтримкою або найняті конкурентами кіберзлочинці, так і хактивісти, професійні кібершахраї або навіть підлітки, озброєні широкодоступними програмами хакерів.

Заходами протидії зовнішнім порушникам є практично весь спектр «класичних» способів забезпечення інформаційної безпеки: розробка та впровадження внутрішніх регламентуючих документів, засобів захисту інформації, заходів активної протидії, реагування та розслідування кіберинцидентів тощо.

Організаціям слід проводити регулярну оцінку власної схильності до ризику атаки зовнішніх зловмисників, при якій потрібно враховувати сферу діяльності, залежність від інформаційних технологій, публічність, привабливість для атакуючих, широту охоплення потенційної атаки. Загалом, саме зовнішні порушники є непередбачуваним і безконтрольним фактором кіберризику, що вимагає реалізації найсучасніших заходів та способів захисту.

Внутрішніми порушниками можуть вважатися фізичні особи – співробітники та керівники компанії, а також юридичні особи, які мають договірні відносини з компанією. Внутрішні порушники класифікуються за

цілеспрямованістю та зловмисністю їх дій, а для здійснення цілеспрямованого несанкціонованого доступу у зловмисного інсайдера мають бути мотив, спосіб та відповідна можливість для атаки.

Постачальники послуг, обладнання або персоналу також несуть ризики інформаційної безпеки – відомі випадки, коли причинами витоків ставали постачальники IT-сервісів, виробники допоміжного обладнання та співробітники компанії-підрядника. Провайдери хмарних сервісів також потрапляють до категорії потенційних внутрішніх порушників, чому може свідчити велика кількість витоків даних із некоректно налаштованих хмарних сховищ.

Крім зовнішніх та внутрішніх порушників не варто забувати і про інші джерела загроз: ***треті особи та сили природи*** можуть вплинути на діяльність компанії.

Так, третіми особами вважатимуться органи структурі державної влади, наслідки від втручання у роботу підприємства може бути пропорційні з впливом стихійного лиха. Новини про проведення слідчих заходів можуть негативно позначитися на іміджі та репутації компанії, а винесений припис про призупинення діяльності на навіть відносно нетривалий термін може фактично означати відхід компанії з ринку. Такими ж наслідками можуть стати вилучення обладнання, опечатування серверних приміщень, арешт ключових керівників компанії. Заходами мінімізації ризиків, породжених впливом третіх осіб, мають бути як неухильне виконання всіх вимог чинного законодавства, і безперервні внутрішні compliance-перевірки. Зрештою, силами природи в контексті категоризації джерел загроз є стихійні лиха, такі як природні та техногенні катастрофи, а також соціальні катастрофи: епідемії, воєнні дії, теракти, революції, страйки та інші форс-мажори.

Для мінімізації ризиків даних пригод часто потрібні великі фінансові вкладення в системи забезпечення безперервності діяльності та відновлення працездатності, а також облік даних ризиків на початкових етапах розвитку компанії: слід ретельно вибирати місце розташування офісів з урахуванням місцевості, близькості інших установ та об'єктів інфраструктури, погодних умов, стану держави та соціуму, враховувати прогнози економічного та соціального розвитку конкретного регіону присутності. Крім мінімізації ризиків впливу стихійних лих описаними вище способами, компанії можуть вибрати ще один спосіб обробки даних ризиків – **страхування**. За продуманої та грамотно обраної схеми страхових виплат можна нівелювати збитки від впливу непереборних сил на бізнес. Однак, будь-якому керівнику та співробітнику завжди варто пам'ятати про те, що життя людини безцінне в порівнянні з навіть найприбутковішим бізнесом, тому за будь-яких обставин порятунок життів та здоров'я людей має бути першим пріоритетом.

2. Вразливість – це нестача засобів захисту інформаційної системи, який може бути використаний порушником (як зовнішнім, так і внутрішнім) для реалізації загроз інформаційній безпеці. Уразливості інформаційної системи можуть бути породжені як помилками під час створення, впровадження чи експлуатації системи, і слабкістю накладених захисних засобів і застосованих

заходів.

З логічної точки зору, не може існувати ідеально захищених та безпечних інформаційних систем, які при цьому не знаходяться в ізольованому просторі, а виконують свою бізнес-функцію, тому навіть у самій здавалося б надійній та перевіреній системі можуть виявитися вразливими.

Загальноприйнятим **способом розрахунку небезпеки вразливості у кількісному** вираженні є використання метрики **CVSS (Common Vulnerability Scoring System)** американського Національного інституту стандартів та технологій (NIST, National Institute of Standards and Technology). Дана метрика дозволяє описати основні особливості вразливості та кількісно оцінити її небезпеку (за шкалою від 0 до 10) залежно від складності експлуатації, впливу на властивості безпеки активу, наявності готового експлойту та його доступності для зловмисника, можливості усунути вразливість, рівня достовірності повідомлення про наявність вразливості, а також у прив'язці до конкретного середовища експлуатації вразливої системи.

Ідея централізовано реєструвати та класифікувати вразливості знайшла свою реалізацію у кількох офіційних реєстрах уразливостей, таких як **MITRE CVE (Common Vulnerabilities and Exposures)**, **NIST NVD (National Vulnerability Database), CERT/CC VND (Vulnerability Notes Database)**.

Реєстр CVE організації MITRE ведеться з 1999 року, і за цей час у ньому були збережені дані про більш ніж 115 тисяч вразливостей. Інформацію до цього реєстру вносять CNA (CVE Numbering Authorities) – зареєстровані організації (такі як державні CERT'и), компанії-виробники ПЗ, а також незалежні дослідники безпеки, які мають повноваження надавати виявленим уразливості ідентифікатор виду CVE-YYYY-NNNN, де YYY – Рік виявлення вразливості, а NNNN – її порядковий номер. На даний момент у списку CNA присутні 98 організацій та осіб.

Крім зазначених офіційних, існує і велика кількість альтернативних реєстрів уразливостей та експлойтів, які ведуться як розробниками ПЗ (наприклад, Microsoft, Cisco, Oracle, IBM, Red Hat, Ubuntu, VMware та інші), так і окремими організаціями та ентузіастами.

Причиною виникнення вразливості може бути помилка, допущена під час розробки або налаштування програмного забезпечення. **Американський Національний інститут стандартів та технологій класифікує 124 типи помилок у своєму переліку CWE (Common Weakness Enumeration)**. Більш того, для кожної з наведених помилок на сайті організації MITRE наведено її докладний опис з прикладами вразливого коду, вказівками щодо виявлення та усунення подібних помилок з прив'язкою до стадій розробки ПЗ, а також з посиланнями на зареєстровані вразливості CVE, які були викликані цією помилкою, і **шаблони атак CAPEC (Common Attack Pattern Enumeration and Classification)**, що пов'язують помилку і можливі атаки.

Для виявлення вразливостей можна застосовувати як автоматизовані системи (сканери вразливостей, системи управління конфігураціями та версіями), так і проводити оцінку захищеності та тести на проникнення, в результаті чого організація отримує інформацію про наявність вразливостей, що

потенційно експлуатуються. Однак потрібно пам'ятати, що кожен день з'являється в середньому кілька десятків нових вразливостей, так що епізодичним аналізом не варто обходитися, а варто вибудовувати безперервний процес управління вразливістю. У його рамках організації можуть циклічно проходити інвентаризацію, класифікацію та пріоритизацію активів, аналіз поточної захищеності, пошук уразливостей та їх обробку (усунення/мінімізація/ізоляція/прийняття) відповідно до їх критичності, подальшої перевірки та оцінки ефективності пройдених кроків.

3. Способи реалізації загроз також класифікуються. Проект **MITRE ATT&CK** є базою знань про способи реалізації загроз, розширюючи список методів до **тактик, технік та процедур (TTPs – Tactics, Techniques, Procedures)**, що застосовуються атакуючими. MITRE ATT&CK пов'язаний із класифікатором шаблонів атак MITRE CAPEC, про який ми говорили раніше. Для кожної з тактик атак наводиться перелік конкретних технік, які супроводжуються детальним технічним описом реалізації атаки, списком ПЗ, що використовується атакуючими, та ідентифікаторами конкретних кіберзлочинних угруповань, що використовують відповідно до свого «почерку» ті чи інші TTPs, за якими атаку можна атрибутувати для успішного протидії чи розслідування.

4. Об'єктами шкідливого впливу при атаці можуть бути всі активи компанії, як матеріальні, так і нематеріальні: люди, інформація, процеси розробки, виробництва та постачання, канали передачі даних, програмні та апаратні засоби та компоненти систем. При цьому слід пам'ятати, що саме люди – співробітники, керівники, аутсорсери – найчастіше найслабша ланка в системі забезпечення інформаційної безпеки компанії. Якщо технічні засоби захисту функціонують відповідно до закладених у них правил і для їх ефективної роботи достатньо зробити коректне налаштування, то для мінімізації «людського фактора» при кібератаках слід безперервно вести роз'яснювальну роботу з персоналом та проводити тренування та навчання, враховуючи психологічні та соціокультурні особливості поведінки співробітників.

5. Видами шкідливого впливу зазвичай є порушення **цілісності, конфіденційності, доступності** інформаційних ресурсів, а також атаки на **невідмовність, справжність, підзвітність** інформації.

Цікавими прикладами **порушення цілісності** можуть бути різноманітні способи маніпулювання та шахрайства з даними, такі як Data Diddling (приховане внесення некоректних змін до системи з метою збереження спотворених відомостей та отримання від цього фінансової вигоди надалі – наприклад, для маніпулювання фінансовою звітністю компанії та вартістю акцій), Salami Fraud (внесення великої кількості дуже малопомітних змін протягом тривалого часу, що в результаті призводить до значних наслідків – наприклад, списання 10 копійок з кожного банківського рахунку всіх клієнтів протягом року), «логічні бомби» (впровадження програмних закладок, що призводять до спотворення даних, що зберігаються/обробляються при настанні певних умов – наприклад,(несанкціоноване нарахування підвищених відсотків за вкладом певному співробітнику банку після його звільнення).

Порушення конфіденційності інформації загрожує не тільки очевидними наслідками в короткостроковій перспективі, наприклад, при виявленні персональних даних клієнтів у відкритому доступі, але й тим, що вкрадена інформація може несподівано «спливти» через кілька років після факту компрометації – наприклад, відомості, що ганьблять компанію або керівника бути розголошені напередодні IPO або призначення на нову посаду. Крадіжка ноу-хау компанії конкурентами може призвести не тільки до втрати конкурентних переваг і частки на ринку, але й до фактів здирництва з боку атакуючих конкурентів, що загрожують оприлюднити «сірі» способи ведення бізнесу компанією.

Атаки, внаслідок яких порушується **доступність інформації**, як правило, виявляються найлегшими для виявлення, одночасно є надзвичайно руйнівними з погляду здійснення операційної діяльності та збереження репутації. Прикладами можуть бути як гучні міжнародні епідемії WannaCry або NotPetya, так і DDoS-атаки на російські платіжні системи та банки. Організації та приватні особи також все частіше стикаються з вірусами-вимагачами, які стають небезпечнішими з року в рік і здатні призупинити функціонування цілих підприємств.

Описані вище сукупні компоненти загроз інформаційної безпеки (джерела, уразливості та способи реалізації загроз, об'єкти та види шкідливого впливу) можуть бути нейтралізовані **захисними заходами**, які традиційно поділяються на організаційні, технічні, фізичні та застосовуються до співробітників, процесів та технологій. **За метою** вживаних заходів існує поділ на наступні види заходів:

– запобіжні;
– директивні;
– превентивні;
– стримуючі;
– коригувальні;
– відновлювальні;
– розслідувальні;
– компенсуючі.

Основними міжнародними стандартами практичного забезпечення інформаційної безпеки є ISO/IEC 27001:2013 Information security management systems – Requirements («Системи управління інформаційної безпеки – Вимоги») та NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations («Міри забезпечення безпеки та конфіденційності для інформаційних систем та організацій»), які включають опис організаційних та технічних вимог для розробки цілісної системи забезпечення та управління інформаційною безпекою. Слід зазначити, що всі заходи захисту, описані в стандарті NIST SP 800-53, включають також і конкретні кроки з реалізації відповідного заходу, що робить цей документ набагато більш докладним, ніж стандарт ISO/IEC 27001:2013.

Впровадження різних технічних засобів захисту доцільно проводити тільки після проходження основних етапів побудови комплексної системи

управління інформаційною безпекою: розробки внутрішніх нормативних документів у галузі ризик-менеджменту та кібербезпеки, інвентаризації та класифікації активів, оцінки та аналізу ризиків, техніко-економічного обґрунтування впровадження конкретних типів засобів захисту. Слід також врахувати, що навіть найсучасніший і «просунутий» засіб вимагає тонкого налаштування для виконання захисних бізнес-функцій у конкретній компанії, тому для економічно ефективного використання потрібно спочатку виробити розуміння того, які саме ризики закриватиме та чи інша система кіберзахисту, а потім відповідним чином її налаштувати та безперервно підтримувати в актуальному стані.

На закінчення хотілося б ще раз відзначити, що розвиток і користь від застосування сучасних інформаційних технологій йдуть пліч-о-пліч з асоційованими з ними ризиками і погрозами. Тому впровадження інформаційних технологій, як будь-який новий проект, що несе у собі певну невідомість, слід поєднувати з аналізом та обробкою ризиків. Однак часто існує застарілий підхід, при якому питання забезпечення інформаційної безпеки розглядаються у відриві від бізнес-контексту, а також не поєднуються з управлінням ризиками. Тільки цілісне розуміння компонентів актуальних загроз інформаційній безпеці разом із застосуванням методик оцінки ризиків впровадження та експлуатації тих чи інших інформаційних систем,

13.2. Загрози цілісності

Цілісність даних (англ. *data integrity*) – підтримка та забезпечення точності та цілісності даних протягом всього життєвого циклу, що є критично важливим аспектом при проектуванні, впровадженні та експлуатації систем, які зберігають, обробляють та постачають дані. Термін має широке значення і може означати різне в залежності від контексту і розділу комп'ютерних наук (криптографія, теорія електричного зв'язку, теорія інформації, безпека).

Загрози цілісності (неправомірна зміна даних). Загрози порушення цілісності – це загрози, пов'язані з імовірністю модифікації тієї чи іншої інформації, що зберігається в інформаційній системі. Порушення цілісності може бути викликано різними чинниками – від умисних дій персоналу до виходу з ладу обладнання.

В телекомунікації цілісність даних часто перевіряють, використовуючи ґеш-суму повідомлення, обчислену алгоритмом MAC (Message authentication code).

У криптографії та інформаційній безпеці цілісність даних (в загальному) – це дані в тому вигляді, в якому вони були створені. Приклади порушень цілісності даних:

- спроба зловмисника змінити номер аккаунта в банківській транзакції, або спроба підробки документа;
- випадкове зміна інформації при передачі або при несправної роботі жорсткого диска;

– перекручування фактів засобами масової інформації з метою маніпуляції громадською думкою.

У теорії баз даних, цілісність даних означає коректність даних та їх несуперечність. Зазвичай вона також включає цілісність зв'язків, що виключає помилки зв'язків між первинним і вторинним ключем. Приміром, коли існують дочірні записи-сироти, які не мають зв'язку з батьківськими записами. Приклади порушень цілісності даних:

– існування записів-сиріт (дочірніх записів, які не мають зв'язку з батьківськими записами);

– існування однакових первинних ключів.

Для перевірки цілісності даних в криптографії використовуються ґеш-функції, наприклад, MD5. Ґеш-функція перетворює сукупність електронних даних довільного розміру в електронні данні фіксованого розміру (число). Якщо дані зміняться, то і число, що генерується ґеш-функцією, теж зміниться.

Цілісність даних – властивість, при виконанні якого дані зберігають заздалегідь певний вид і якість.

Методи забезпечення цілісності інформації

Методи і способи реалізації вимог, викладених у визначенні терміна, докладно описуються в рамках єдиної схеми забезпечення інформаційної безпеки об'єкта (захисту інформації).

Основними методами забезпечення цілісності інформації (даних) при зберіганні в автоматизованих системах є:

– забезпечення відмовостійкості (резервування, дублювання, дзеркалювання обладнання і даних, наприклад через використання RAID-масивів);

– забезпечення безпечного відновлення (резервне копіювання і електронне архівування інформації).

Одним з дієвих методів реалізації вимог цілісності інформації при її передачі по лініям зв'язку є **криптографічний захист інформації** (шифрування, ґешування, електронний цифровий підпис).

При комплексному підході до захисту бізнесу, напрям забезпечення цілісності та доступності інформації (ресурсів бізнес-процесів) переростає в план заходів, що спрямовані на забезпечення безперервності бізнесу.

Цілісність даних в криптографії

Шифрування даних саме по собі, не гарантує, що цілісність даних не буде порушена, тому в криптографії використовуються додаткові методи для гарантування цілісності даних. Під порушенням цілісності розуміється наступне:

– інверсія бітів;

– додавання нових бітів (зокрема абсолютно нових даних) третьою стороною;

– видалення яких-небудь бітів даних;

– зміна порядку слідування біт або груп біт.

У криптографії рішення задачі цілісності інформації передбачає застосування заходів, що дозволяють виявляти не стільки випадкові викривлення інформації, так як для цієї мети цілком підходять методи теорії кодування з виявленням і виправленням помилок, скільки цілеспрямоване зміна інформації активним криптоаналітиком. Процес контролю цілісності забезпечується введенням в передану інформацію надмірності. Це досягається додаванням до повідомлення деякої перевірочної комбінації. Така комбінація обчислюється згідно з певним алгоритмом і відіграє роль індикатора, за допомогою якого перевіряється цілісність повідомлення. Саме цей момент дає можливість перевірити, чи були змінені дані третьою стороною. Ймовірність того, що дані були змінені, служить мірою імітостійкості шифру.

Додаткову надлишкову інформацію, внесену до повідомлення, називають імітовставкою. Вироблятися імітовставка може як до початку, так і одночасно з шифруванням повідомлення.

Основні загрози цілісності

У більшості випадків винуватцями загроз цілісності є штатні співробітники організацій, добре знайомі з режимом роботи і заходами захисту. Це ще раз підтверджує небезпеку внутрішніх загроз, хоча говорять і пишуть про них значно менше, ніж про зовнішні.

З метою порушення **цілісності** зловмисник (як правило, штатний співробітник) може:

- ввести неправильні дані;
- змінити дані;
- знищити дані.

Іноді змінюються змістовні дані, іноді – службова інформація.

Потенційно уразливі з погляду порушення цілісності не тільки дані, але і програми. Впровадження шкідливого програмного забезпечення – приклад подібного порушення.

Загрозами **динамічної цілісності** є:

- порушення атомарності транзакцій,
- переупорядковування,
- крадіжка,
- дублювання даних або внесення додаткових повідомлень (мережевих пакетів і т.п.).

Відповідні дії в мережевому середовищі називаються активним прослуховуванням.

13.3. Загрози доступності

Доступність (англ. *Availability*) – властивість інформаційного ресурсу, яка полягає в тому, що користувач та/або процес, який володіє відповідними повноваженнями, може використовувати цей ресурс відповідно до правил, встановлених політикою безпеки не очікуючи довше заданого (прийнятного)

інтервалу часу.

Суть властивості полягає в тому, що потрібний інформаційний ресурс знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний.

Загрози доступності (здійснення дій, які унеможливлюють чи ускладнюють доступ до ресурсів інформаційної системи). Порушення доступності являє собою створення таких умов, при яких доступ до послуги або інформації або заблокований, або можливий за час, який не забезпечить виконання тих чи інших бізнес-цілей.

Основні загрози доступності

Загрози доступності класифікуються за компонентами інформаційних систем (ІС), на які спрямовані загрози:

- відмова користувачів;
- внутрішня відмова інформаційної системи;
- відмова інфраструктури, що підтримує ІС.

Стосовно **користувачів** розглядаються такі загрози:

- небажання працювати з інформаційною системою (найчастіше виявляється, коли необхідно освоювати нові можливості і в разі розбіжності між запитами користувачів і фактичними можливостями та технічними характеристиками);
- неможливість працювати із системою через відсутність відповідної підготовки (недолік загальної комп'ютерної освіти, невміння інтерпретувати діагностичні повідомлення, невміння працювати з документацією і т.п.);
- неможливість працювати із системою через відсутність технічної підтримки (неповнота документації, нестача довідкової інформації тощо).

Основними **джерелами внутрішніх відмов** є:

- порушення (випадкове або навмисне) правил експлуатації;
- вихід системи зі штатного режиму експлуатації;
- помилки при (пере)конфігурації системи;
- відмови програмного і апаратного забезпечення.

Як засіб виведення системи зі штатного режиму експлуатації може використовуватися агресивне споживання ресурсів (звичайно – смуги пропускання мереж, обчислювальних можливостей процесорів або оперативної пам'яті). Для виведення систем з штатного режиму експлуатації можуть використовуватися вразливі місця у вигляді програмних і апаратних помилок.

При прорахунках у конфігурації системи локальна програма здатна практично монополізувати процесор та/або фізичну пам'ять, звівши швидкість виконання інших програм до нуля. Простий приклад віддаленого споживання ресурсів – атака, що одержала найменування "SYN-повінь". Вона є спробою переповнити таблицю "напіввідкритих" TCP-з'єднань сервера (встановлення з'єднань починається, але не закінчується). Така атака щонайменше утрудняє встановлення нових з'єднань з боку легальних користувачів, тобто сервер виглядає як недоступний. По відношенню до атаки "Papa Smurf" уразливі мережі, що сприймають ping-пакети з широкомовними адресами. Відповіді на

такі пакети “з’їдають” смугу пропускання. Програма “Teardrop” видалено “підвішує” комп’ютери, експлуатуючи помилку в збірці фрагментованих IP-пакетів.

Віддалене споживання ресурсів останнім часом спостерігається в особливо небезпечній формі – як скоординовані розподілені атаки, коли на сервер з безлічі різних адрес з максимальною швидкістю прямують цілком легальні запити на з’єднання та/або обслуговування. Відзначимо, що якщо має місце архітектурний прорахунок у вигляді розбалансованості між пропускною спроможністю мережі і продуктивністю сервера, то захиститися від розподілених атак на доступність украй важко.

Відмови програмного забезпечення часто провокуються впровадженням в ІС так званого **шкідливого програмного забезпечення**, дії якого спрямовані на:

- руйнування даних;
- руйнування або пошкодження апаратури (носіїв даних).

Таке пошкодження може викликатися як природними причинами так і штучними. На жаль, джерела безперебійного живлення, що знаходяться в масовому використанні, не захищають від потужних короткочасних імпульсів (наприклад, блискавок), і випадки вигорання устаткування – не рідкість. Потужній короткочасний імпульс, здатний зруйнувати дані на магнітних носіях, можна згенерувати і штучним чином – за допомогою так званих високоенергетичних радіочастотних гармат. Однак, в наших умовах подібну загрозу слід все ж таки визнати надуманою.

Стосовно **інфраструктури** рекомендується розглядати такі загрози:

- порушення роботи (випадкове або навмисне) систем зв’язку, електроживлення, водо– і/або теплопостачання, кондиціонування;
- руйнування або пошкодження приміщень;
- неможливість або небажання обслуговуючого персоналу і/або користувачів виконувати свої обов’язки (цивільні безлади, аварії на транспорті, терористичний акт або його загроза, страйк тощо).

13.4. Загрози конфіденційності.

Конфіденційність (англ. *confidentiality*) – властивість, яка не підлягає розголосові; довірливість, секретність, суто приватність.

Конфіденційність адміністративна [mandatory confidentiality] – послуга безпеки, що забезпечує конфіденційність інформації відповідно до принципів керування доступом адміністративного.

Конфіденційність довірча [discretionary confidentiality] – послуга безпеки, що забезпечує конфіденційність інформації відповідно до принципів керування доступом довірчого.

Конфіденційність інформації [information confidentiality] – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і (або) процесом. Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею.

Загрози конфіденційності (неправомірний доступ до інформації). Загроза порушення конфіденційності полягає в тому, що інформація стає відомою тому, хто не володіє повноваженнями доступу до неї. Вона має місце, коли отримано доступ до деякої інформації обмеженого доступу, що зберігається в комп'ютерній системі або передається від однієї системи до іншої. У зв'язку з загрозою порушення конфіденційності, використовується термін «витік». Подібні загрози можуть виникати внаслідок «людського фактора» (наприклад, випадкове делегування тому або іншому користувачеві привілеїв іншого користувача), збоїв роботи програмних та апаратних засобів. До інформації обмеженого доступу належить державна таємниця (комерційна таємниця, персональні дані, професійні види таємниці: лікарська, адвокатська, банківська, службова, нотаріальна таємниця страхування, слідства й судочинства, листування, телефонних переговорів, поштових відправлень, телеграфних або інших повідомлень (таємниця), відомості про сутність винаходу, корисної моделі або промислового зразка до офіційної публікації (ноу-хау) та ін).

Основні загрози конфіденційності

У загальному випадку, конфіденційну інформацію можна поділити на **службову** та **предметну**.

Службова інформація (наприклад, паролі користувачів) не належить певній предметній галузі, в ІС вона грає технічну роль, але її розкриття особливо небезпечно, оскільки воно може забезпечити несанкціонований доступ до всієї інформації, зокрема предметної.

Навіть якщо інформація зберігається в комп’ютері або призначена для комп’ютерного використання, загрози її конфіденційності можуть носити некомп'ютерний і взагалі нетехнічний характер.

Багатьом людям доводиться бути користувачами не одного, а кількох інформаційних сервісів. Якщо для доступу до таких систем використовуються **багаторазові паролі** або інша конфіденційна інформація, то напевно ці дані зберігатимуться не тільки в голові, але і в записнику або на папері, які користувач часто залишає на робочому столі, а то і просто губить. І справа тут не в неорганізованості людей, а в початковій непридатності парольної схеми. Неможливо пам’ятати багато різних паролів. Рекомендації щодо їх регулярної зміни тільки погіршують стан, змушуючи застосовувати нескладні схеми чергування, або взагалі прагнути звести справу до паролів, що легко запам’ятовуються і вгадуються.

Описаний клас вразливих місць можна назвати **розміщенням конфіденційних даних у середовищі, де їм не забезпечено (часто – і не може бути забезпечено) необхідний захист**. Загроза ж полягає в тому, що хтось не відмовиться дізнатися секрети, які самі просяться в руки. Крім паролів, що зберігаються в записниках користувачів, до цього класу потрапляє передача конфіденційних даних у відкритому вигляді (у розмові, в листі, мережею), яка робить можливим перехоплення даних. Для атаки можуть використовуватися різні технічні засоби (підслуховування або прослуховування розмов, пасивне прослуховування мережі і т.п.), але ідея одна – здійснити доступ до даних у той

час, коли вони найменше захищені.

Вельми небезпечною загрозою є **виставки**, на які багато організацій відправляють устаткування з виробничої мережі, з усіма збереженими на них даними, залишаючи тим самим паролі. При віддаленому доступі вони продовжують передаватися у відкритому вигляді. Це погано навіть в межах захищеної мережі організації, а в об'єднаній мережі виставки – це дуже суворе випробування чесності всіх учасників.

Ще один приклад загрози, про яку часто забувають, – зберігання даних **на резервних носіях**. Для захисту даних на основних носіях застосовуються розвинені системи управління доступом, тоді як копії нерідко просто лежать у шафах і дістати доступ до них може багато хто.

Перехоплення даних – дуже серйозна загроза, і якщо конфіденційність дійсно є критичною, а дані передаються багатьма каналами, їх захист може виявитися достатньо складним і дорогим. Технічні засоби перехоплення доступні, прості в експлуатації, а встановити їх, наприклад на кабельну мережу, може хто завгодно, тому цю загрозу потрібно брати до уваги стосовно не тільки зовнішніх, а й внутрішніх комунікацій.

Крадіжки устаткування є загрозою не тільки для резервних носіїв, але і для комп'ютерів, особливо портативних. Часто ноутбуки залишають без нагляду на роботі або в автомобілі, іноді просто гублять.

Небезпечною нетехнічною загрозою конфіденційності є методи **соціальної інженерії**, такі як **маскарад** – виконання дій під виглядом особи, що володіє повноваженнями для доступу до даних.

До неприємних загроз, від яких важко захищатися, можна віднести **зловживання повноваженнями**. На багатьох типах систем привілейований користувач (наприклад системний адміністратор) здатний прочитати будь-який (незашифрований) файл, дістати доступ до пошти будь-якого користувача і т.д.

Інший приклад – нанесення збитку при сервісному обслуговуванні. Звичайно сервісний інженер дістає необмежений доступ до устаткування і має можливість діяти в обхід програмних захисних механізмів.

Такі основні загрози, які завдають найбільшого збитку суб'єктам інформаційних відносин.

13.5. Загрози автентичності

Автентифіка́ція – процедура встановлення належності користувачеві інформації в системі пред'явленого ним ідентифікатора. З позицій інформаційної безпеки автентифікація є частиною процедури надання доступу для роботи в інформаційній системі, наступною після ідентифікації і передує авторизації.

Існують наступні визначення автентичності згідно стандартів NIST:

– Властивість того, що дані походять із передбачуваного джерела, згідно NIST SP 800-38 та NIST SP 800-63-3.

– Властивість бути справжнім, бути перевіреним і довіряти; впевненість у дійсності передачі, повідомлення або автора повідомлення, згідно NIST SP 800-30, NIST SP 800-37, NIST SP 800-39, NIST SP 800-53, NIST SP 800-60,

NIST SP 800-137.

5 поширених типів автентифікації

Кіберзлочинці завжди вдосконалюють свої атаки. У результаті групи безпеки стикаються з багатьма проблемами, пов'язаними з автентифікацією. Ось чому компанії починають впроваджувати більш складні стратегії реагування на інциденти, включаючи автентифікацію як частину процесу. У наведеному нижче списку розглядаються деякі поширені методи автентифікації, які використовуються для захисту сучасних систем.

1. Автентифікація на основі пароля

Паролі є найпоширенішими методами автентифікації. Паролі можуть бути у вигляді рядка літер, цифр або спеціальних символів. Щоб захистити себе, вам потрібно створити надійні паролі, які містять комбінацію всіх можливих варіантів.

Однак паролі схильні до фішингових атак і поганої гігієни, що послаблює ефективність. Середня людина має близько 25 різних облікових записів в Інтернеті, але лише 54% користувачів використовують різні паролі для своїх облікових записів.

Правда полягає в тому, що паролів потрібно запам'ятати багато. У результаті багато людей обирають зручність, а не безпеку. Більшість людей використовують прості паролі замість створення надійних, оскільки їх легше запам'ятати.

Суть полягає в тому, що паролі мають багато недоліків і недостатні для захисту інформації в Інтернеті. Хакери можуть легко вгадати облікові дані користувача, переглядаючи всі можливі комбінації, поки не знайдуть збіг.

2. Багатофакторна автентифікація

Багатофакторна автентифікація (MFA) – це метод автентифікації, який вимагає двох або більше незалежних способів ідентифікації користувача. Приклади включають коди, згенеровані зі смартфона користувача, тести Captcha, відбитки пальців, голосові біометричні дані або розпізнавання обличчя.

Методи та технології автентифікації MFA підвищують довіру користувачів, додаючи кілька рівнів безпеки. MFA може бути гарним захистом від більшості зломів облікових записів, але він має свої підводні камені. Люди можуть втратити свої телефони або SIM-карти і не зможуть згенерувати код автентифікації.

3. Автентифікація на основі сертифіката

Технології автентифікації на основі сертифікатів ідентифікують користувачів, машини чи пристрої за допомогою цифрових сертифікатів. Цифровий сертифікат – це електронний документ, створений за ідеєю водійського посвідчення чи паспорта.

Сертифікат містить цифрову ідентифікацію користувача, включаючи відкритий ключ, і цифровий підпис центру сертифікації. Цифрові сертифікати підтверджують право власності на відкритий ключ і видаються тільки центром сертифікації. Користувачі надають свої цифрові сертифікати під час входу на сервер. Сервер перевіряє достовірність цифрового підпису та центру сертифікації. Потім сервер використовує криптографію, щоб підтвердити, що

користувач має правильний закритий ключ, пов'язаний із сертифікатом.

4. Біометрична автентифікація

Біометрична автентифікація – це процес безпеки, який базується на унікальних біологічних характеристиках людини. Ось основні переваги використання технологій біометричної автентифікації:

– Біологічні характеристики можна легко порівняти з авторизованими характеристиками, збереженими в базі даних.

– Біометрична автентифікація може контролювати фізичний доступ, якщо вона встановлена на воротах і дверях.

– Ви можете додати біометричні дані в процес багатофакторної автентифікації.

Технології біометричної автентифікації використовуються споживачами, урядами та приватними корпораціями, включаючи аеропорти, військові бази та національні кордони. Ця технологія набуває все більшого поширення завдяки можливості досягти високого рівня безпеки, не створюючи тертя для користувача. Загальні методи біометричної автентифікації включають:

– **Розпізнавання обличчя** – зіставляє різні характеристики обличчя особи, яка намагається отримати доступ до затвердженого обличчя, яке зберігається в базі даних. Розпізнавання облич може бути непослідовним під час порівняння облич під різними кутами або порівняння людей, які виглядають схожими, наприклад, близьких родичів. Жвавість обличчя, як пасивна жвавість, запобігає підробці.

– **Сканери відбитків пальців** – зіставте унікальні візерунки на відбитках пальців людини. Деякі нові версії сканерів відбитків пальців можуть навіть оцінювати судинні малюнки на пальцях людей. Сканери відбитків пальців наразі є найпопулярнішою біометричною технологією для повсякденних споживачів, незважаючи на їх часті неточності. Таку популярність можна віднести до iPhone.

– **Розпізнавання мовця** – також відоме як біометрія голосу, вивчає шаблони мовлення мовця для формування певних форм і звукових якостей. Пристрій із захистом голосу зазвичай покладається на стандартні слова для ідентифікації користувачів, як і пароль.

– **Сканери очей** – включають такі технології, як розпізнавання райдужної оболонки ока та сканери сітківки ока. Сканери райдужної оболонки проектують яскраве світло в око та шукають унікальні візерунки в кольоровому кільці навколо зіниці ока. Потім шаблони порівнюються із затвердженою інформацією, що зберігається в базі даних. Автентифікація на основі ока може мати неточності, якщо людина носить окуляри або контактні лінзи.

5. Автентифікація на основі маркерів

Технології автентифікації на основі токенів дозволяють користувачам вводити свої облікові дані один раз і отримувати натомість унікальний зашифрований рядок випадкових символів. Потім ви можете використовувати маркер для доступу до захищених систем замість того, щоб знову вводити свої облікові дані. Цифровий маркер підтверджує, що ви вже маєте дозвіл на доступ. Варіанти використання автентифікації на основі маркерів включають RESTful API, які використовуються кількома фреймворками та клієнтами.

Атаки на автентифікацію

На даний час виявлені наступні атаки на автентифікацію:

1. Клонування або запозичення «Shoulder Surfing».
2. Sniff the credentials (шукати облікові дані).
3. Метод проб і помилок.
4. Атака на відмову в обслуговуванні (DoS, DDoS).
5. Отримати з резервної копії.
6. Атаки на автентифікацію користувача веб-сайту.
7. Атаки на паролі (Фішинг; Атака «людина посередині; Атака грубою силою; Додавання облікових даних; Кейлоггери).
8. Слабкі облікові дані для входу.
9. Перерахування імен користувачів.
10. Базова автентифікація HTTP.
11. Погане керування сеансами.
12. Залишення в системі.
13. SQL ін'єкція.
14. Небезпечна зміна та відновлення пароля.
15. Помилка двофакторної автентифікації.
16. Вразлива логіка автентифікації
17. Людська недбалість

Розглянемо їх більш детально:

1. Клонування або запозичення «Shoulder Surfing» – це атака, яка зазвичай виконується шляхом перегляду через плече або пошуку облікових даних для входу та використання їх для входу.

2. Sniff the credentials (шукати облікові дані) – це метод, який фіксує облікові дані під час їх передачі в процес входу. Збираємо пакети через wireshark або подібне програмне забезпечення для аналізу пакетів і шукаємо паролі та токени.

3. Метод проб і помилок – ця атака просто пробує різні комбінації, поки зловмисник не отримає одне право, щоб мати можливість увійти.

4. Атака на відмову в обслуговуванні (DoS, DDoS) – полягає в тому, що зловмисник може пошкодити систему, що заблокує оцінку системи іншими, тобто перевантаження системи для блокування користувача, запобігання доступу до системи.

5. Отримати з резервної копії – це можливість отримати інформацію про вхід із резервної копії на жорсткому диску та використовувати інформацію для входу, щоб отримати доступ до облікового запису.

6. Атаки на автентифікацію користувача веб-сайту.

Цей тип атаки спрямований і намагається використати процес автентифікації, який веб-сайт використовує для перевірки ідентичності користувача, служби чи програми.

Таблиця 13.1 – Атаки автентифікації користувача веб-сайту

Типи атак	Опис атаки
Груба сила	Дозволяє зловмиснику вгадати ім’я користувача, пароль, номер кредитної картки або криптографічний ключ за допомогою автоматизованого процесу проб і помилок.
Недостатня автентифікація	Дозволяє зловмиснику отримати доступ до веб-сайту, що містить конфіденційний вміст або функції, без належної автентифікації на веб-сайті.
Слабка перевірка відновлення пароля	Дозволяє зловмиснику отримати доступ до веб-сайту, який надає йому можливість незаконно отримати, змінити або відновити пароль іншого користувача.

Сигнатури, викликані цією атакою

Таблиця 13.2 – Сигнатури, викликані атаками автентифікації, включають:

Ім'я підпису	Опис
HTTP_Auth_ContainsBinary	Шукає автентифікацію HTTP, яка містить двійкові дані.
HTTP_Auth_TooLong	Виявляє рядок авторизації HTTP, який довший за настроюване системою значення максимальної довжини авторизації HTTP. Цей підпис замінює HTTP_NS_Admin_Overflow.
HTTP_Authentication	Виявляє базову автентифікацію HTTP на веб-сервері та реєструє імена користувачів і паролі. Ця подія безпеки класифікується як подія аудиту. Це не обов’язково вказує на атаку чи загрозу у вашій мережі.
HTTP_Authentication_Format_String	Виявляє атаку на рядок формату базової автентифікації HTTP в іменах користувачів і паролях.
HTTP_IIS_Hit_Highlighting_Auth_ Bypass	Шукає спроби обійти обмеження безпеки за допомогою вразливості у функціях підсвічування звернень сервера Microsoft IIS.
HTTP_Login_Known_User	Визначає ім’я для входу та зіставляє його з визначеними користувачем іменами для входу для добре відомих імен для входу.
HTTPS_ClearText_Session	Виявляє дійсний запит HTTP та відповідь на порт 443, який не зашифровано.

7. Атаки на паролі

Атаки на паролі є однією з найпоширеніших форм зламу корпоративних і особистих даних. Атака на пароль – це просто спроба хакера викрасти ваш пароль. 81% витоків даних було спричинено скомпрометованими обліковими даними. Оскільки паролі можуть містити невелику кількість літер і цифр, паролі стають менш безпечними. Хакери знають, що багато паролів розроблено погано, тому атаки на паролі залишатимуться методом атаки, доки паролі використовуються.

Захистіть себе від атак на пароль за допомогою наведеної нижче інформації.

7.1. Фішинг

Фішинг – це коли хакер, видаючи себе за надійну сторону, надсилає вам шахрайський електронний лист, сподіваючись, що ви добровільно розкриєте свою особисту інформацію. Іноді вони призводять вас до підроблених екранів «скинути пароль»; в інших випадках посилання встановлюють шкідливий код на ваш пристрій. Ми висвітлюємо кілька прикладів у блозі OneLogin.

Ось кілька прикладів фішингу:

– Ви отримуєте електронний лист від щось схоже на goodwebsite.com із проханням скинути пароль, але ви не читали уважно, а насправді це goodwobsite.com. Ви «скидаєте свій пароль», і хакер викрадає ваші облікові дані.

– Хакер націлює вас саме на електронну пошту, яка нібито надійшла від друга, колеги чи партнера. Він має коротку загальну анонсу («Перегляньте рахунок-фактуру, який я долучив, і дайте мені знати, чи це має сенс») і сподівається, що ви клацнете зловмисне вкладення.

– Ви отримуєте текстове повідомлення (SMS-фішинг або смішинг) або телефонний дзвінок (голосовий фішинг або вішинг) від хакера, який повідомляє вам, що ваш обліковий запис заморожено або що виявлено шахрайство. Ви вводите дані свого облікового запису, і хакер їх краде.

– Ви або ваша організація отримуєте електронний лист нібито від високопоставленої особи у вашій компанії. Ви не виконуєте домашнє завдання щодо правдивості електронної пошти та не надсилаєте конфіденційну інформацію хакеру.

Щоб уникнути фішингових атак, виконайте такі дії:

– **Перевірте, хто надіслав електронний лист**: подивіться на рядок «Від:» у кожному електронному листі, щоб переконатися, що особа, за яку себе видають, відповідає адресі електронної пошти, яку ви очікуєте.

– **Ще раз перевірте джерело**: якщо ви сумніваєтеся, зв’яжіться з особою, від якої надійшов електронний лист, і переконайтеся, що він був відправником.

– **Зверніться до своєї IT-команди**: IT-відділ вашої організації часто може сказати вам, чи електронний лист, який ви отримали, є законним.

7.2. Атака «людина посередині».

Атаки типу «людина посередині» (MitM) – це випадки, коли хакер або скомпрометована система сидить між двома нескомпрометованими людьми чи системами та розшифровує інформацію, яку вони передають один одному,

зокрема паролі. Якщо Аліса та Боб передають нотатки в класі, але Джеремі має передати ці нотатки, Джеремі має можливість бути людиною посередині. Подібним чином у 2017 році Equifax видалив свої програми з App Store і Google Play, оскільки вони передавали конфіденційні дані через незахищені канали, де хакери могли викрасти інформацію про клієнтів.

Щоб запобігти атакам типу "людина посередині":

– **Увімкніть шифрування на маршрутизаторі.** Якщо до вашого модему та маршрутизатора може отримати доступ будь-хто з вулиці, він може використовувати технологію «аналізатора», щоб побачити інформацію, яка передається через нього.

– **Використовуйте надійні облікові дані та двофакторну автентифікацію.** Багато облікових даних маршрутизатора ніколи не змінюються з імені користувача та пароля за замовчуванням. Якщо хакер отримує доступ до адміністрування вашого маршрутизатора, він може перенаправити весь ваш трафік на свої зламані сервери.

– **Використовуйте VPN.** Захищена віртуальна приватна мережа (VPN) допоможе запобігти атакам типу "людина посередині", гарантуючи, що всі сервери, на які ви надсилаєте дані, є надійними.

7.3. Атака грубою силою

Якщо пароль еквівалентний використанню ключа, щоб відкрити двері, атака грубою силою – це використання тарану. Хакер може спробувати 2,18 трильйона комбінацій пароля/імена користувача за 22 секунди, і якщо ваш пароль простий, ваш обліковий запис може опинитися під прицілом.

Атака грубої сили, наприклад атака за словником, – це спроба отримати незаконний доступ до системи або облікового запису користувача шляхом введення великої кількості випадково згенерованих або попередньо згенерованих комбінацій імен користувачів і паролів, доки не буде знайдено те, що працює.

Якщо є помилкова система захисту від грубої сили, наприклад помилка в логіці автентифікації, брандмауері або протоколі захищеної оболонки (SSH), зловмисники можуть викрасти облікові дані та процеси для входу, ставлячи під загрозу безпеку облікових даних користувача.

Щоб запобігти атакам грубої сили:

– Використовуйте складний пароль. Різниця між шестизначним паролем, що складається лише з малих літер, і десятизначним паролем із змішаним регістром, із змішаними символами, величезна. Зі збільшенням складності вашого пароля ймовірність успішної атаки грубою силою зменшується.

– Увімкніть і налаштуйте віддалений доступ. Запитайте у відділі IT, чи використовує ваша компанія керування віддаленим доступом. Такий інструмент керування доступом, як OneLogin, зменшить ризик атаки методом грубої сили.

– Потрібна багатофакторна автентифікація. Якщо у вашому обліковому записі ввімкнено багатофакторну автентифікацію (MFA), потенційний хакер може надіслати запит на доступ до вашого облікового запису лише другому фактору. Імовірно, хакери не матимуть доступу до вашого мобільного пристрою чи відбитка пальця, а це означає, що вони будуть заблоковані у вашому

обліковому записі.

7.4. Атака за словником

Тип атаки грубої сили, атаки за словником покладаються на нашу звичку вибирати «основні» слова як наш пароль, найпоширеніші з яких хакери зібрали в «злом словників». Більш складні словникові атаки включають слова, важливі для вас особисто, як-от місце народження, ім'я дитини чи ім'я домашньої тварини.

Щоб запобігти атаці за словником:

– Ніколи не використовуйте слова зі словника як пароль. Якщо ви прочитали це в книзі, воно ніколи не повинно бути частиною вашого пароля. Якщо вам потрібно використовувати пароль замість інструменту керування доступом, розгляньте можливість використання системи керування паролями.

– Блокування облікових записів після багатьох невдалих паролів. Блокування облікового запису може викликати розчарування, коли ви на короткий час забули пароль, але альтернативою часто є незахищеність облікового запису. Зробіть п'ять або менше спроб, перш ніж ваша програма повідомить вам заспокоїтися.

– Розгляньте можливість інвестування в менеджер паролів. Менеджери паролів автоматично генерують складні паролі, які допомагають запобігти словниковим атакам.

7.5. Додавання облікових даних

Якщо вас раніше зламували, ви знаєте, що ваші старі паролі, ймовірно, просочилися на поганий веб-сайт. Додавання облікових даних використовує облікові записи, паролі яких ніколи не змінювалися після злому. Хакери спробують різні комбінації колишніх імен користувачів і паролів, сподіваючись, що жертва ніколи їх не змінила.

Щоб запобігти надходженню облікових даних:

– Контролюйте свої облікові записи. Існують платні служби, які відстежуватимуть ваші ідентифікаційні дані в Інтернеті, але ви також можете скористатися безкоштовними службами, як-от haveIbeenpwned.com, щоб перевірити, чи пов'язана ваша адреса електронної пошти з нещодавніми витоками.

– Регулярно змінюйте свої паролі. Чим довше один пароль залишається незмінним, тим більша ймовірність того, що хакер знайде спосіб його зламати.

– Використовуйте менеджер паролів. Подібно до атаки за словником, багатьох атак із підкиданням облікових даних можна уникнути, маючи надійний і безпечний пароль. Менеджер паролів допомагає підтримувати їх.

7.6. Кейлоггери

Клавіатурні шпигуни – це тип шкідливого програмного забезпечення, призначеного для відстеження кожного натискання клавіш і звітування про це хакеру. Як правило, користувач завантажує програмне забезпечення, вважаючи його законним, лише для того, щоб установити кейлоггер без попередження.

Щоб захистити себе від кейлоггерів:

– Перевірте своє фізичне обладнання. Якщо хтось має доступ до вашої робочої станції, він може встановити апаратний кейлоггер для збору інформації

про натискання клавіш. Регулярно перевіряйте свій комп'ютер і територію навколо, щоб переконатися, що знаєте кожну частину апаратного забезпечення.

– Запустіть перевірку на віруси. Використовуйте перевірене антивірусне програмне забезпечення для регулярного сканування комп'ютера. Антивірусні компанії зберігають свої записи про найпоширеніші кейлоггери шкідливих програм і позначають їх як небезпечні.

Запобігання атакам на пароль

Найкращий спосіб усунути атаку на пароль – це уникати її. Запитайте свого IT-фахівця про проактивне інвестування в загальну політику безпеки, яка включає:

– **Багатофакторна автентифікація.** Використання фізичного токена (наприклад, Yubikey) або персонального пристрою (наприклад, мобільного телефону) для автентифікації користувачів гарантує, що паролі не є єдиними воротами для доступу.

– **Віддалений доступ.** Використання розумної платформи віддаленого доступу, як-от OneLogin, означає, що окремі веб-сайти більше не є джерелом довіри користувачів. Натомість OneLogin гарантує, що особу користувача підтверджено, а потім здійснює вхід.

– **Біометрія.** Зловмиснику буде дуже важко відтворити ваш відбиток пальця чи форму обличчя. Увімкнення біометричної автентифікації перетворює ваш пароль лише на одну з кількох точок довіри, які хакер повинен подолати.

8. Слабкі облікові дані для входу

Коли користувачі реєструються для облікового запису на сайті або в програмі, яка використовує вхід на основі пароля, їм пропонується створити ім'я користувача та пароль.

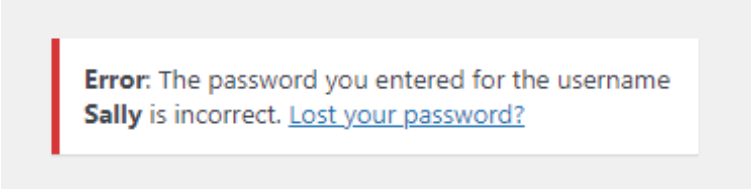
Однак якщо пароль передбачуваний, це може призвести до вразливості в процесі автентифікації. Передбачувані імена користувачів можуть полегшити зловмисникам націлювання на конкретних користувачів.

Замість того, щоб використовувати повну атаку грубої сили, зловмисники шукатимуть облікові записи з паролями, які легко вгадати, які використовуються занадто часто.. Вони спробують ввести такі звичайні облікові дані, як «admin», «admin1» і «password1». Без обмежень на слабкі паролі навіть сайти, захищені від атак грубої сили, можуть виявитися скомпрометованими.

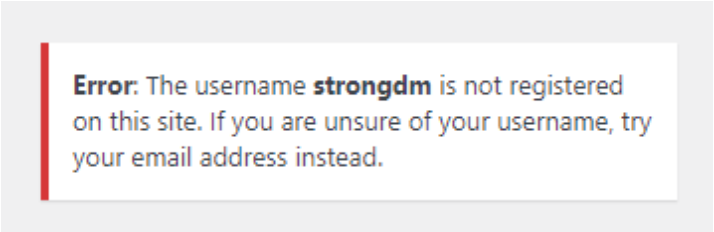
9. Перерахування імен користувачів

Перерахування імен користувачів не є точною вразливістю автентифікації. Але це може полегшити життя зловмисника, знизивши вартість інших атак, таких як атаки грубої сили або слабкі перевірки облікових даних.

Цей процес нумерації імені користувача підтверджує, чи дійсне ім'я користувача. Наприклад:



У цьому випадку ім'я користувача правильне, а пароль – ні.



Тут ім’я користувача недійсне.

Проблема з нумерацією імен користувачів полягає в тому, що зловмисники можуть визначити, які імена користувачів дійсні. Потім вони можуть спробувати зламати дійсні облікові записи користувачів за допомогою методів грубої сили, не витрачаючи час і гроші на тестування безлічі недійсних імен облікових записів.

10. Базова автентифікація HTTP

Цей класичний протокол веб-автентифікації простий у застосуванні, однак він не позбавлений ризиків.

Базова автентифікація HTTP проста: під час кожного запиту надсилаються ім’я користувача та пароль. Однак якщо відповідні протоколи безпеки, такі як шифрування сеансу TLS, не використовуються для зв’язку, інформація про ім’я користувача та пароль може бути надіслана відкрито, що полегшить зловмисникам викрадення облікових даних.

Оскільки включені облікові дані містять дуже мало контексту, їх можна легко використати в атаках, таких як підробка міжсайтових запитів (CSRF). Крім того, оскільки вони додаються до кожного окремого запиту, сучасні браузери зазвичай кешують цю інформацію на невизначений термін, з мінімальною можливістю «вийти» та запобігти повторному використанню облікових даних локальним зловмисником у майбутньому.

11. Погане керування сеансами

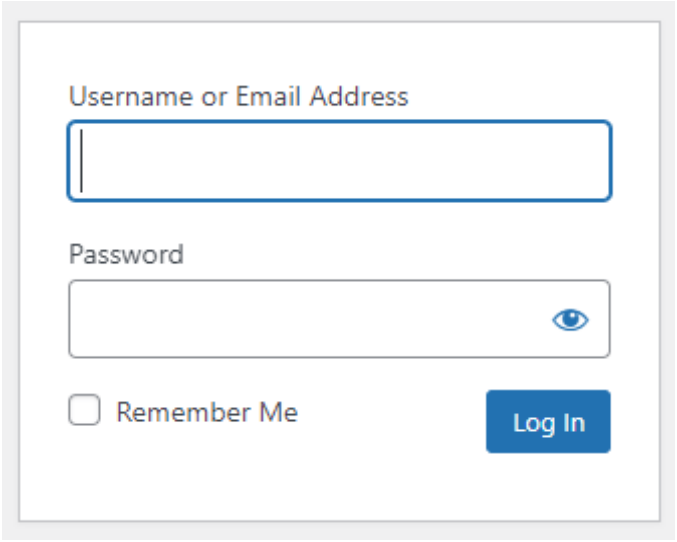
Уразливість в управлінні ідентифікаторами сеансів призводить до викрадення дійсних автентифікованих сеансів. Це одна з поширених веб-уразливостей для обходу паролів.

Існує кілька вразливостей, пов’язаних із неправильним керуванням сеансом, наприклад відсутність тайм-аутів сеансу, виявлення ідентифікаторів сеансу в URL-адресах, файли cookie сеансу без установленого прапорця «Лише Http» і погане визнання сеансу недійсним.

Якщо зловмисники можуть захопити контроль над існуючим сеансом, вони легко проникають у систему, припускаючи особу вже автентифікованого користувача, повністю минаючи процес автентифікації.

12. Залишення в системі

Прапорець «Запам’ятати мене» або «Залишати мене в системі» під формою входу дозволяє надзвичайно легко залишатися в системі після закриття сеансу. Він генерує файл cookie, який дозволяє вам пропустити процес входу.



Однак це може призвести до вразливості автентифікації на основі файлів cookie, якщо зловмисник може передбачити файл cookie або визначити шаблон його створення. Вони можуть використовувати такі зловмисні методи, як атаки грубої сили, щоб передбачити файли cookie, і міжсайтовий сценарій (XSS) для злому облікових записів користувачів, дозволяючи зловмисному серверу використовувати законний файл cookie.

Якщо файл cookie погано розроблений або захищений, зловмисники можуть отримати паролі або інші конфіденційні (і захищені законом) дані, такі як адреси користувачів або дані облікового запису, із збережених файлів cookie.

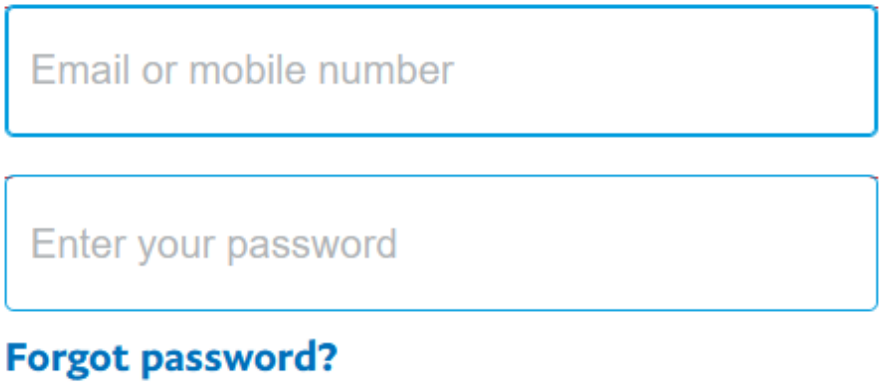
13. SQL-ін'єкція

SQL-ін’єкція – це вектор атаки, який неочікуваним чином використовує зловмисний код SQL для маніпулювання та доступу до бази даних.

Ін’єкції SQL можуть уможливити атаки на механізми автентифікації шляхом викрадення відповідних даних (наприклад, погано захищених ґешів паролів) із незахищеної бази даних. Вони також можуть обійти механізми автентифікації, якщо впроваджений код SQL виконується внутрішнім (і вже авторизованим) інструментом, який не зміг достатньо перевірити зовнішній вхід.

14. Небезпечна зміна та відновлення пароля

Іноді користувачі забувають або просто хочуть змінити свої паролі та натискають посилання «Забули пароль» або «Забули пароль».



Процес скидання пароля створює вразливість автентифікації, якщо програма використовує слабкий механізм відновлення пароля, як-от прості контрольні запитання, відсутність CAPTCHA або повідомлення електронної пошти для скидання пароля з надто довгими часами очікування або без них.

Якщо функція відновлення пароля має недоліки, зловмисники потенційно можуть використати методи грубої сили або отримати доступ до інших зламаних облікових записів, щоб отримати доступ до облікових записів користувачів і облікових даних, які добре захищені за звичайних обставин.

15. Помилка двофакторної автентифікації

Хоча двофакторна автентифікація (2FA) ефективна для безпечної автентифікації, вона може спричинити критичні проблеми безпеки, якщо її не впровадити належним чином. Зловмисники можуть визначити чотири- та шестизначні коди перевірки 2FA за допомогою атак обміну SIM-картою, якщо вони надіслані через SMS. Деяка двофакторна автентифікація також не є справді двофакторною; якщо користувач намагається отримати доступ до конфіденційної інформації на викраденому телефоні за допомогою кешованих облікових даних, «другий фактор», який надсилає повідомлення на той самий телефон, не додає додаткової безпеки. Уразливість двофакторної автентифікації також може виникнути, якщо немає захисту від грубої сили для блокування облікового запису після певної кількості спроб входу.

16. Вразлива логіка автентифікації

Логічні вразливості поширені в програмних додатках. Це відбувається в результаті поганого кодування або дизайну, що впливає на автентифікацію та авторизацію доступу та функціональність програми. Помилка логіки програми може бути спричинена зловживанням функціональністю, слабкими заходами безпеки або пропущеним кроком у процедурі перевірки.

Наприклад, програма може запропонувати користувачеві відповісти на таємне запитання, яке логіка вважає таким, що «знає лише правильна особа». Але такі запитання, як день народження користувача чи дівоче прізвище матері, часто знайти легко. Ця вразливість дозволяє кібер-зловмисникам легко обійти автентифікацію та отримати незаконний доступ до таких облікових записів.

17. Людська недбалість

Згідно зі звітом Shred-it за 2020 рік, до 31% керівників старшого рівня назвали недбалість співробітників другою основною причиною витоку їхніх даних. Людська помилка може призвести до серйозних уразливостей автентифікації, якими набагато легше скористатися, ніж атаками грубої сили, ін’єкціями SQL та обходами автентифікації. Ця недбалість включає такі дії, як:

– Залишати комп’ютер увімкненим і незаблокованим у громадському місці
– Втрата пристроїв через крадіжку.
– Витік конфіденційної інформації незнайомцям.
– Написання поганого коду.

13.6. Загрози через технічні канали

Для перехоплення, обробки та аналізу інформації за допомогою **каналів витоку інформації (КВІ)** можуть використовуватися різноманітні **технічні засоби (ТЗс)**, а також люди (порушники). Тоді існуючі КВІ залежно від джерел і одержувачів інформації утворюють чотири основних типи каналів:

– «людина – людина»;

– «людина – ТЗс»;

– «ТЗс – ТЗс»;

– «ТЗс – людина».

Якщо інформаційний потік поширюється в напрямку від носія до одержувача, то утворюється ***узагальнений канал витоку***, якщо ж інформаційний потік у вигляді явної або прихованої дії направлений за вищезгаданими чотирма типами каналів від порушника до носія інформації, то виникає так званий ***узагальнений канал інформаційного впливу на носій інформації (канал спеціального впливу)***. Залежно від того, на який параметр носія інформації задумано здійснити вплив, порушником можуть бути застосовані психічні, фізичні, програмно-математичні, радіоелектронні та інші способи і засоби. Параметрами, на які задумано здійснити вплив, можуть бути різні характеристики матеріальних носіїв, у тому числі й власні характеристики головного прямого носія інформації – людини.

Найбільший потенціал інформативності мають КВІ, у яких для отримання конфіденційної інформації використовуються різні технічні засоби. Такі канали одержали назву **технічних (ТКВІ)**. Структура будь-якого ТКВІ, що утворюється в результаті перехоплення, може бути представлена у вигляді системи передачі інформації.

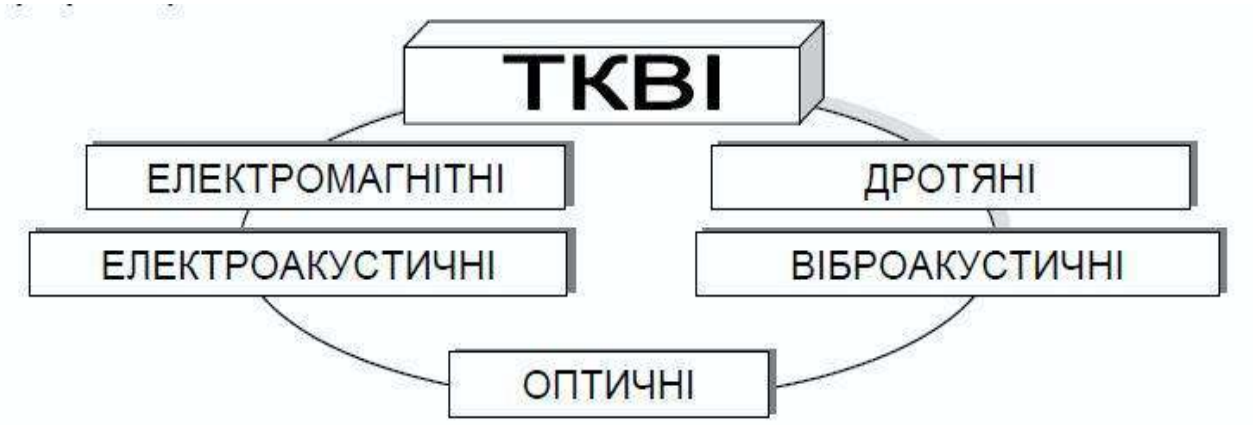


Рисунок 13.1 – Види технічних каналів витоку інформації (ТКВІ)

Структура технічних каналів витоку інформації (ТКВІ)

При цьому процес передачі повідомлень розбивається на три основні етапи.

– На початку кожне повідомлення a(t) перетворюється передавачем у небезпечний (інформаційний) сигнал b(t).

– Небезпечний сигнал переміщується трактом його поширення, де на нього діє завада p(t), внаслідок чого він частково затухає.

– Далі одержаний на приймальній стороні небезпечний сигнал b'(t) перетворюється приймачем порушника в повідомлення a'(t). Оскільки завади в загальному випадку мають випадковий характер, сигнал на вході приймача b'(t) буде випадковим чином відрізнятися від b(t) і повідомлення a(t) може відрізнятися від a'(t).

ТКВІ може бути утворений як за допомогою спеціальних закладних пристроїв (мініатюрні передавачі) та приймачів, так і за допомогою тільки приймачів, які приймають небезпечні сигнали, утворені несанкціонованим перетворенням сигналів з каналів передачі даних у технічних засобах обробки інформації.

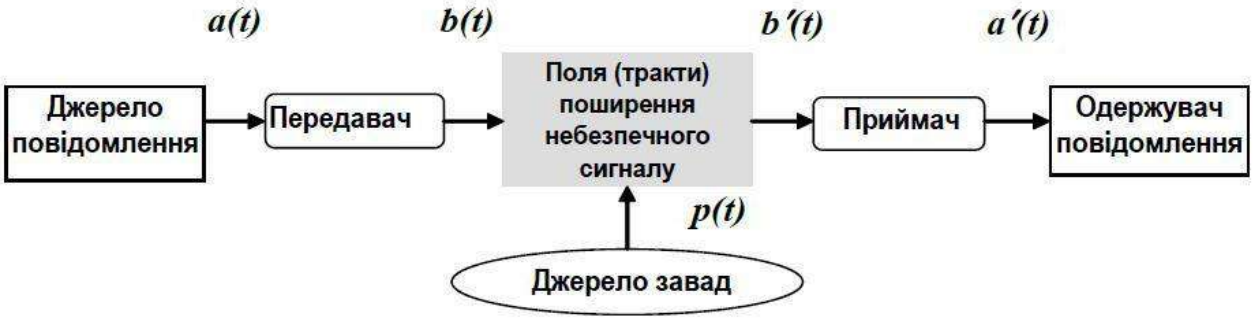


Рисунок 13.2 – Процес передачі повідомлень

Класифікація технічних каналів витоку інформації (ТКВІ)

Схема можливих каналів витоку і несанкціонованого доступу до інформації в типовому одноповерховому приміщенні показана на рисунку нижче.



Рисунок 13.3 – Можливі канали витоку інформації (КВІ) та несанкціонованого доступу (НСД)

На рисунку використанні наступні умовні позначення:
1 – Витік за рахунок структурного звуку в стінах і перекриттях.
2 – Зняття інформації із стрічки принтера, погано стертих дискет і т. п.
3 – Зняття інформації з використанням відеозакладок.
4 – Програмно-апаратні закладки в ПЕОМ.
5 – Радіозакладки у стінах і меблях.
6 – Зняття інформації із системи вентиляції.
7 – Лазерне зняття акустичної інформації з вікон.
8 – Виробничі й технологічні відходи.
9 – Комп'ютерні віруси, логічні бомби і т.п.
10 – Зняття інформації шляхом наведень і "нав'язування".
11 – Дистанційне зняття відеоінформації (оптика).

12 – Зняття акустичної інформації з використанням диктофонів.
13 – Крадіжка носіїв інформації.
14 – Високочастотний канал витоку в побутовій техніці.
15 – Зняття інформації направленим мікрофоном.
16 – Внутрішні канали витоку інформації (через обслуговуючий персонал).
17 – Несанкціоноване копіювання.
18 – Витік за рахунок побічного випромінювання терміналу.
19 – Зняття інформації за рахунок використання "телефонного вуха".
20 – Зняття з клавіатури і принтера за акустичним каналом.
21 – Зняття з монітора з електромагнітного канала.
22 – Візуальне зняття з монітора і принтера.
23 – Наведення на лінії комунікацій і сторонні провідники.
24 – Витік через лінії зв'язку.
25 – Витік ланцюгами заземлення.
26 – Витік мережею електрогодинника.
27 – Витік трансляційною мережею та гучномовним зв'язком.
28 – Витік охоронно-пожежною сигналізацією.
29 – Витік мережею електроживлення.
30 – Витік мережею опалювання, газо- і водопостачання.

Компрометація інформації (один з видів інформаційних інфекцій). Реалізується, як правило, за допомогою несанкціонованих змін у базі даних, у результаті чого її споживач змушений або відмовитися від неї, або докладати додаткових зусиль для виявлення змін і відновлення правдивих відомостей. При використанні скомпрометованої інформації споживач піддається небезпеці прийняття правильних рішень.

Несанкціоноване використання інформаційних ресурсів, з одного боку, є наслідком її витоку й засобом її компрометації. З іншого боку, воно має самостійне значення, тому що може завдати великої шкоди керованій системі (аж до повного виходу ІТ з ладу) або її абонентам.

Помилкове використання інформаційних ресурсів, які є санкціонованими, може призвести до руйнування, витоку або компрометації зазначених ресурсів. Дана загроза найчастіше є наслідком помилок, наявних у ПЗ ІТ.

Несанкціонований обмін інформацією між абонентами може привести до одержання одним із них відомостей, доступ до яких йому заборонений. Наслідки ті ж, що й при несанкціонованому доступі.

Відмова від інформації полягає в невизнанні одержувачем або відправником цієї інформації фактів її одержання або відправлення. Це дозволяє одній із сторін розривати укладені фінансові угоди "технічним" шляхом, формально не відмовляючись від них, наносячи тим самим другій стороні значний збиток.

Порушення інформаційного обслуговування – загроза, джерелом якої є сама ІТ. Затримка з наданням інформаційних ресурсів абонентові може призвести до тяжких для нього наслідків. Відсутність у користувача своєчасних

даних, необхідних для ухвалення рішення, може викликати його нераціональні дії.

Незаконне використання привілеїв. Будь-яка захищена система містить засоби, використовувані в надзвичайних ситуаціях, або засоби, які здатні функціонувати з порушенням існуючої політики безпеки. Наприклад, на випадок раптової перевірки користувач повинен мати можливість доступу до всіх наборів системи. Зазвичай, ці засоби використовуються адміністраторами, операторами, системними програмістами й іншими користувачами, що виконують спеціальні функції. Більшість систем захисту в таких випадках використовують набори привілеїв, тобто для виконання певної функції потрібний певний привілей. Звичайно, користувачі мають мінімальний набір привілеїв, а адміністратори – максимальний.

Набори привілеїв охороняються системою захисту. Несанкціоноване (незаконне) захоплення привілеїв можливе за наявності помилок у системі захисту, але найчастіше відбувається в процесі керування системою захисту, зокрема при недбалому користуванні привілеями. Суворе дотримання правил керування системою захисту, а також принципу мінімуму привілеїв дозволяє уникнути таких порушень. Під час опису в різній літературі різноманітних загроз для ІС і способів їх реалізації широко використовується поняття атаки на ІС.

Атака – зловмисні дії зломщика (спроби реалізації ним будь-якого виду загрози). Наприклад, атакою є застосування кожної зі шкідливих програм. Серед атак на ІС часто виділяють "маскарад" і "злом системи", які можуть бути результатом реалізації різноманітних загроз (або комплексу загроз).

Під "**маскарадом**" розуміється виконання яких-небудь дій одним користувачем ІС від імені іншого користувача. Такі дії іншому користувачеві можуть бути дозволені. Порушення полягає в присвоєнні прав і привілеїв, що називається симуляцією або моделюванням. Цілі "маскараду" – приховування яких-небудь дій за ім'ям іншого користувача або присвоєння прав і привілеїв іншого користувача для доступу до його наборів даних або для використання його привілеїв. Можуть бути й інші способи реалізації "маскараду", наприклад створення й використання програм, які в певнім місці можуть змінити певні дані, у результаті чого користувач одержує інше ім'я. "Маскарадом" називають також передачу повідомлень у мережі від імені іншого користувача. Найнебезпечніший "маскарад" у банківських системах електронних платежів, де неправильна ідентифікація клієнта може призвести до величезних збитків. Особливо це стосується платежів з використанням електронних карт. Використовуваний у них метод ідентифікації за допомогою персонального ідентифікатора досить надійний. Але порушення можуть відбуватися внаслідок помилок його використання, наприклад втрати кредитної картки або використанні очевидного ідентифікатора (свого ім'я й т. д.). Для запобігання "маскараду" необхідно використовувати надійні методи ідентифікації, блокування спроб злому системи, контроль входів у неї. Необхідно фіксувати всі події, які можуть свідчити про "маскарад", у системному журналі для його наступного аналізу. Також бажано не використовувати програмні продукти, що містять помилки, які можуть привести до "маскараду".

Під **зломом системи** розуміють навмисне проникнення в систему, коли зломщик не має санкціонованих параметрів для входу. Способи злому можуть бути різними, і при деяких з них відбувається збіг з раніше описаними загрозами. Так, об'єктом полювання часто стає пароль іншого користувача. Пароль може бути розкритий, наприклад, шляхом перебору можливих паролів. Злом системи можна здійснити також, використовуючи помилки програми входу.

Основне навантаження захисту системи від злому несе **програма входу**. Алгоритм уведення ім'я й пароля, їхнє шифрування, правила зберігання й зміни паролів не повинні містити помилок. Протистояти злому системи допоможе, наприклад, обмеження спроб неправильного уведення пароля (тобто виключити досить великий перебір) з наступним блокуванням термінала й повідомленням адміністратора у випадку порушення. Крім того, адміністратор безпеки повинен постійно контролювати активних користувачів системи: їхні імена, характер роботи, час входу й виходу й т. д. Такі дії допоможуть вчасно встановити факт злому й почати необхідні дії.

Умовою, що сприяє реалізації багатьох видів загроз ІС, є наявність "люків". **Люк-схованка**, не документована точка входу в програмний модуль, що входить до складу ПЗ ІС і ІТ. Люк вставляється в програму, звичайно, на етапі налагодження для полегшення роботи: даний модуль можна викликати в різних місцях, що дозволяє налагоджувати окремі частини програми незалежно. Наявність люка дозволяє викликати програму нестандартним чином, що може відбитися на стані системи захисту. Люки можуть залишитися в програмі з різних причин:

– їх могли забути забрати;

– для подальшого налагодження;

– для забезпечення підтримки готової програми;

– для реалізації таємного доступу до програми після її установки.

Більша небезпека люків компенсується високою складністю їх виявлення (якщо, звичайно, не знати заздалегідь про їх наявність), тому що виявлення люків – результат випадкового й трудомісткого пошуку. Захист від люків один – не допускати їхньої появи в програмі, а при прийманні програмних продуктів, розроблених іншими виробниками, варто проводити аналіз вихідних текстів програм з метою виявлення люків.

Реалізація загроз ІС приводить до різних видів прямих або непрямих втрат. **Втрати** можуть бути пов'язані з **матеріальним збитком**:

– вартість компенсації, відшкодування іншого побічно втраченого майна;

– вартість ремонтно-відбудовних робіт;

– витрати на аналіз, дослідження причин і величини збитку;

– додаткові витрати на відновлення інформації, пов'язані з відновленням роботи й контролем даних і т. д.

Втрати можуть виражатися в обмеженні банківських інтересів, фінансових витратах або у втраті клієнтури.

Статистика показує, що у всіх країнах збитки від зловмисних дій безупинно зростають. Причому основні причини збитків пов'язані не стільки з недостатністю засобів безпеки як таких, скільки з відсутністю взаємозв'язку між ними, тобто з нереалізованістю системного підходу. Тому необхідно випереджальними темпами вдосконалювати комплексні засоби захисту.

13.7. Загрози через соціальну інженерію.

Всі ми знаємо про зловмисника, який використовує свій технічний досвід для проникнення в захищені комп'ютерні системи та злому конфіденційних даних. Цей тип зловмисників постійно робить новини, спонукаючи нас протистояти їхнім подвигам, інвестуючи в нові технології, які зміцнять наш мережевий захист.

Однак є ще один тип зловмисників, які використовують різні тактики, щоб оминути наші інструменти та рішення. Їх називають "соціальними інженерами", тому що вони використовують одну слабкість, яка є в кожній організації: людська психологія. Використовуючи телефонні дзвінки та інші засоби спілкування з користувачами, ці зловмисники змушують людей передавати доступ до конфіденційної інформації організації.

Соціальна інженерія – термін, який охоплює широкий спектр шкідливих дій. Зосередимося на п'яти найпоширеніших типах атак, які використовують соціальні інженери.

1. Фішинг

Фішинг є найпоширенішим типом атаки соціальної інженерії, що відбувається сьогодні. Але що? На високому рівні більшість фішинг-шахраїв намагаються виконати три речі:

– Отримати особисту інформацію, таку як імена, адреси та номери соціального страхування.

– Використовувати скорочені або вводять в оману посилання, які перенаправляють користувачів на підозрілі веб-сайти, на яких розміщуються цільові фішингові сторінки.

– Включити погрози, страх і почуття терміновості у спробі змусити користувача реагувати якнайшвидше.

Немає двох однакових фішингових листів. Насправді існує як мінімум шість різних підкатегорій атак фішингу. Крім того, ми всі знаємо, що деякі з них погано опрацьовані, оскільки в них повідомлення страждають від орфографічних та граматичних помилок. Тим не менш, ці електронні листи зазвичай мають одну і ту ж ціль – використовувати підроблені веб-сайти або форми для крадіжки облікових даних користувача та інших особистих даних.

У нещодавній фішинг кампанії використовується скомпрометований обліковий запис електронної пошти, щоб відправити листа. У цих повідомленнях просили одержувачів переглянути запропонований документ, клацнувши вбудовану URL-адресу. Ця шкідлива URL-адреса, захищена URL-адресою Symantec для захисту від кліків, перенаправила одержувачів на зламаний обліковий запис SharePoint, який доставив другу шкідливу URL-адресу, вбудовану в документ OneNote. Цей URL, у свою чергу, перенаправляє користувачів на сторінку фішингу, що зображує портал входу в систему Microsoft Office 365.

2. Приводи

Привід – це ще одна форма соціальної інженерії, де зловмисники концентруються на створенні хорошого прийменника чи сфабрикованого сценарію, який вони використовують, щоб спробувати вкрасти особисту інформацію своїх жертв. У цих типах атак шахрай зазвичай каже, що їм потрібна певна кількість інформації від своєї мети, щоб підтвердити свою особистість. Насправді вони крадуть ці дані та використовують їх для вчинення крадіжки особистих даних або проведення вторинних атак.

Більш просунуті атаки іноді намагаються обдурити свої цілі, роблячи щось, що зловживає цифровими та/або фізичними вадами організації. Наприклад, зловмисник може видати себе зовнішнього аудитора IT-послуг, щоб він міг переконати групу фізичної безпеки цільової компанії пустити їх у будинок.

У той час як фішингові атаки в основному використовують страх і терміновість у своїх інтересах, атаки з приводом ґрунтуються на створенні хибного почуття довіри до жертви. Це вимагає від зловмисника побудувати достовірну історію, яка залишає мало місця для сумнівів із боку їхньої мети.

Привід може приймати та набуває різних форм. Незважаючи на це, багато суб'єктів загроз, які приймають цей тип атаки, вирішують маскуватися під кадри чи співробітників відділу розвитку фінансів.

3. Принада

Принада багато в чому схожа на атаки фішинга. Однак те, що відрізняє їх від інших видів соціальної інженерії, – це обіцянка будь-якого предмета чи блага, які зловмисники використовують для спокуси жертв. Приманки можуть використовувати пропозицію безкоштовного завантаження музики або фільмів, наприклад, щоб обманом змусити користувачів передати облікові дані для входу.

Зловмисники можуть також зосередитись на використанні людської цікавості за допомогою фізичних засобів.

Наприклад, ще в липні 2018 року KrebsOnSecurity повідомив про кампанію з нападу на державні установи та органи місцевого самоврядування у Сполучених Штатах. Операція розіслала китайські поштові марковані конверти, які містили заплутаний лист разом із компакт-диском (CD). Ціль полягала в тому, щоб розбудити цікавість одержувачів, щоб вони завантажували компакт-диск і тим самим ненавмисно заражали свої комп'ютери шкідливим ПЗ.

4. Що за що (quid pro quo)

Подібно до цькування, напади quid pro quo обіцяють вигоду в обмін на інформацію. Ця вигода зазвичай набуває форми послуги, тоді як цькування зазвичай набуває форми користі. Один з найбільш поширених типів атак quid pro quo, що з'явилися в останні роки, – це коли шахраї видають себе за Адміністрацію соціального забезпечення США (SSA). Ці підроблені співробітники SSA зв'язуються зі випадковими особами, повідомляють їм, що з їхнього боку виникла проблема з комп'ютером, і просять, щоб ці особи підтвердили свій номер соціального страхування, все це спрямоване на крадіжку особистих даних. В інших випадках, виявлених Федеральною торговою комісією (FTC), зловмисники створюють підроблені веб-сайти SSA, які кажуть, що можуть допомогти користувачам подати заявку на нові карти соціального

забезпечення, але натомість просто крадуть їхню особисту інформацію.

Тим не менш, важливо відзначити, що зловмисники можуть використовувати пропозиції quid pro quo, які набагато менш витончені, ніж хитрощі на тему SSA. Як показали попередні атаки, офісні працівники більш ніж готові віддати свої паролі за дешеву ручку або навіть плитку шоколаду.

5. Хвостовик (Tailgating)

Наш останній тип соціальної атаки на сьогоднішній день відомий як Tailgating. У цих типах атак хтось без належної автентифікації слідує за перевіреним співробітником в обмежену область. Зловмисник може видати себе за водія служби доставки та почекати зовні будівлі, щоб розпочати роботу. Коли співробітник отримує схвалення служби безпеки та відчиняє двері, зловмисник просить співробітника притримати двері, тим самим одержуючи доступ до будівлі. Tailgating не працює у всіх корпоративних умовах, таких як великі компанії, входи до яких вимагають використання карти-ключа. Однак на середніх підприємствах зловмисники можуть зав'язати розмову зі співробітниками та використати цю демонстрацію знайомства, щоб обійти стійку реєстрації. Фактично, Колін Грінлес, консультант з безпеки в Siemens Enterprise Communications, використав цю тактику, щоб отримати доступ до кількох поверхів і кімнат даних у фінансовій компанії, зареєстрованій на біржі FTSE. Він навіть зміг відкрити магазин у залі засідань на третьому поверсі та працювати там протягом кількох днів.

Рекомендації щодо соціальної інженерії

Зловмисники, які беруть участь в атаках соціальної інженерії, полюють на людську психологію та цікавість, щоб поставити під загрозу інформацію. Пам'ятаючи про цей фокус, орієнтований на людину, організації повинні допомогти своїм співробітникам протистояти атакам такого типу.

Ось кілька порад, які організації можуть включити до своїх навчальних програм безпеки, які допоможуть користувачам уникнути схем соціальної інженерії:

– Не відкривайте листи з ненадійних джерел. Зв'яжіться з другом або членом сім'ї особисто або по телефону, якщо ви отримали від них підозрілі повідомлення.

– Не вірте реченням від незнайомих людей. Сумнівайтесь! Якщо пропозиції здаються надто хорошими, щоб бути правдою, вони, мабуть, це шахрайство.

– Заблокуйте свій ноутбук, коли ви залишаєтеся робоче місце.

– Купити антивірусне програмне забезпечення. Жодне AV-рішення не може захистити від будь-якої загрози, яка ставить під загрозу інформацію користувачів, але вони можуть допомогти захистити від деяких атак.

– Прочитайте політику конфіденційності компанії, щоб зрозуміти, за яких обставин ви можете або повинні впустити незнайомця в будівлю.

Розділ 14. Оцінка захищеності інформації в інформаційно-телекомунікаційних системах (ІКС)

14.1. Оцінка захищеності інформації в інформаційно-телекомунікаційних системах згідно НД ТЗІ 2.5-004-99. «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»

14.2. Концептуальна схема оцінки безпеки інформації.

14.3. Кількісна та якісна оцінки безпеки інформації.

14.1. Оцінка захищеності інформації в інформаційно-телекомунікаційних системах згідно НД ТЗІ 2.5-004-99. «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»

Цей нормативний документ (далі – Критерії) – установлює критерії оцінки захищеності інформації, оброблюваної в комп'ютерних системах, від несанкціонованого доступу. Критерії є методологічною базою для визначення вимог з захисту інформації в комп'ютерних системах від несанкціонованого доступу; створення захищених комп'ютерних систем і засобів захисту від несанкціонованого доступу; оцінки захищеності інформації в комп'ютерних системах і їх придатності для обробки критичної інформації (інформації, що вимагає захисту).

Критерії надають:

1. Порівняльну шкалу для оцінки надійності механізмів захисту інформації від несанкціонованого доступу, реалізованих в комп'ютерних системах.

2. Базу (орієнтири) для розробки комп'ютерних систем, в яких мають бути реалізовані функції захисту інформації.

Критерії можуть застосовуватися до всього спектра комп'ютерних систем, включаючи однорідні системи, багатопроцесорні системи, бази даних, вбудовані системи, розподілені системи, мережі, об'єктно-орієнтовані системи та ін.

В цьому нормативному документі використовуються такі позначення і скорочення:

Загальні терміни:

– АС – автоматизована система;
– КС – комп'ютерна система;
– КЗЗ – комплекс засобів захисту;
– НСД – несанкціонований доступ;
– ОС – обчислювальна система;
– ПЗ – програмне забезпечення;
– ПЗП – постійний запам'ятовуючий пристрій;
– ПРД – правила розмежування доступу;

Позначення послуг:

– КД – довірча конфіденційність;
– КА – адміністративна конфіденційність;
– КО – повторне використання об'єктів;
– КК – аналіз прихованих каналів;
– КВ – конфіденційність при обміні;
– ЦД – довірча цілісність;
– ЦА – адміністративна цілісність;
– ЦО – відкат;
– ЦВ – цілісність при обміні;
– ДР – використання ресурсів;
– ДВ – стійкість до відмов;
– ДЗ – гаряча заміна;
– ДВ – відновлення після збоїв;
– НР – реєстрація;
– НИ – ідентифікація і автентифікація;
– НК – достовірний канал;
– НО – розподіл обов'язків;
– НЦ – цілісність КЗЗ;
– НТ – самотестування;
– НВ – автентифікація при обміні;
– НА – автентифікація відправника;
– НП – автентифікація одержувача.

Побудова і структура критеріїв захищеності інформації

В процесі оцінки спроможності комп'ютерної системи забезпечувати захист оброблюваної інформації від несанкціонованого доступу розглядаються вимоги двох видів:

– вимоги до функцій захисту (послуг безпеки);
– вимоги до гарантій.

В контексті Критеріїв комп'ютерна система розглядається як набір функціональних послуг. Кожна послуга являє собою набір функцій, що дозволяють протистояти певній множині загроз. Кожна послуга може включати декілька рівнів. Чим вище рівень послуги, тим більш повно забезпечується захист від певного виду загроз. Рівні послуг мають ієрархію за повнотою захисту, проте не обов'язково являють собою точну підмножину один одного. Рівні починаються з першого (1) і зростають до значення n, де n – унікальне для кожного виду послуг.

Функціональні критерії розбиті на чотири групи, кожна з яких описує вимоги до послуг, що забезпечують захист від загроз одного із чотирьох основних типів.

Конфіденційність. Загрози, що відносяться до несанкціонованого ознайомлення з інформацією, становлять загрози конфіденційності. Якщо існують вимоги щодо обмеження можливості ознайомлення з інформацією, то відповідні послуги треба шукати в розділі “Критерії конфіденційності”. В цьому

розділі описані такі послуги (в дужках наведені умовні позначення для кожної послуги): довірча конфіденційність, адміністративна конфіденційність, повторне використання об'єктів, аналіз прихованих каналів, конфіденційність при обміні (експорті/імпорті).

Цілісність. Загрози, що відносяться до несанкціонованої модифікації інформації, становлять загрози цілісності. Якщо існують вимоги щодо обмеження можливості модифікації інформації, то відповідні послуги треба шукати в розділі "Критерії цілісності". В цьому розділі описані такі послуги: довірча цілісність, адміністративна цілісність, відкат і цілісність при обміні.

Доступність. Загрози, що відносяться до порушення можливості використання комп'ютерних систем або оброблюваної інформації, становлять загрози доступності. Якщо існують вимоги щодо захисту від відмови в доступі або захисту від збоїв, то відповідні послуги треба шукати в розділі "Критерії доступності". В цьому розділі описані такі послуги: використання ресурсів, стійкість до відмов, горяча заміна, відновлення після збоїв.

Спостереженість. Ідентифікація і контроль за діями користувачів, керованість комп'ютерною системою становлять предмет послуг спостереженості і керованості. Якщо існують вимоги щодо контролю за діями користувачів або легальністю доступу і за спроможністю комплексу засобів захисту виконувати свої функції, то відповідні послуги треба шукати у розділі "Критерії спостереженості". В цьому розділі описані такі послуги: реєстрація, ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність комплексу засобів захисту, самотестування, автентифікація при обміні, автентифікація відправника (невідмова від авторства), автентифікація одержувача (невідмова від одержання).

Крім функціональних критеріїв, що дозволяють оцінити наявність послуг безпеки в комп'ютерній системі, цей документ містить критерії гарантій, що дозволяють оцінити коректність реалізації послуг. Критерії гарантій включають вимоги до архітектури комплексу засобів захисту, середовища розробки, послідовності розробки, випробування комплексу засобів захисту, середовища функціонування і експлуатаційної документації. В цих Критеріях вводиться сім рівнів гарантій (Г-1,..., Г-7), які є ієрархічними. Ієрархія рівнів гарантій відбиває поступово наростаючу міру певності в тому, що реалізовані в комп'ютерній системі послуги дозволяють протистояти певним загрозам, що механізми, які їх реалізують, в свою чергу коректно реалізовані і можуть забезпечити очікуваний споживачем рівень захищеності інформації під час експлуатації комп'ютерної системи.

Структуру Критеріїв показано на рисунку 14.1.

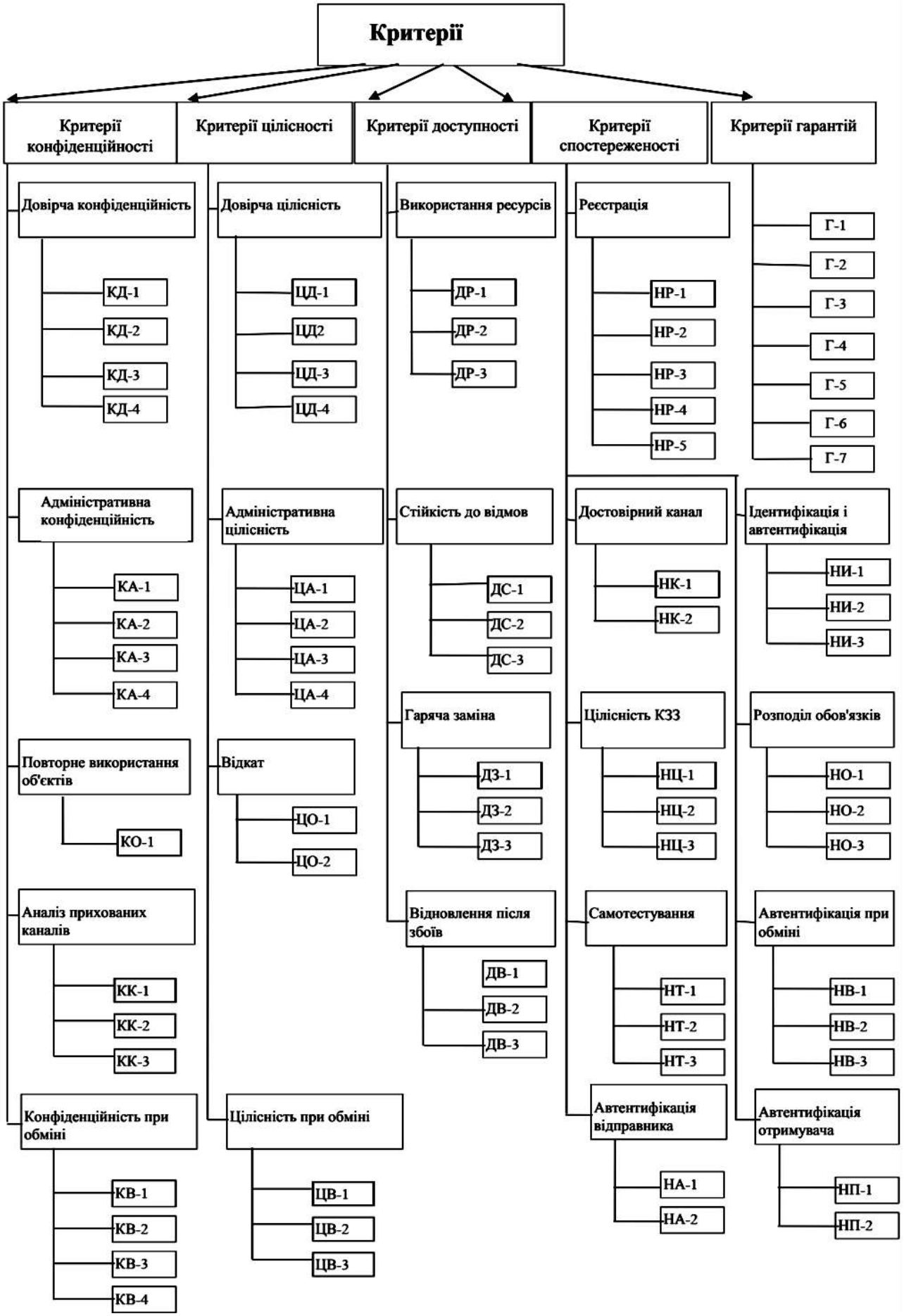


Рисунок 14.1 – Структура критеріїв

Всі описані послуги є більш-менш незалежними. Якщо ж така залежність виникає, тобто реалізація якої-небудь послуги неможлива без реалізації іншої, то цей факт відбивається як необхідні умови для даної послуги (або її рівня). За винятком послуги *аналіз прихованих каналів* залежність між функціональними послугами і гарантіями відсутня. **Рівень послуги *цілісність комплексу засобів захисту* НЦ-1 є необхідною умовою абсолютно для всіх рівнів всіх інших послуг.**

Порядок оцінки комп'ютерної системи на предмет відповідності цим Критеріям визначається відповідними нормативними документами. Експертна комісія, яка проводить оцінку комп'ютерної системи, визначає, які послуги і на якому рівні реалізовані в даній комп'ютерній системі, і як дотримані вимоги гарантій. Результатом оцінки є рейтинг, що являє собою упорядкований ряд (перелічення) буквено-числових комбінацій, що позначають рівні реалізованих послуг, в поєднанні з рівнем гарантій. Комбінації упорядковуються в порядку опису послуг в критеріях. Для того, щоб до рейтингу комп'ютерної системи міг бути включений певний рівень послуги чи гарантій, повинні бути виконані всі вимоги, перелічені в критеріях для даного рівня послуги або гарантій.

Критерії конфіденційності

Для того, щоб КС могла бути оцінена на предмет відповідності критеріям конфіденційності, КЗЗ оцінюваної КС повинен надавати послуги з захисту об'єктів від несанкціонованого ознайомлення з їх змістом (компрометації). Конфіденційність забезпечується такими послугами: довірча конфіденційність, адміністративна конфіденційність, повторне використання об'єктів, аналіз прихованих каналів, конфіденційність при обміні.

Довірча конфіденційність

Ця послуга дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. Рівні даної послуги ранжуються на підставі повноти захисту і вибірковості керування.

<table>
<tr><th>КД-1. Мінімальна довірча конфіденційність</th><th>КД-2. Базова довірча конфіденційність</th><th>КД-3. Повна довірча конфіденційність</th><th>КД-4. Абсолютна довірча конфіденційність</th></tr>
<tr><td colspan="2">Політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься</td><td colspan="2">Політика довірчої конфіденційності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС</td></tr>
<tr><td colspan="4">КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу</td></tr>
<tr><td>процесу і захищеного об'єкта</td><td colspan="2">користувача і захищеного об'єкта</td><td>користувача, процесу і захищеного об'єкта</td></tr>
<tr><td colspan="4">Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта</td></tr>
</table>

<table>
<tr><td colspan="4">КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити</td></tr>
<tr><td>конкретні процеси і/або групи процесів, які мають право одержувати інформацію від об'єкта</td><td>конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта</td><td>конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта</td><td>конкретних користувачів і процеси (і групи користувачів і процесів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта</td></tr>
<tr><td rowspan="2">—</td><td colspan="3">КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити</td></tr>
<tr><td>конкретних користувачів і/або групи користувачів, які мають право ініціювати процес</td><td colspan="2">конкретних користувачів (і групи користувачів), які мають, а також тих, що не мають права ініціювати процес</td></tr>
<tr><td colspan="4">Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації. Як частина політики довірчої конфіденційності повинні бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту</td></tr>
<tr><td colspan="2">НЕОБХІДНІ УМОВИ: НИ-1</td><td colspan="2">НЕОБХІДНІ УМОВИ: КО-1, НИ-1</td></tr>
</table>

Для усіх інших послуг існують аналогічні таблиці, які приведені у стандарті, який повністю наведений у додатку А.

Адміністративна конфіденційність

Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від захищених об'єктів до користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості управління.

Повторне використання об'єктів

Ця послуга дозволяє забезпечити коректність повторного використання розділюваних об'єктів, гарантуючи, що в разі, якщо розділюваний об'єкт виділяється новому користувачу або процесу, то він не містить інформації, яка залишилась від попереднього користувача або процесу.

Аналіз прихованих каналів

Аналіз прихованих каналів виконується з метою виявлення і усунення потоків інформації, які існують, але не контролюються іншими послугами. Рівні даної послуги ранжируються на підставі того, чи виконується тільки виявлення, контроль або перекриття прихованих каналів.

Конфіденційність при обміні

Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Критерії цілісності

Для того, щоб КС могла бути оцінена на предмет відповідності критеріям цілісності, КЗЗ оцінюваної КС повинен надавати послуги з захисту оброблюваної інформації від несанкціонованої модифікації. Цілісність забезпечується такими послугами: довірча цілісність, адміністративна цілісність, відкат, цілісність при обміні.

Довірча цілісність

Ця послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Адміністративна цілісність

Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від користувачів до захищених об'єктів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Відкат

Ця послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкатити) захищений об'єкт до попереднього стану. Рівні даної послуги ранжируються на підставі множини операцій, для яких забезпечується відкат.

Цілісність при обміні

Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Критерії доступності

Для того, щоб КС могла бути оцінена на відповідність критеріям доступності, КЗЗ оцінюваної КС повинен надавати послуги щодо забезпечення можливості використання КС в цілому, окремих функцій або оброблюваної інформації на певному проміжку часу і гарантувати спроможність КС функціонувати у випадку відмови її компонентів. Доступність може забезпечуватися в КС такими послугами: використання ресурсів, стійкість до відмов, гаряча заміна, відновлення після збоїв.

Використання ресурсів

Ця послуга дозволяє користувачам керувати використанням послуг і ресурсів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування доступністю послуг КС.

Стійкість до відмов

Стійкість до відмов гарантує доступність КС (можливість використання інформації, окремих функцій або КС в цілому) після відмови її компонента. Рівні даної послуги ранжируються на підставі спроможності КЗЗ забезпечити можливість функціонування КС в залежності від кількості відмов і послуг, доступних після відмови.

Гаряча заміна

Ця послуга дозволяє гарантувати доступність КС (можливість використання інформації, окремих функцій або КС в цілому) в процесі заміни окремих компонентів. Рівні даної послуги ранжируються на підставі повноти реалізації.

Відновлення після збоїв

Ця послуга забезпечує повернення КС у відомий захищений стан після відмови або переривання обслуговування. Рівні даної послуги ранжируються на підставі міри автоматизації процесу відновлення.

Критерії спостереженості

Для того, щоб КС могла бути оцінена на предмет відповідності критеріям спостереженості, КЗЗ оцінюваної КС повинен надавати послуги з забезпечення відповідальності користувача за свої дії і з підтримки спроможності КЗЗ виконувати свої функції. Спостереженість забезпечується в КС такими послугами: реєстрація (аудит), ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність КЗЗ, самотестування, ідентифікація і автентифікація при обміні, автентифікація відправника, автентифікація отримувача

Реєстрація

Реєстрація дозволяє контролювати небезпечні для КС дії. Рівні даної послуги ранжируються залежно від повноти і вибірковості контролю, складності засобів аналізу даних журналів реєстрації і спроможності вияву потенційних порушень.

Ідентифікація і автентифікація

Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до КС. Рівні даної послуги ранжируються залежно від числа задіяних механізмів автентифікації.

Достовірний канал

Ця послуга дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ. Рівні даної послуги ранжируються залежно від гнучкості надання можливості КЗЗ або користувачу ініціювати захищений обмін.

Розподіл обов'язків

Ця послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Рівні даної послуги ранжируються на підставі вибірковості керування можливостями користувачів і адміністраторів.

Цілісність комплексу засобів захисту

Ця послуга визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

Самотестування

Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Рівні даної послуги ранжируються на підставі можливості виконання тестів у процесі запуску або штатної роботи.

Ідентифікація і автентифікація при обміні

Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ранжируються на підставі повноти реалізації.

Автентифікація відправника

Ця послуга дозволяє забезпечити захист від відмови від авторства і однозначно встановити належність певного об'єкта певному користувачу, тобто той факт, що об'єкт був створений або відправлений даним користувачем. Рівні даної послуги ранжируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною.

Автентифікація отримувача

Ця послуга дозволяє забезпечити захист від відмови від одержання і дозволяє однозначно встановити факт одержання певного об'єкта певним користувачем. Рівні даної послуги ранжируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною.

Критерії гарантій

Критерії гарантій включають вимоги до архітектури КЗЗ, середовища розробки, послідовності розробки, середовища функціонування, документації і випробувань КЗЗ. В цих критеріях вводиться сім рівнів гарантій, які є ієрархічними. Вимоги викладаються за розділами. Для того, щоб КС одержала певний рівень гарантій (якщо вона не може одержати більш високий), повинні бути задоволені всі вимоги, визначені для даного рівня в кожному з розділів.

Архітектура

Вимоги до архітектури забезпечують гарантії того, що КЗЗ у змозі повністю реалізувати політику безпеки.

Середовище розробки

Вимоги до середовища розробки забезпечують гарантії того, що процеси розробки і супроводження оцінюваної КС є повністю керованими з боку Розробника.

Послідовність розробки

Вимоги до процесу проектування (послідовності розробки) забезпечують гарантії того, що на кожній стадії розробки (проектування) існує точний опис КС і реалізація КС точно відповідає вихідним вимогам (політиці безпеки).

Середовище функціонування

Вимоги до середовища функціонування забезпечують гарантії того, що КС поставляється Замовнику без несанкціонованих модифікацій, а також інсталюється і ініціюється Замовником так, як це передбачається Розробником.

Документація

Вимоги до документації є загальними для всіх рівнів гарантій.

У вигляді окремих документів або розділів (підрозділів) інших документів Розробник повинен подати опис послуг безпеки, що реалізуються КЗЗ, настанови адміністратору щодо послуг безпеки, настанови користувача щодо послуг безпеки.

В описі функцій безпеки повинні бути викладені основні, необхідні для правильного використання послуг безпеки, принципи політики безпеки, що реалізується КЗЗ оцінюваної КС, а також самі послуги.

Настанови адміністратору щодо послуг безпеки мають містити опис засобів інсталяції, генерації і запуску КС, опис всіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації і запуску КС, опис властивостей КС, які можуть бути використані для періодичної оцінки правильності функціонування КЗЗ, а також інструкції щодо використання адміністратором послуг безпеки для підтримки політики безпеки, прийнятої в організації, що експлуатує КС.

Настанови користувачу щодо послуг безпеки мають містити інструкції щодо використання функцій безпеки звичайним користувачем (не адміністратором).

Назва документів (розділів) не регламентується. Опис послуг безпеки може відрізнятися для користувача і адміністратора. Настанови адміністратору і настанови користувачу можуть бути об'єднані в настанови з установлення і експлуатації.

Випробування комплексу засобів захисту

Вимоги	**Г-1**	**Г-2**	**Г-3**	**Г-4**	**Г-5**	**Г-6**	**Г-7**
Розробник повинен подати для перевірки програму і методику випробувань, процедури випробувань усіх механізмів, що реалізують послуги безпеки. Мають бути представлені аргументи для підтвердження достатності тестового покриття	+	=	=	=	=	=	=
Розробник повинен подати докази тестування у вигляді детального переліку результатів тестів і відповідних процедур тестування, з тим, щоб отримані результати могли бути перевірені шляхом повторення тестування	+	=	=	=	=	=	=

Розробник повинен усунути або нейтралізувати всі знайдені “слабкі місця” і виконати повторне тестування КЗЗ для підтвердження того, що виявлені недоліки були усунені і не з'явилися нові “слабкі місця ”	-	+	=	=	=	=	=
Розробник повинен виконати тести з подолання механізмів захисту і довести, що КЗЗ відносно або абсолютно стійкий до такого роду атак з боку Розробника	-	-	-	+	=	+	=

14.2. Концептуальна схема оцінки безпеки інформації

Відповідно до стандарту ISO/IEC 15408 «Критерії оцінки безпеки інформаційних технологій» (Загальні критерії) загальна схема забезпечення інформаційної безпеки, має такий вигляд (рис. 14.2). На схемі показано взаємодію основних суб’єктів та об’єктів забезпечення інформаційної безпеки. Дана схема можна використовувати як основу для побудови концептуальної моделі інформаційної безпеки (ІБ) державних інформаційних ресурсів (ДІР).

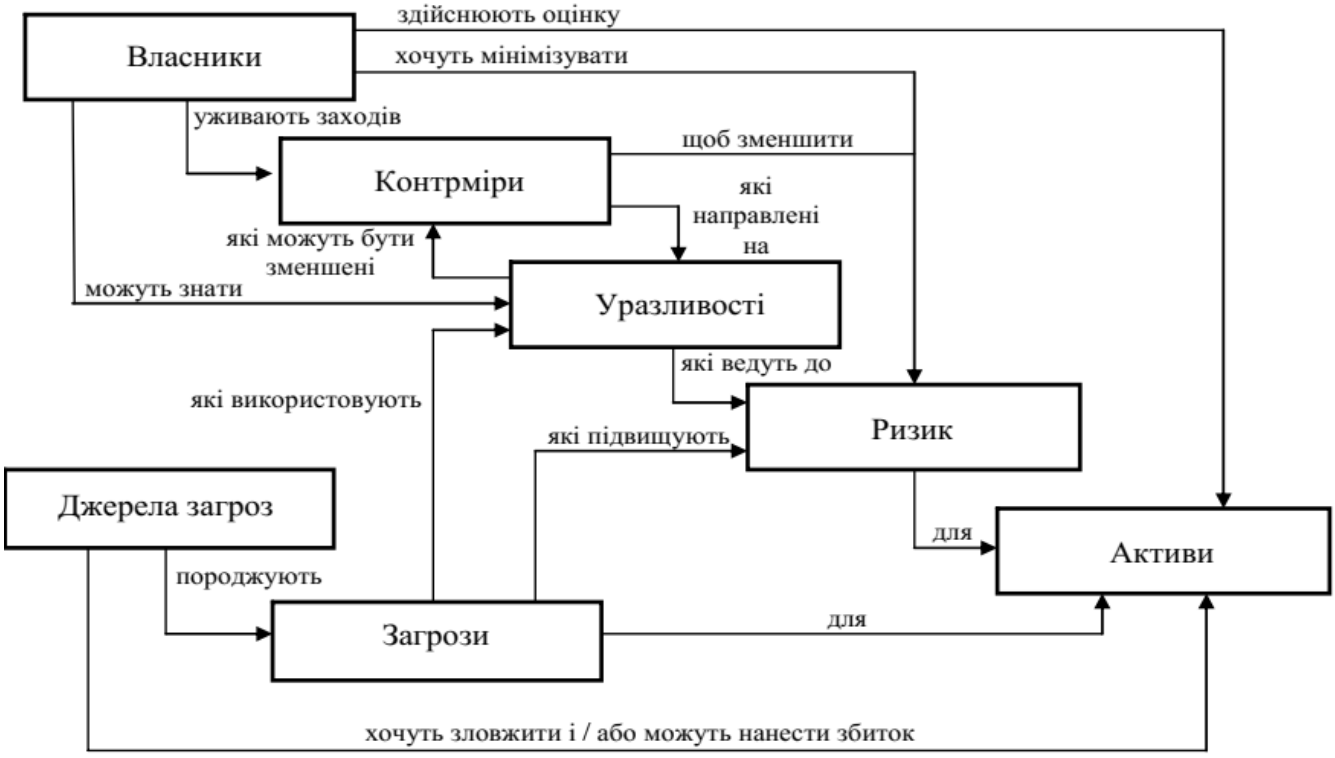


Рисунок 14.2 – Загальна схема забезпечення інформаційної безпеки відповідно до стандарту ISO/IEC 15408 «Критерії оцінки безпеки інформаційних технологій»

Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» (від 23 лютого 2006 року № 3475-IV зі змінами від 28.07.2022 року) державні інформаційні ресурси (ДІР) визначає наступним чином: ***державні інформаційні ресурси –*** систематизована інформація, що є доступною за допомогою інформаційних технологій, право на володіння, використання або розпорядження якою належить державним органам, військовим формуванням, утвореним відповідно до законів України, державним підприємствам, установам та організаціям, а також інформація, створення якої передбачено законодавством та яка обробляється фізичними або юридичними особами відповідно до наданих їм повноважень суб'єктами владних повноважень.

Крім того існує розширене визначення поняття ДІР.

Державні інформаційні ресурси – це результат інтелектуальної та практичної діяльності, що сформовані в усіх сферах життєдіяльності людини, суспільства і держави, зафіксовані і систематизовані на відповідних матеріальних носіях інформації, як окремі документи і масиви документів, банки і бази даних та знань, усі види архівів і бібліотек, музейні фонди, інформаційні ресурси які обробляються й передаються у інформаційних системах державного і/або загального призначення, інші ресурси, що містять дані, відомості і знання, які є об'єктом права власності держави незалежно від форми власності на час їх створення і мають споживчу цінність, а також такі, що призначені для розвитку і задоволення потреб громадян, суспільства, держави та підлягають захисту згідно визначеної політики безпеки й чинного законодавства.

Інформаційна безпека (ІБ) визначається як стан захищеності інформаційного середовища держави, суспільства та особистості, якій забезпечує його формування, збереження, використання і розвиток в інтересах громадян, організації чи держави. Там же наведено більш розширене визначення ІБ.

Інформаційна безпека – це стан захищеності властивостей інформації (інформаційних ресурсів), що належить державі, суспільству і особистості, за якого забезпечується її оброблення, зберігання, поширення і прогресивний розвиток незалежно від (або в умовах) наявності чи реалізації внутрішніх і зовнішніх інформаційних загроз.

До основних **компонентів концептуальної моделі ІБ ДІР** можуть бути віднесені:

– об'єкти загроз ДІР;

– загрози ДІР (нормативно-правового, організаційного, інженерно-технічного спрямування), за відповідними властивостями інформації (конфіденційність, цілісність, доступність);

– джерела загроз ДІР;

– уразливості ДІР;

– ризик реалізації загрози ДІР через уразливість;

– цілі джерел загроз ДІР;

– джерела відомостей про ДІР;

– способи неправомірного оволодіння ДІР (способи доступу до ДІР);

– напрями захисту ДІР (нормативно-правовий, організаційний, інженерно-технічний);

– способи захисту ДІР;

– засоби захисту ДІР

Об'єкти загроз ДІР (відповідно до визначеного авторами поняття ДІР) – всі інформаційні ресурси держави, суспільства або громадян, які підлягають захисту згідно визначеної політики безпеки й чинного законодавства.

Загрози ДІР – це потенційний або реальний стан небезпеки державним інформаційним ресурсам та безпосередньо їх властивостям (конфіденційності, цілісності, доступності), який може бути сформовано на основі реалізації будь-якого процесу та/або вчиненні діяння (та/або бездіяльності), спрямовано на порушення політики безпеки об'єкта інформаційної діяльності (державних інформаційних ресурсів) та такий, що завдає збитку державі. Крім того, через призму загальних напрямів забезпечення безпеки інформації (правовий захист, організаційний захист, інженерно-технічний захист) загрози ДІР можуть бути визначені як загрози відповідного спрямування:

– загрози нормативно-правового спрямування – загрози, які виникають в разі навмисного або ненавмисного порушення (впливу або/та дії на процес створення та застосування) спеціальних законів, інших нормативно-правових актів, правил, процедур та заходів, що забезпечують захист інформації на правовій основі;

– загрози організаційного спрямування – виникають у результаті навмисного або ненавмисного порушення регламентації виробничої діяльності та взаємовідносин виконавців на нормативно-правовій основі, що виключає або суттєво утруднює реалізацію процесів протидії несанкціонованому порушенню властивостей інформації (інформаційних ресурсів);

– загрози інженерно-технічного спрямування – загрози, що пов'язані з використанням різноманітних фізичних, апаратних, програмних, програмно-апаратних методів та засобів, які реалізують процеси розголошення, витоку, несанкціонованого доступу, інших форм незаконного спотворення і втручання до інформаційних ресурсів, а також призводять до різних видів збитків власнику ресурсів.

Джерела загроз ДІР – носії загроз безпеці інформації ДІР (кібертерористи та кіберзловмисники, персонал підданий корупційним діям, адміністративно-управлінські органи державної влади і т. д.). У цілому всі джерела загроз безпеці інформації можна розділити на три групи обумовлені діями суб'єкта (антропогенні джерела загроз); обумовлені технічними засобами (техногенні джерела загроз); зумовлені стихійними джерелами.

Уразливості ДІР – чинники, що призводять до порушення безпеки інформації на конкретному об'єкті інформаційної діяльності.

Ризик реалізації загрози ДІР

Існує декілька визначень поняття ризику:

– Ризик – функція ймовірності реалізації певної загрози, виду і величини завданих збитків.

– Ризик – потенційна можливість використання уразливостей активу або групи активів реальною загрозою для заподіяння збитку організації (ISO/IEC 27005:2008).

– Ризик – комбінація ймовірності події і її наслідків (BS 7799-3:2006).

Таким чином ***ризик реалізації загрози ДІР*** – потенційна можливість використання уразливостей державних інформаційних ресурсів реальною загрозою для заподіяння збитку державі, суспільству, окремому громадянину.

Цілі джерел загроз ДІР – ознайомлення з конфіденційними відомостями, їх модифікація з корисною метою, знищення для нанесення прямого матеріального збитку.

Джерела відомостей про ДІР – люди, документи та документообіг в цілому (паперовий, електронний), відкриті публікації, технічні носії інформації, технічні засоби виробничої та трудової діяльності, продукція та відходи виробництва.

Способи неправомірного оволодіння ДІР (способи доступу до ДІР) – розголошення джерелами конфіденційних відомостей, витік інформації через технічні засоби, несанкціонований доступ до відомостей, що підлягають охороні.

Напрями захисту ДІР – це нормативноправові категорії, орієнтовані на забезпечення комплексного захисту інформації від внутрішніх та зовнішніх загроз на державному рівні, на рівні підприємства або організації, а також на рівні окремої особистості. До основних напрямків захисту ДІР відносяться відповідно до комплексного підходу до захисту ДІР нормативноправовий, організаційний та інженернотехнічний.

Способи захисту ДІР – будь-які міри, шляхи, способи та дії, які забезпечують попередження протиправних дій, їх запобігання, припинення та протидію несанкціонованому доступу до ДІР.

Засоби захисту ДІР – фізичні, апаратні, програмні засоби та криптографічні методи. Криптографічні методи можуть бути реалізовані як апаратно так і змішано програмно-апаратними засобами.

Таким чином, **концептуальна модель ІБ ДІР може бути представлена у вигляді наступної схеми** (рис. 14.3).



Рисунок 14.3 – Концептуальна модель інформаційної безпеки державних інформаційних ресурсів

14.3. Кількісна та якісна оцінки безпеки інформації

Розглянемо класифікацію існуючих методів і засобів оцінки інформаційних ризиків.

Оцінка ризику – це процес, який використовується для присвоєння значень наслідків, ймовірності виникнення та рівня ризику. Вона включає в себе:

1. Оцінку ймовірності загроз і вразливостей, які можливі.
2. Розрахунок впливу, який може мати загроза на кожен актив.
3. Визначення кількісної (вимірні) або якісної (описуваної) вартості ризику.

Треба взяти до уваги те, що ці три змінні рідко незалежні одина від одної. В області інформаційної безпеки, є зв'язок між вартістю активів, впливом і ймовірністю. Наприклад, більш імовірно, що хакер буде використовувати уразливість, яка викликає більший вплив, ніж уразливість з низьким рівнем впливу. Крім того, цінний актив має більшу імовірність компрометації, ніж марний. Таким чином, в цій області повинно прийматися до уваги більше, ніж просто випадкові дії. Необхідно брати до уваги, що при наявності достатнього часу і рішучості, люди мають можливість обійти майже всі заходи безпеки. Вони можуть бути надзвичайно творчими, коли мотивовані. Таким чином, фактор мотивації повинен бути серйозно розглянутий в процесі оцінки безпеки інформаційного ризику.

На рис. 14.4 представлені три способи, за допомогою яких можна проводити оцінку інформаційних ризиків:

1. Методи.
2. Управляючі документи.
3. Інструменти.

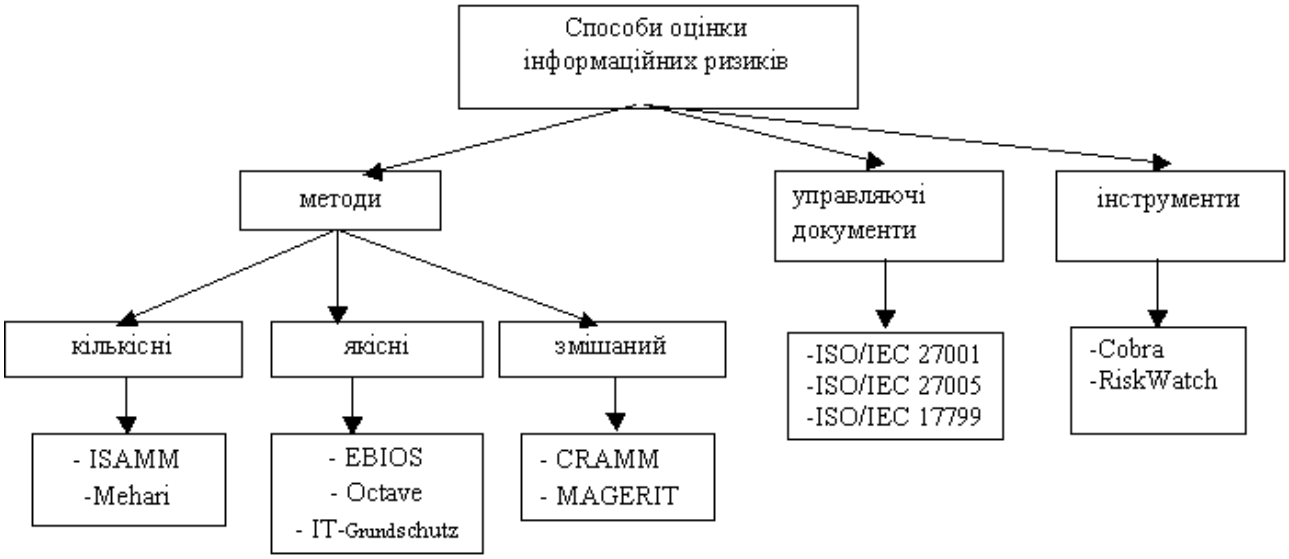


Рисунок 14.3 – Способи оцінки інформаційних ризиків

1. Методи

Метод розуміється, як систематизована сукупність кроків, дій, які необхідно зробити для вирішення певної задачі або досягти поставленої мети, в даному випадку провести оцінку ризиків. Тобто, метод мається на увазі покрокова інструкція плюс інструмент (програмний продукт) для проведення оцінки ризиків на підприємстві.

Всі методи оцінки ризику можна розділити на кількісні, якісні або комбінацію кількісних методів з якісними (змішаний).

Кількісні методи використовують вимірні, об'єктивні дані для визначення вартості активів, імовірність втрати і пов'язаних з ними ризиків. Мета полягає в тому, щоб обчислити числові значення для кожного з компонентів, зібраних в ході оцінки ризиків та аналізу витрат і переваг.

Якісні методи використовують відносний показник ризику або вартості активу на основі рейтингу або поділ на категорії, такі як низький, середній, високий, не важливо, важливо, дуже важливо, чи за шкалою від 1 до 10. Якісна модель оцінює дії й імовірності виявлених ризиків швидким і економічно ефективним способом. Набори ризиків записані і проаналізовані в якісній оцінці ризику, та можуть послужити основою для цілеспрямованої кількісної оцінки.

Раніше кількісні підходи використовувалися частіше. Однак, останнім часом використання суворо кількісних управлінь ризиками зазвичай призводить до важкої, тривалої роботи, і немає великих переваг перед якісним методом оцінки ризиків. **Комбінація кількісного і якісного методу** являє собою змішану сукупність переваг і недоліків вище згаданих методів.

Таблиця 14.1 – Переваги та недоліки методів оцінки інформаційних ризиків

	Кількісний	**Якісний**
Переваги	– ризики є пріоритетнішими фінансових наслідків; – активи є пріоритетнішими фінансових цінностей; – отримання спрощених результатів управління ризиком та поверненням інвестицій у забезпечення безпеки; – результати можуть бути виражені в управлінській специфічній термінології (наприклад, грошові значення і ймовірність виражається у вигляді певного відсотка); – точність має тенденцію до збільшення з плином часу, так як організація постійно веде записи даних.	– забезпечує прозорість і розуміння класифікації ризику; – можливість досягти консенсусу; – немає необхідності визначати фінансову вартість активів; – легше залучити людей, які не є експертами в області комп'ютерної безпеки.
Недоліки	– вплив значення, привласнених ризикам на підставі суб'єктивних думок учасників; – процес для досягнення надійних результатів і консенсусу займає багато часу; – розрахунок може бути складним і трудомістким; – результати представлені тільки в грошовому еквіваленті і їх складно інтерпретувати для «нетехнічних людей»; – процес вимагає спеціальних знань, тому складно навчити персонал.	– недостатня відмінність між важливими ризиками; – важко виправдати інвестиції в контроль реалізації, тому що немає підстав для аналізу витрат і переваг; – результати залежать від якості команди управління ризиками, яка буде створена.

Далі будуть розглянуті кращі світові методи для проведення повноцінної оцінки ризиків.

Методи оцінки ризику:

1.1. ISAMM

Виробник: Бельгія.

Опис: ISAMM була розроблена на основі Telindus. Це кількісний тип методології управління ризиками, де оцінюються ризики, виражаючи їх через щорічні очікувані збитків в грошових одиницях:

*Щорічні очікувані збитки (ALE) = [ймовірність] * [середній вплив].*

ISAMM дозволяє показувати й моделювати зниження ризику для кожного поліпшеного контролю і порівнювати з його вартістю реалізації. Ефективність методу дозволяє виконувати обґрунтовану оцінку ризику в рамках, з мінімальними витратами часу і зусиль. Останньою еволюцією в методології ISAMM є уявлення активів. Це означає, що він може бути використаний для запуску оцінки ризиків щодо активів або згрупувати набір активів. Цей метод оцінки ризиків складається з трьох основних частин: огляду; оцінки; результат розрахунків та звітність.

Метод оцінки ризику: кількісний.

Наявність допоміжних програмних інструментів: немає, але має хорошу керівну документацію.

1.2. Mehari

Виробник: Франція.

Опис: Це модель управління ризиками, з модульними компонентами і процесами. Модуль оцінки охоплює, крім інформаційної системи, організацію та її місця розташування в цілому, а також умови роботи, правові та нормативні аспекти.

Метод оцінки ризику: якісний і кількісний.

Наявність допоміжних програмних інструментів: є.

1.3. EBIOS

Виробник: Франція.

Опис: EBIOS являє собою повний набір посібників. Виробляються кращі практики, а також додатки документів, орієнтовані на кінцевих користувачів в різних контекстах. Цей метод широко використовується як в державному, так і приватному секторі. EBIOS формалізує підхід до оцінки ризику в області інформаційної безпеки систем. Метод враховує всі технічні об'єкти (програмне і апаратне забезпечення, мережі) і нетехнічні об'єкти (організації, людські аспекти, фізична безпека).

Метод оцінки ризику: якісний.

Наявність допоміжних програмних інструментів: є.

1.4. Octave

Виробник: США.

Опис: OCTAVE є самостійним підходом, що вказує на те, що персонал несе відповідальність за встановлення стратегії безпеки організації. OCTAVE вимагає аналізу в розгляді відносини між критично важливими активами, загрозами для цих активів і вразливостями (як організаційні, так і технологічні). Він визначає

пов'язані з інформацією активи, які важливі для організації і зосереджує діяльність на ці активи, тому що вони мають найбільш важливе значення для організації (акцент на кількох важливих активів, не більше п'яти). Існують різні OCTAVE методи, засновані на OCTAVE критеріях:

– OCTAVE;

– OCTAVE-S;

– OCTAVE Allegro.

Метод оцінки ризику: якісний.

Наявність допоміжних програмних інструментів: є.

1.5. IT-Grundschutz

Виробник: Німеччина.

Опис: IT-Grundschutz пропонує спосіб для створення системи управління інформаційною безпекою. Вона включає в себе як загальні рекомендації по забезпеченню безпеки IT так і допоміжні технічні рекомендації для досягнення необхідного рівня IT безпеки для конкретного домену.

У методі IT-Grundschutz представлені каталоги:

– модулі;

– каталоги загроз;

– каталоги захисту.

Метод оцінки ризику: якісний.

Наявність допоміжних програмних інструментів: є.

1.6. CRAMM

Виробник: Великобританія.

Опис: Метод CRAMM досить складно використовувати без CRAMM інструменту. У інструмента такаж назва, як і у методу – CRAMM. В основі методу CRAMM лежить комплексний підхід до оцінки ризиків, поєднуючи кількісні та якісні методи аналізу. Метод є універсальним і підходить як для великих, так і для дрібних організацій, як урядового, так і комерційного сектора. Грамотне використання методу CRAMM дозволяє отримувати дуже хороші результати, найбільш важливим з яких є можливість економічного обгрунтування витрат організації на забезпечення інформаційної безпеки та безперервності бізнесу. Економічно обгрунтована стратегія управління ризиками дозволяє, в кінцевому підсумку, заощаджувати кошти, уникаючи невиправданих витрат.

Метод оцінки ризику: якісний і кількісний.

Наявність допоміжних програмних інструментів: є.

1.7. Назва методу: Magerit

Виробник: Іспанія.

Опис: Magerit є відкритою методологією аналізу та управління ризиками пропонованої в якості основи і керівництва:

– для того, щоб особи відповідальні за інформаційні системи знали про існування ризиків і необхідність розглядати їх своєчасно;

– для пропозиції систематичного методу аналізу цих ризиків;

– для опису і планування відповідних заходів по утриманню ризику під контролем;

– для підготовки організації по процесу оцінки, аудиту, сертифікації та акредитації.

Метод оцінки ризику: кількісний і якісний.

Наявність допоміжних програмних інструментів: є.

2. Управляючі документи

Крім методів оцінки ризиків використовують управляючі документи. Де теоретично описуються і даються методичні вказівки процесу оцінки ризиків, але не дається конкретних технологій. Найвідоміші стандарти, які використовуються на території України: ISO 27001, ISO 27005, ISO 17799.

2.1. ISO/IEC 27001

Опис: Міжнародний стандарт ISO/IEC 27001 визначає процеси, що представляють можливість бізнесу встановлювати, застосовувати, переглядати, контролювати і підтримувати ефективну систему менеджменту інформаційної безпеки.

У даному стандарті регламентовані вимоги до розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та вдосконалення документованої системи менеджменту інформаційної безпеки в контексті існуючих бізнес ризиків організації.

Зазначені вимоги реалізуються в рамках документованих процесів менеджменту інформаційної безпеки, структурованих по моделі PDCA (Plan-Do-Check-Act). Стандарт ISO/IEC 27001 являє наочну модель менеджменту, що дозволяє здійснювати оцінку ризиків, проектування і реалізацію системи інформаційної безпеки, її менеджмент і переоцінку.

2.2. ISO/IEC 27005

Опис: Цей стандарт призначений для визначення в організації підходу до менеджменту ризиків в залежності, наприклад, від області дії СМІБ, області застосування менеджменту ризиків або сектора промисловості. Забезпечує рекомендації для менеджменту ризиків інформаційної безпеки, які включають інформацію і менеджмент ризиків безпеки технологій телекомунікації.

Стандарт підтримує загальні концепції, визначені в ISO/IEC 27001, і призначений для сприяння адекватного забезпечення інформаційної безпеки на основі підходу, пов'язаного з менеджментом ризику.

Застосуємо для організацій усіх типів (наприклад, комерційних підприємств, державних установ, некомерційних організацій), які планують здійснювати менеджмент ризиків, для компрометації інформаційної безпеки організації.

2.3. ISO/IEC 17799

Опис: У відповідності зі стандартом ISO 17799, при створенні ефективної системи безпеки особливу увагу слід приділити комплексному підходу до управління інформаційною безпекою. З цих причин в якості елементів управління розглядаються не тільки технічні, але й організаційно-адміністративні заходи, спрямовані на забезпечення наступних вимог до інформації:

– конфіденційність;
– цілісність;
– достовірність;
– доступність.

Порушення кожного з них може спричинити за собою значні втрати як у вигляді збитків, так і у вигляді неотриманого доходу.

3. Інструменти

Крім методів та управляючих документів використовують інструменти для оцінки ризиків. Інструменти являють собою програмне забезпечення з документацією про правила використання. Найвідомішими інструментами, існуючими без методики з покроковою інструкцією є: Cobra, RiskWatch.

3.1. Cobra

Виробник: Великобританія.

Опис: Cobra програмний інструмент, який дозволяє проводити оцінку ризиків у галузі безпеки.

Він оцінює відносну важливість усіх загроз і вразливостей, генерує відповідні рішення та рекомендації. Це автоматично пов'язує виявлені ризики з потенційними наслідками для бізнес-одиниці. Крім того, конкретний район або питання може бути розглянуте "самостійно", без будь-яких наслідків для організації.

3.2. RiskWatch

Виробник: США.

Опис: RiskWatch являє собою сімейство програмних продуктів, побудованих на загальному програмному ядрі, які призначені для управління різними видами ризиків та підтримки великого різновиду стандартів.

У RiskWatch в якості критеріїв для оцінки та управління ризиками використовуються:

– очікувані річні втрати (Annual Loss Expectancy, ALE);
– оцінка повернення інвестицій (Return on Investment, ROI).

RiskWatch орієнтована на точну кількісну оцінку співвідношення втрат від загроз безпеки і затрат на створення системи захисту.

Висновок

Отже, важливим кроком при побудові комплексної системи захисту інформації є вибір методів, управляючих документів та інструментів. Зазвичай організації не знають, які з існуючих способів оцінки ризиків кращі саме для їх умов. Процес оцінки повинен бути адаптований до індивідуальних особливостей організації, але в той же час узгоджений з кращими стандартами та провідними практиками. У даному розділі була розглянута класифікація основних способів оцінки інформаційних ризиків. Також наведено огляд кращих методів, керівних документів та інструментів. Вибрати найкращий спосіб оцінки ризику полягає в їх детальному порівнянні, використовуючи різні критерії. Якщо критерії, які використовуються, застосовані до всіх моделей оцінки ризиків, організація може порівняти різні моделі об'єктивно і прийняти рішення про запровадження найкращих з них.

Розділ 15. Управління інформаційною та/або кібербезпекою

15.1. Управління кіберінцидентами: Поняття кіберінцидента/кібератаки. Розслідування кіберінцидентів/кібератак.

15.2. Управління ризиками в інформаційній та/або кібербезпеці: Загальна концепція управління ризиками ІБ. ISO/IEC 27005:2018, IEC 31010:2019, NIST SP 800-39, NIST SP 800-37, NIST SP 800-30, NIST SP 800-137 (Ризики інформаційної безпеки. Аналіз та оцінка ризику. Прийняття ризику. Зменшення ризику. Страхування (перекладання) ризику). Системи класу Incident Response Platform

15.1. Управління кіберінцидентами: Поняття кіберінцидента/кібератаки. Розслідування кіберінцидентів/кібератак

1.1 Поняття кіберінцидента/кібератаки

Інцидент кібербезпеки, (скорочено **кіберінцидент**) – подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів.

Хакерська атака (кібератака) – спроба реалізації загрози. Тобто, це дії кібер-зловмисників (хакерів) або шкідливих програм, які спрямовані на захоплення інформаційних даних віддаленого комп'ютера, отримання повного контролю над ресурсами комп'ютера або на виведення системи з ладу.

Під **атакою** (англ. *attack*, англ. *intrusion*) **на інформаційну систему** розуміють дії (процеси) або послідовність зв'язаних між собою дій порушника, які приводять до реалізації загроз інформаційним ресурсам шляхом використання уразливостей цієї інформаційної системи.

Типи атак на інформаційні системи:

- Віддалене проникнення (remote penetration).
- Локальне проникнення (local penetration).
- Атака на відмову в обслуговуванні (denial of service).
- Мережні сканери (network scanners).
- Сканери уразливостей (vulnerability scanners).
- Зламувачі паролів (password crackers).
- Аналізатори протоколів (sniffers).
- Спам e-mail (Mailbombing).
- Перехоплення каналу зв'язку (Man-in-the-Middle).

Атака на відмову в обслуговуванні

DoS (від англ. *Denial of Service* – Відмова в обслуговуванні) – атака, що має своєю метою змусити сервер не відповідати на запити. Такий вид атаки не передбачає отримання деякої секретної інформації, але іноді буває підмогою в ініціалізації інших атак. Наприклад, деякі програми через помилки в своєму коді можуть викликати виняткові ситуації, і при відключенні сервісів здатні виконувати код, наданий зловмисником або атаки лавинного типу, коли сервер не може обробити величезну кількість вхідних пакетів.

DDoS (від англ. *Distributed Denial of Service* – Розподілена DoS) – підтип DoS-атаки, що має ту ж мету що і DoS, але що проводяться не з одного комп'ютера, а з декількох комп'ютерів в мережі. У даних типах атак використовується або виникнення помилок, що призводять до відмови сервісу, або спрацьовування захисту, що приводить до блокування роботи сервісу, а в результаті також до відмови в обслуговуванні. DDoS використовується там, де звичайний DoS неефективний. Для цього кілька комп'ютерів об'єднуються, і кожен виробляє DoS-атаку на систему жертви. Разом це називається DDoS-атака.

Будь-яка атака являє собою не що інше, як спробу використовувати недосконаліть системи безпеки жертви або для отримання інформації, або для нанесення шкоди системі, тому причиною будь-якої вдалої атаки є професіоналізм крекерів і цінність інформації, а також недостатня компетенція адміністратора системи безпеки зокрема, недосконаліть програмного забезпечення та недостатня увага до питань безпеки в компанії в цілому.

Аналізатори протоколів *(sniffers)*

Також досить поширений вид атаки, заснований на роботі мережевої карти в режимі promiscuous mode, а також monitor mode для мереж Wi-Fi. В такому режимі всі пакети, отримані мережевою картою, пересилаються на обробку спеціальному додатку, званому сніффером. В результаті зловмисник може отримати велику кількість службової інформації: хто, звідки і куди передавав пакети, через які адреси ці пакети проходили. Найбільшою небезпекою такої атаки є отримання самої інформації, наприклад логінів і паролів співробітників, які можна використовувати для незаконного проникнення в систему під виглядом звичайного співробітника компанії.

Mailbombing

Вважається найстарішим методом атак, хоча суть його проста і примітивна: велика кількість поштових повідомлень роблять неможливими роботу з поштовими скриньками, а іноді і з цілими поштовими серверами. Для цієї цілі було розроблено безліч програм, і навіть недосвідчений користувач може зробити атаку, вказавши всього лише e-mail жертви, текст повідомлення, і кількість необхідних повідомлень. Такі програми дозволяють ховати реальний IP-адрес відправника, використовуючи для розсилки анонімний поштовий сервер. Цій атаці складно запобігти, так як навіть поштові фільтри провайдерів не можуть визначити реального відправника спаму. Провайдер може обмежити кількість листів від одного відправника, але адреса відправника і тема часто генеруються випадковим чином.

Man-in-the-Middle

Вид атаки, коли зловмисник перехоплює канал зв'язку між двома системами, і отримує доступ до всієї інформації, що передається. При отриманні доступу на такому рівні зловмисник може модифікувати інформацію потрібним йому чином, щоб досягти своєї цілі. Мета такої атаки – незаконне отримання, крадіжка або фальсифікування переданої інформації, або ж отримання доступу до ресурсів мережі. Такі атаки вкрай складно відстежити, оскільки зазвичай зловмисник знаходиться всередині організації.

Урядові політики

Уряди різних країн мають різні політики реакції на кібератаки проти інформаційних систем країни.

Україна

Законодавство України визначає: **Кібератака** – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей:

–порушення конфіденційності;

–цілісності;

–доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах;

–отримання несанкціонованого доступу до таких ресурсів;

–порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем;

–використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту.

США

26.07.2016 Президент Сполучених Штатів Америки Барак Обама підписав наказ (директиву) PPD-41, якою доповнив вже чинне законодавство новими правилами реагування на істотні кібератаки на важливі інформаційні системи країни (як урядові, так і приватні). Даним наказом визначено:

1. Кіберінцидент. Подія, що відбулась в, чи спричинена через комп'ютерну мережу, яка ставить під загрозу цілісність, конфіденційність, або доступність комп'ютерів, інформаційних або комунікаційних системи або мереж, реальної або віртуальної інфраструктури контрольованої комп'ютерами або інформаційними системами, або присутньої в них інформації. Також до кіберінцидентів можуть бути віднесені вразливості в інформаційних системах, процедурах кібербезпеки, внутрішньому управлінні або реалізації, які можуть бути використані як загроза.

2. Важливий кіберінцидент. Інцидент або сукупність інцидентів, які можуть завдати істотної шкоди національній безпеці, міжнародним відносинам, економіці Сполучених Штатів або суспільному спокою, громадянським свободам, безпеці та здоров'ю громадян Сполучених Штатів.

Також даним наказом запроваджено градацію рівня загрози від кібератак, аналогічну терористичній. Шкала має 6 градацій: від рівня 0 (білий), до рівня 5 (чорний), з проміжними рівнями 1 (зелений), 2 (жовтий), 3 (помаранчевий) та 4 (червоний).

1.2 Розслідування кіберінцидентів/кібератак

Сьогодні дуже поширене словосполучення «цифрова криміналістика», причому використовують його досить часто. Але що це таке? Взагалі **цифрова криміналістика (digitalforensics)** – це наука про розкриття злочинів, пов'язаних з комп'ютерною інформацією. Разом з тим існує більш повне визначення, яке, на мій погляд, набагато вірніше. **Комп'ютерно-технічна експертиза** – одна з різновидів судових експертиз, об'єктом якої є комп'ютерна техніка й/або комп'ютерні носії інформації, а метою – пошук й закріплення доказів. Прирахування до можливих об'єктів даного виду експертизи віддалених об'єктів, що не перебувають у повному розпорядженні експерта (насамперед, комп'ютерних мереж) поки є спірним питанням, і вирішується він по-різному.

Проводиться така експертиза як за кримінальними справами, так і за цивільними. За кримінальними справами вона може бути призначена слідчим (у рамках досудового наслідку) або судом і поручається конкретному експертові або експертній установі. Результатом експертизи є висновок експерта, який є доказом у справі. За цивільними справами експертиза може бути призначена судом, замовлена однією зі сторін або призначена нотаріусом з ініціативи тієї або іншої сторони.

Звичайно перед експертом ставляться питання такого роду:

– про наявність на досліджуваних об'єктах інформації, що відноситься до справи (у тому числі в неявному, вилученому, схованому або зашифрованому виді);

– про можливість використання досліджуваних об'єктів для певних цілей (наприклад, для доступу в мережу);

– про дії, зроблені з використанням об'єктів;

– про властивості програм для ЕОМ, зокрема про їхню приналежність до числа шкідливих;

– про ідентифікацію знайдених електронних документів, програм для ЕОМ, користувачів комп'ютера.

Разом з тим варто відзначити, що методи комп'ютерно-технічної експертизи часто використовуються при реагуванні на інциденти, пов'язані зі шкідливими програмами. При цьому в ході розслідування, як правило, експерт повинен одержати відповідь на наступні питання:

– Хто зробив атаку?

– Коли відбулася атака?

– Які сервери або робочі станції постраждали?

– Які цілі й мотиви атакуючих?

Стримування

Перше, із чого починається робота над інцидентом, – це його стримування. Фактично від вас потрібно стримати поширення зловреду й тим самим звузити можливий ареал поширення й зменшити збиток.

Чи відключати заражений комп’ютер від мережі фізично? Поширена думка, що це необхідно. Сьогодні думають, що ні. Чому? Так тому що велике поширення дістали засоби інтелектуального керування мережею, і ви сьогодні можете легко вивести будь-який комп’ютер в окрему віртуальну мережу VLAN. Адже насамперед потрібно зробити так, щоб ваша заражена система не могла взаємодіяти з мережею підприємства. А як саме ви це забезпечите, не так уже важливо. Наступним етапом у вашій роботі буде збір інформації.

Збір інформації

На даному етапі від вас буде потрібно зробити повний образ оперативної пам'яті й жорсткого диска зараженого комп'ютера. Саме в цей момент ви зможете одержати інформацію, яка дозволить зрозуміти, як ви будете працювати із зараженням.

Одним з інструментів для одержання повного образа пам'яті й копіювання жорсткого диска є програма FTK Imager Manager. FTK Imager Lite – інструмент попереднього перегляду й візуалізації даних, використовуваний для одержання даних (доказів) у судово-обґрунтованій формі шляхом створення копій даних без внесення змін у вихідні дані.

FTK Imager призначений для:

1. Створення криміналістичних копій:
– локальних жорстких дисків;
– компакт-дисків і DVD;
– флеш-накопичувачів і інших USB-пристроїв;
– папок;
– окремих файлів.
2. Перегляду файлів і папок на окремих жорстких дисках, мережних дисках, zip-дисках, компакт-дисках і DVD, флеш-накопичувачах і інших пристроях USB.
3. Попереднього перегляду вмісту судових дампів, що зберігаються на локальних або мережних дисках.
4. Перегляду в режимі тільки для читання.
5. Експорту файлів і папок із криміналістичних дампів.
6. Відновлення вилучених з «Кошика» файлів, якщо вони не були перезаписані на диску.

Створення ґешів файлів для перевірки цілісності даних з помо щью кожної із двох ґеш-функцій, доступних в FTK Imager: Message Digest 5 (MD5) і Secure Hash Algorithm (SHA-1).

7. Створення ґешів для звичайних файлів і образів дисків (включаючи файли усередині образів дисків), які згодом можна використовувати в якості зразка, щоб підтвердити цілісність ваших доказів. Ґеш, створений FTK Imager, може використовуватися для перевірки того, що ґеш дампа й ґеш диска

збігаються після створення образа й що образ залишається незмінним після створення.

Окремо хотілося б підкреслити, що за допомогою цього програмного забезпечення ви одержуєте побітову копію, включаючи нерозмічені області диска, у яких найчастіше й перебуває шкідлива програма.

Одержання образу оперативної пам'яті

Створити образ оперативної пам'яті можна, вибравши пункти меню File, Capture Memory. Урахуйте, що деякі додатки можуть перешкоджати зняттю образа оперативної пам'яті.

Якщо ви зіштовхнулися з таким, скористайтеся інструментом Belkasoft Live RAM Capturer.

Наступним кроком буде зняття образа жорсткого диска.

Зняття образа жорсткого диска

Для виконання цього кроку досліджуваний комп'ютер слід відключити. Причому, як не дивно пролунає, потрібно просто витягтися вилку з розетки, а не скористатися стандартною процедурою відключення. Чому? Так тому що при відключенні стандартним способом ви можете втратити частину тимчасових файлів, чого не можна допустити. Створення образа жорсткого диска проводиться тим же інструментом FTK Imager. Виберіть пункт меню File, а потім Createdіskimage. При цьому необхідно скопіювати весь фізичний диск, включаючи невикористовувані сектори, тому що в них можуть зберігатися файли й настроювання шкідливої програми.

Джерела доказів інциденту

Необхідно врахувати, що залежно від типу інциденту вам може знадобитися збір інформації з різних джерел.

Приведу кілька прикладів.

– Журнали міжмережевих екранів дозволять вам довідатися, які з'єднання використовувалися для підключення до зовнішньої мережі.

– Журнали контролера домену містять інформацію про те, до яких ресурсів запитувався доступ з використанням скомпрометованого облікового запису.

– Журнали сервера імен DNS містять доменні імена, які запитували шкідливі програми.

Передача даних

На наступному етапі дані передаються у відділ інформаційної безпеки або стороннім організаціям для проведення розслідування, при цьому необхідно прикладати ґеші образів. якщо образ диска зняти із використанням Ftkimager, то ґеш цього образа втримується у вікні Imagesummary. якщо ж ваша утиліта для збору даних не підтримує обчислення ґеша, то прийдеться скористатися, наприклад, утилітою hashdeep.

На цьому перший етап проведення розслідування можна вважати завершеним.

І далі фахівці з інформаційної безпеки аналізують передані дані.

З юридичної точки зору, задля встановлення змісту та обсягу повноважень суб'єктів, які здійснюють розслідування кіберінцидентів та кібератак, визначимо сутність цієї діяльності. Так, **розслідування кібератак та кіберінцидентів** – структурована сукупність дій та заходів, які здійснюються в межах забезпечення кібербезпеки України поза кримінальним процесом уповноваженими суб'єктами та спрямовані на встановлення механізму, обставин, засобів і знарядь та виконавців кіберінцидентів і кібератак, мінімізацію їх негативного впливу та шкідливих наслідків, а також вжиття заходів з попередження кіберінцидентів та кібератак у майбутньому.

Проведення розслідування кіберінцидентів та кібератак поза межами кримінального процесу означає, що особи, які його проводять, не можуть застосовувати інструментарій процесуальних, слідчих та негласних слідчих (розшукових) дій. Аналіз нормативно-правових актів, які регулюють оперативно-службову діяльність органів СБУ, дає підстави стверджувати, що з метою встановлення обставин, які підлягають з'ясуванню **під час розслідування кібератак та кіберінцидентів, співробітники СБУ мають право**:

– здійснювати опитування осіб (за їх згодою отримуючи від них усні або письмові пояснення), які можуть повідомити будь-яку інформацію, що має значення для досягнення відповідних цілей розслідування;

– отримувати від очевидців кіберінцидента чи кібератаки, службових осіб підприємства, установи, організації або інших громадян речі і документи, що мають значення для встановлення відповідних обставин кіберподії, яка є предметом розслідування;

– отримувати у встановленому порядку дані щодо загроз національній безпеці з використанням кіберпростору або будь-яких інших кіберзагроз об'єктам кібербезпеки, кібератак та/або обставин, інформація про які може сприяти запобіганню, виявленню і припиненню таких загроз, протидії кіберзлочинам, кібератакам та мінімізації їх наслідків;

– у порядку, погодженому із керівником підприємства, установи, організації, проводити візуальний і технічний огляд комп'ютерної та периферійної техніки, яка містить сліди кіберподії;

– ознайомлюватись з документами та даними, що характеризують діяльність підприємств, установ та організацій, вивчати їх, за рахунок коштів, що виділяються на утримання підрозділів, які здійснюють оперативно-розшукову діяльність, виготовляти копії з таких документів, на вимогу керівників підприємств, установ та організацій – виключно на території таких підприємств, установ та організацій;

– застосовувати спеціальне програмне забезпечення або технічні пристрої з метою отримання, збирання та накопичення інформації, необхідної для встановлення обставин кіберінцидента чи кібератаки;

– залучати до проведення окремих заходів фахівців СБУ, проводити з ними консультації та отримувати від них письмові висновки щодо предмета розслідування;

– здійснювати комп'ютерно-технічне дослідження а) зразків цифрової інформації, отриманої у ході ознайомлення з документами та даними, що

характеризують діяльність підприємств, установ та організацій, б) комп'ютерної техніки, мережевих апаратних засобів та їх комплектуючих, залучати до таких досліджень відповідних фахівців;

– за наявності підстав, передбачених ст. 207 КПК України, затримувати особу, в діях якої вбачаються ознаки кримінального правопорушення, та тимчасово вилучати її майно з метою подальшої передачі затриманої особи та вилученого майна уповноваженій службовій особі для вирішення питання про внесення даних про виявлене кримінальне правопорушення в ЄРДР та оформлення процесуального затримання особи в порядку ст. 208 КПК України

Необхідно враховувати також, що розслідування кіберінцидентів та кібератак підрозділами СБУ носить відкритий характер і здійснюється в межах захисту кібербезпеки України. Результати окремих заходів можуть використовуватись в оперативній і контррозвідувальній діяльності, якщо їх зміст відповідає таким потребам. Проте сам процесуальний порядок не визначений ні нормативно-правовими актами СБУ, ні чинним законодавством, що ускладнює реалізацію окремих повноважень та знижує ефективність протидії кіберзагрозам

15.2. Управління ризиками в інформаційній та/або кібербезпеці: Загальна концепція управління ризиками ІБ. ISO/IEC 27005:2018, IEC 31010:2019, NIST SP 800-39, NIST SP 800-37, NIST SP 800-30, NIST SP 800-137 (Ризики інформаційної безпеки. Аналіз та оцінка ризику. Прийняття ризику. Зменшення ризику. Страхування (перекладання) ризику). Системи класу Incident Response Platform

2.1 Загальна концепція управління ризиками ІБ

Управління ризиками дозволяє ефективно та раціонально вибудовувати процеси ІБ та розподіляти ресурси для захисту активів компанії, а оцінка ризиків дозволяє застосовувати доцільні заходи щодо їх мінімізації: для захисту від суттєвих та актуальних загроз логічно застосовуватиме більш дорогі рішення.

Крім цього, вибудований процес управління ризиками ІБ дозволить розробити і в разі потреби застосувати чіткі плани забезпечення безперервності діяльності та відновлення працездатності (Business Continuity & Disaster Recovery): глибока опрацювання різних ризиків допоможе заздалегідь врахувати, наприклад, раптову потребу у віддаленому доступі для великої кількості співробітників, як це може статися у разі епідемій чи колапсу транспортної системи.

Під **ризиком інформаційної безпеки, або кіберризиком**, розуміють потенційну можливість використання вразливостей активів конкретною загрозою заподіяння шкоди організації. Під величиною ризику умовно розуміють добуток ймовірності негативної події та розміру шкоди. У свою чергу, під ймовірністю події розуміється твір ймовірності загрози та небезпеки вразливості, виражені в якісній чи кількісній формі. Умовно ми можемо висловити це логічною формулою:

Величина Ризика = Ймовірність Події

Існують також умовні класифікації ризиків:

– за джерелом ризику (наприклад, атаки хакерів чи інсайдерів, фінансові помилки, вплив державних регуляторів, юридичні претензії контрагентів, негативний інформаційний вплив конкурентів);

– за метою (інформаційні активи, фізичні активи, репутація, бізнес-процеси);

– за тривалістю впливу (операційні, тактичні, стратегічні).

Управління ризиками в інформаційній та/або кібербезпеці як правило включає в себе наступні пункти:

– Визначення ризику інформаційної безпеки.
– Аналіз та оцінка ризику.
– Прийняття ризику.
– Зменшення ризику.
– Страхування (перекладання) ризику).

В цій лекції розглянемо ці пункти як у загальній концепції управління ризиками ІБ так й у відповідних стандартах: ISO/IEC 27005:2018, IEC 31010:2019, NIST SP 800-39, NIST SP 800-37, NIST SP 800-30, NIST SP 800-137.



Рисунок 15.1 – Концепції, підходи та стандарти управління ризиками ІБ

Цілі **аналізу ризиків** ІБ наступні:

1. Ідентифікувати активи та оцінити їх цінність.
2. Ідентифікувати загрози активам та вразливості у системі захисту.
3. Прорахувати ймовірність реалізації загроз та їхнього впливу на бізнес (англ. business impact).

4. Дотриматися балансу між вартістю можливих негативних наслідків та вартістю заходів захисту, дати рекомендації керівництву компанії з обробки виявлених ризиків.

Етапи з 1-го по 3-й є **оцінкою ризику** (англ. risk assessment) і є збиранням наявної інформації. Етап 4 є вже безпосередньо **аналіз ризиків** (англ. risk analysis), тобто, вивчення зібраних даних та видачу результатів/вказівок для подальших дій. У цьому важливо розуміти власний рівень упевненості у коректності проведеної оцінки. На етапі 4 також пропонуються **методи обробки для кожного з актуальних ризиків**:

– передача (наприклад, шляхом страхування);

– уникнення (наприклад, відмова від впровадження тієї чи іншої технології чи сервісу);

– прийняття (свідома готовність завдати шкоди у разі реалізації ризику);

– мінімізація (застосування заходів для зниження ймовірності негативної події, що призводить до реалізації ризику).

Збиток від реалізації атаки може бути **прямим** або **непрямим**.

– Прямий збиток – це безпосередні очевидні й легко прогнозовані втрати компанії, такі як втрати прав інтелектуальної власності, розголошення секретів виробництва, зниження вартості активів або їх часткове або повне руйнування, судові витрати та виплата штрафів і компенсацій тощо.

– Непрямі збитки можуть означати **якісні** або **непрямі** втрати.

Якісними втратами можуть бути призупинення або зниження ефективності діяльності компанії, втрата клієнтів, зниження якості вироблених товарів або послуг. **Непрямі** втрати – це, наприклад, недоотриманий прибуток, втрата ділової репутації, додатково понесені витрати. Крім цього, у зарубіжній літературі зустрічаються також такі поняття, як **тотальний ризик** (англ. total risk), який є присутнім, якщо взагалі ніяких заходів захисту не впроваджується, а також **залишковий ризик** (англ. residual risk), який присутній, якщо загрози реалізувалися, попри впроваджені заходи захисту.

Аналіз ризиків може бути як **кількісним**, і **якісним**.

Розглянемо один із способів **кількісного** аналізу ризиків. Основними показниками вважатимемо такі величини:

– **ALE** – annual loss expectancy, очікувані річні втрати, тобто, **«вартість» всіх інцидентів за рік**.

– **SLE** – single loss expectancy, очікувані разові втрати, тобто, **«вартість» одного інциденту**.

– **EF** – exposure factor, чинник відкритості перед загрозою, тобто, **який відсоток активу зруйнує загроза за її успішної реалізації**.

– **ARO** – annualized rate of occurrence, **середня кількість інцидентів на рік** відповідно до статистичних даних.

Значення SLE обчислюється як добуток розрахункової вартості активу та значення EF, тобто:

$$SLE=AssetValue*EF.$$

При цьому вартість активу слід включати і штрафні санкції за його недостатній захист.

Значення ALE обчислюється як добуток SLE та ARO, тобто:

*ALE=SLE*ARO*.

Значення ALE допоможе проранжувати ризики – ризик із високим ALE буде найкритичнішим. Далі розраховане значення ALE можна буде використовувати для визначення максимальної вартості реалізованих заходів захисту, оскільки, згідно з загальноприйнятим підходом, вартість захисних заходів не повинна перевищувати вартість активу або величину прогнозованої шкоди, а розрахункові доцільні витрати на атаку для зловмисника повинні бути меншими, ніж очікуваний ним прибуток від цієї атаки. Цінність заходів захисту також можна визначити, віднімаючи від розрахункового значення ALE до впровадження заходів захисту значення розрахункового значення ALE після впровадження заходів захисту, а також віднімаючи щорічні витрати на реалізацію цих заходів. Умовно записати цей вислів можна так:

(Цінність заходів захисту для компанії) = (ALE до впровадження заходів захисту) – (ALE після впровадження заходів захисту) – (Щорічні витрати на реалізацію заходів захисту)

Прикладами **якісного** аналізу ризиків можуть бути, наприклад, метод Дельфі, в якому проводиться анонімне опитування експертів у кілька ітерацій до досягнення консенсусу, і навіть мозковий штурм та інші приклади оцінки т.зв. «експертним методом».

Далі наведемо короткий та невичерпний **список різних методологій ризик-менеджменту**, а найпопулярніші з них ми розглянемо далі вже детально.

1. **Фреймворк «NIST Risk Management Framework»** на базі американських урядових документів NIST (National Institute of Standards and Technology, Національного інституту стандартів і технологій США) включає набір взаємопов'язаних т.зв. «спеціальних публікацій» (англ. Special Publication (SP), для простоти сприйняття називати їх стандартами):

1.1. Стандарт **NIST SP 800-39 «Managing Information Security Risk» («Управління ризиками інформаційної безпеки»)** пропонує трирівневий підхід до управління ризиками: організація, бізнес-процеси, інформаційні системи. Цей стандарт описує методологію процесу управління ризиками: визначення, оцінка, реагування та моніторинг ризиків.

1.2. Стандарт **NIST SP 800-37 «Risk Management Framework for Information Systems and Organizations» («Фреймворк управління ризиками для інформаційних систем та організацій»)** пропонує для забезпечення безпеки та конфіденційності використання підходу управління життєвим циклом систем.

1.3. Стандарт **NIST SP 800-30 «Guide for Conducting Risk Assessments» («Посібник з проведення оцінки ризиків»)** сфокусований на IT, ІБ та операційних ризиках. Він описує підхід до процесів підготовки та проведення оцінки ризиків, комунікування результатів оцінки, а також подальшої підтримки процесу оцінки.

1.4. Стандарт **NIST SP 800-137 «Information Security Continuous Monitoring» («Безперервний моніторинг інформаційної безпеки»)** описує

підхід до процесу моніторингу інформаційних систем та IT-середовищ з метою контролю застосованих заходів обробки ризиків ІБ та необхідності їх перегляду.

2. **Стандарти** Міжнародної організації зі стандартизації **ISO** (International Organization for Standardization):

2.1. Стандарт **ISO/IEC 27005:2018 «Information technology – Security techniques – Information security risk management» («Інформаційна технологія. Методи та засоби забезпечення безпеки. Менеджмент ризику інформаційної безпеки»)** входить до серії стандартів ISO 27000 і є логічно взаємопов'язаним ІБ із цієї серії. Цей стандарт відрізняється фокусом на ІБ під час розгляду процесів управління ризиками.

2.2. Стандарт **ISO/IEC 27102:2019 «Information security management – Guidelines for cyber-insurance» («Управління інформаційною безпекою. Посібник з кіберстрахування»)** пропонує підходи до оцінки необхідності придбання кіберстрахування як заходи обробки ризиків, а також до оцінки та взаємодії зі страховиком.

2.3. Серія стандартів **ISO/IEC 31000:2018** описує підхід до ризик-менеджменту без прив'язки до IT/ІБ. Він гармонізований у вигляді **ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та настанови (ISO 31000:2018, IDT).** У цій серії варто відзначити стандарт **ISO/IEC 31010:2019 «Risk management – Risk assessment techniques»** – цей стандарт у вітчизняному варіанті **ДСТУ IEC/ISO 31010:2013 Керування ризиком. Методи загального оцінювання ризику (IEC/ISO 31010:2019, IDT).**

3. Методологія **FRAP (Facilitated Risk Analysis Process)** є відносно спрощеним способом оцінки ризиків, з фокусом лише на найкритичніших активах. Якісний аналіз проводиться за допомогою експертної оцінки.

4. Методологія **OCTAVE (Operationally Critical Threat, Asset, Vulnerability Evaluation)** сфокусована на самостійній роботі членів бізнес-підрозділів. Вона використовується для масштабної оцінки всіх інформаційних систем та бізнес-процесів компанії.

5. Стандарт **AS/NZS 4360** є австралійським і новозеландським стандартом з фокусом як на IT-системах, а й у бізнес-здоров'я компанії, тобто, пропонує глобальніший підхід до управління ризиками. Зазначимо, що даний стандарт замінено на стандарт **AS/NZS ISO 31000-2009**.

6. Методологія **FMEA (Failure Modes and Effect Analysis)** пропонує проведення оцінки системи з погляду її слабких місць для пошуку ненадійних елементів.

7. Методологія **CRAMM (Central Computing and Telecommunications Agency Risk Analysis and Management Method)** пропонує використання автоматизованих засобів управління ризиками.

8. Методологія **FAIR (Factor Analysis of Information Risk)** – пропрієтарний фреймворк щодо кількісного аналізу ризиків, що пропонує модель побудови системи управління ризиками з урахуванням економічно ефективного підходу, прийняття поінформованих рішень, порівняння заходів управління ризиками, фінансових показників і точних ризик-моделей.

9. Концепція **COSO ERM (Enterprise Risk Management)** описує шляхи інтеграції ризик-менеджменту зі стратегією та фінансовою ефективністю діяльності компанії та наголошує на важливості їх взаємозв'язку. У документі описані такі компоненти управління ризиками, як стратегія та постановка цілей, економічна ефективність діяльності компанії, аналіз та перегляд ризиків, корпоративне управління та культура, а також інформація, комунікація та звітність.

Спеціальні публікації **NIST SP 800-39, NIST SP 800-37 та NIST SP 800-30** пропонують логічно пов'язаний системний підхід до **оцінки та обробки ризиків**, а **NIST SP 800-53, NIST SP 800-53A** пропонують конкретні заходи щодо **мінімізації ризиків ІБ**. Однак слід мати на увазі, що дані документи за своєю суттю мають лише рекомендаційний характер і не є стандартами (наприклад, на відміну від документів NIST FIPS), а також те, що вони спочатку розроблялися для компаній і організацій зі США. Це накладає певні обмеження їх використання: так, організації що неспроможні отримати міжнародну сертифікацію з виконання положень даних документів, а застосування всього набору пов'язаних фреймворків NIST може виявитися надмірно трудомістким і недоцільним. Найчастіше компанії обирають шлях сертифікації за вимогами Міжнародної Організації зі Стандартизації (International Organization for Standardization, ISO), отримуючи, наприклад, статус «**ISO 27001 Certified**», визнаний у всьому світі. До серії стандартів ISO 27000 входять документи, присвячені інформаційній безпеці та управлінню ризиками. Розглянемо основний документ цієї серії з управління ризиками ІБ: стандарт **ISO/IEC 27005:2018**.

2.2 ISO/IEC 27005:2018

Стандарт **ISO/IEC 27005:2018 «Information technology – Security techniques – Information security risk management» («Інформаційні технології – Техніки забезпечення безпеки – Управління ризиками інформаційної безпеки»)** є вже третьою ревізією: першу версію стандарту було опубліковано у 2005 році, а другу – у 2011. Стандарт гармонізовано в Україні у вигляді **ДСТУ ISO/IEC 27005:2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT)**.

Документ вводить кілька ризик-специфічних термінів. Так, **засобом захисту** (англ. control) називається міра, що змінює ризик. У поняття **контекстів** (англ. context) входять зовнішній контекст, що означає зовнішнє середовище функціонування компанії (наприклад, політичне, економічне, культурне середовище, а також взаємини із зовнішніми стейкхолдерами), і внутрішній контекст, що означає внутрішнє середовище функціонування компанії (внутрішні процеси, політики, стандарти, системи, цілі та культуру організації, взаємини з внутрішніми стейкхолдерами, а також договірні зобов'язання).

Ризик – це результат неточності (англ. uncertainty) при досягненні цілей; при цьому неточність означає стан нестачі інформації, що відноситься до певної події, її наслідків або ймовірності її настання.

Під **рівнем ризику** (англ. level of risk) розуміється величина ризику, виражена у творі наслідків значних подій та ймовірності виникнення цих подій.

Залишковий ризик (англ. Residual risk) – ризик, що залишився після проведення процедури обробки ризиків.

Під **оцінкою ризику** (англ. risk assessment) розуміють загальний процес ідентифікації (тобто пошуку, визначення та описи ризику), аналізу (тобто розуміння природи ризику та визначення його рівня) та оцінки небезпеки (тобто порівняння результатів аналізу ризику з ризик-критеріями визначення допустимості його величини) ризиків.

Обробка ризиків – це процес модифікації ризиків, який може включати:

– уникнення ризику шляхом відмови від дій, які можуть призвести до ризиків;

– прийняття чи збільшення ризику з метою досягнення бізнес-цілей;

– усунення джерел ризику;

– зміна ймовірності реалізації ризику;

– зміна очікуваних наслідків реалізації ризику;

– перенесення (поділ) ризику;

– збереження ризику.

Процес управління ризиками ІБ з погляду авторів стандарту ISO/IEC 27005:2018 має характеризуватися такими особливостями:

1. Оцінка ризиків ведеться з урахуванням наслідків ризиків для бізнесу та ймовірності виникнення ризиків. Здійснюються ідентифікація ризиків, їх аналіз та порівняння (з урахуванням обраного рівня ризик-толерантності).
2. Імовірність та наслідки ризиків доводяться до зацікавлених сторін та приймаються ними.
3. Встановлюється пріоритет обробки ризиків та конкретних дій щодо зниження ризиків.
4. У процес прийняття рішень щодо управління ризиками залучаються стейкхолдери, які потім також інформуються про статус управління ризиками.
5. Оцінюється ефективність проведеної обробки ризиків.
6. Контролюються та регулярно переглядаються ризики і сам процес управління ними.
7. На основі нової інформації процес управління ризиками безперервно покращується.
8. Проводиться навчання співробітників та керівників щодо ризиків та дій для їх зниження.

Сам **процес управління ризиками складається з наступних** кроків (процесів), які відповідають прийнятому в стандарті ISO 27001 підходу **PDCA (Plan – Do – Check – Act)**:

1. Визначення контексту.
2. Оцінка ризиків.
3. Розробка плану обробки ризиків.
4. Ухвалення ризиків.
5. Використання розробленого плану обробки ризиків.

6. Безперервний моніторинг та перегляд ризиків.

7. Підтримка та покращення процесу управління ризиками ІБ.

Розглянемо далі кожен із цих кроків докладніше.

2.2.1. Визначення контексту

Вхідними даними при визначенні контексту є всі релевантні ризик-менеджменту відомості про компанію. В рамках цього процесу вибирається підхід до управління ризиками, який повинен включати критерії оцінки ризиків, критерії оцінки негативного впливу (англ. impact), критерії прийняття ризиків. Крім цього, слід оцінити та виділити необхідні для здійснення даного процесу ресурси.

Критерії оцінки ризиків повинні бути вироблені для оцінки ризиків ІБ у компанії та повинні враховувати вартість інформаційних активів, вимоги до їх конфіденційності, цілісності, доступності, роль інформаційних бізнес-процесів, вимоги законодавства та договірних зобов'язань, очікування стейкхолдерів, можливі негативні наслідки для гудвілу та репутації компанії.

Критерії оцінки негативного впливу повинні враховувати рівень збитків або витрат компанії на відновлення після реалізованого ризику ІБ з урахуванням рівня значущості ІТ активу, порушення інформаційної безпеки (тобто втрати активом властивостей конфіденційності, цілісності, доступності), вимушений простий бізнес-процесів, економічні втрати, порушення планів та дедлайнів, збитки репутації, порушення вимог законодавства та договірних зобов'язань.

Критерії прийняття ризиків можна висловити як ставлення очікуваної бізнес-вигоди до очікуваного ризику. При цьому для різних класів ризиків можна застосовувати різні критерії: наприклад, ризики невідповідності законодавству можуть бути прийняті в принципі, а високі фінансові ризики можуть бути прийняті, якщо вони є частиною договірних зобов'язань. Крім цього, слід враховувати і прогнозований часовий період актуальності ризику (довгострокові та короткострокові ризики). Критерії прийняття ризиків необхідно розробляти, враховуючи бажаний (цільовий) рівень ризику з можливістю прийняття топ-менеджментом ризиків вище за цей рівень за певних обставин, а також можливість прийняття ризиків за умови подальшої обробки ризиків протягом обумовленого часового періоду.

Крім вищезгаданих критеріїв, у рамках процесу визначення контексту слід врахувати межі та обсяг (англ. scope) процесу управління ризиками ІБ: потрібно взяти до уваги бізнес-цілі, бізнес-процеси, плани та політики компанії, структуру та функції організації, застосовні законодавчі та інші вимоги, інформаційні активи, очікування стейкхолдерів, взаємодія з контрагентами. Розглядати процес управління ризиками можна у межах конкретної ІТ-системи, інфраструктури, бізнес-процесу чи межах певної частини всієї компанії.

2.2.2. Оцінка ризиків

У рамках проведення процесу оцінки ризиків компанія має оцінити вартість інформаційних активів, ідентифікувати актуальні загрози та вразливості, отримати інформацію про поточні засоби захисту та їх ефективність, визначити потенційні наслідки реалізації ризиків. В результаті оцінки ризиків компанія повинна отримати кількісну чи якісну оцінку ризиків, а

також пріоритизацію цих ризиків з урахуванням критеріїв оцінки небезпеки ризиків та цілей компанії. Сам **процес оцінки** ризиків складається з дій щодо **ідентифікації** (англ. identification) ризиків, **аналізу** (англ. analysis) ризиків, оцінки **небезпеки** (англ. evaluation) ризиків.

2.2.2.1. Ідентифікація ризиків

Метою ідентифікації ризиків є визначення того, що може статися і призвести до потенційних збитків, а також отримати розуміння того, як, де і чому ця шкода може статися. При цьому слід враховувати ризики незалежно від того, чи джерело цих ризиків під контролем організації чи ні. В рамках цього процесу слід провести:

– ідентифікацію (інвентаризацію) активів, отримавши у результаті список IT-активів та бізнес-процесів;

– ідентифікацію загроз, при цьому слід враховувати навмисні та випадкові загрози, зовнішні та внутрішні джерела загроз, а інформацію про можливі загрози можна отримувати як у внутрішніх джерел в організації (юристи, HR, IT тощо), так і зовнішніх (страхові компанії, зовнішні консультанти, статистична інформація тощо);

– ідентифікацію наявних та запланованих до впровадження заходів захисту для виключення їх дублювання;

– ідентифікацію вразливостей, які можуть бути проексплуатовані актуальними загрозами та завдати шкоди активам; у своїй слід враховувати вразливості у програмному чи апаратному забезпеченні, а й у структурі організації, її бізнес-процесах, персоналі, фізичної інфраструктурі, відносинах з контрагентами;

– ідентифікацію наслідків реалізації загроз порушення конфіденційності, цілісності, доступності IT-активів.

2.2.2.2. Аналіз ризиків

Аналіз ризиків може бути проведений з різною глибиною, залежно від критичності активів, кількості відомих уразливостей, а також з урахуванням інцидентів, що відбулися раніше. Методологія аналізу ризиків може бути як якісною, так і кількісною: як правило, спочатку застосовують якісний аналіз для виділення високопріоритетних ризиків, а потім вже для виявлених ризиків застосовують кількісний аналіз, який є більш трудомістким і дає більш точні результати.

При використанні **якісного аналізу** фахівці оперують шкалою описової оцінки небезпеки (наприклад, низька, середня, висока) потенційних наслідків деяких подій та ймовірності настання цих наслідків.

При використанні методів **кількісного аналізу** вже застосовуються чисельні величини, з урахуванням історичних даних про інциденти, що вже відбулися. Слід мати на увазі, що у разі відсутності надійних фактів, що перевіряються, кількісна оцінка ризиків може дати лише ілюзію точності.

При безпосередньо процесі аналізу ризиків спочатку проводиться оцінка потенційних наслідків інцидентів ІБ: оцінюється рівень їхнього негативного впливу на організацію з урахуванням наслідків від порушень властивостей конфіденційності, цілісності, доступності інформаційних активів. Проводяться

перевірка та аудит наявних активів з метою їхньої класифікації залежно від критичності, також оцінюється (бажано у грошових величинах) потенційний негативний вплив порушення властивостей ІБ цих активів на бізнес.

Оцінка вартості активів проводиться в рамках **аналізу негативного впливу на бізнес** (Business Impact Analysis) і може бути розрахована виходячи з вартості заміни або відновлення активів/інформації, а також наслідків втрати або компрометації активів/інформації: розглядаються фінансові, юридичні, репутаційні аспекти.

Далі проводиться оцінка імовірності виникнення інциденту, тобто, всіх потенційних сценаріїв реалізації загроз. Слід врахувати частоту реалізації загрози та легкість експлуатації вразливостей, керуючись статистичною інформацією про аналогічні загрози, а також даними про мотивацію та можливості навмисних джерел загроз (побудова моделі порушника), привабливість активів для атакуючих, наявних уразливостей, застосованих заходів захисту, а у разі розгляду ненавмисно загроз – враховувати місце розташування, погодні умови, особливості обладнання, людські помилки тощо. Залежно від необхідної точності оцінки активи можна групувати або розділяти з точки зору застосовних до них сценаріїв атак.

Нарешті проводиться визначення рівня ризиків для всіх сценаріїв із розробленого списку сценаріїв атак. Величина очікуваного ризику є вірогідністю сценарію інциденту та його наслідків.

2.2.2.3. Оцінка небезпеки ризиків

В рамках процесу оцінки небезпеки ризиків проводиться порівняння отриманих на попередньому етапі рівнів ризиків із критеріями порівняння ризиків та критеріями прийняття ризиків, отриманими на етапі визначення контексту. При прийнятті рішень слід враховувати наслідки реалізації загроз, можливість виникнення негативних наслідків, рівень власної впевненості в коректності проведеної ідентифікації та аналізу ризиків. Слід врахувати властивості ІБ активів (наприклад, якщо втрата конфіденційності нерелевантна для організації, то всі ризики, що порушують дану властивість, можна відкинути), а також важливість бізнес-процесів, що обслуговуються певним активом (наприклад, ризики, що зачіпають малозначущий бізнес-процес, можуть бути визнані низькопріоритетними).

2.2.3. Обробка ризиків ІБ

На початок здійснення цього підпроцесу ми вже маємо список приоритизованих ризиків відповідно до критеріїв оцінки небезпеки ризиків, пов'язаних зі сценаріями інцидентів, які можуть призвести до реалізації цих ризиків. В результаті проходження **етапу обробки** ризиків ми повинні вибрати **заходи захисту**, призначені для **модифікації** (англ. modification), **збереження** (англ. retention), **уникнення** (англ. avoidance) або **передачі** (англ. sharing) ризиків, а також обробити **залишкові ризики** та сформувати **план обробки ризиків**.

Зазначені опції обробки ризиків (модифікацію, збереження, уникнення або передачу) слід вибирати в залежності від результатів процесу оцінки ризиків,

очікуваної оцінки вартості впровадження заходів захисту та очікуваних переваг кожної опції, при цьому їх можна комбінувати (наприклад, модифікувати ймовірність ризику та передавати залишковий ризик). Перевагу слід віддавати легкореалізованим та низькобюджетним заходам, які при цьому дають великий ефект зниження ризиків та закривають більшу кількість загроз, а у разі необхідності застосування дорогих рішень слід давати економічне обґрунтування їх застосування. Загалом слід прагнути максимально знизити негативні наслідки, а також враховувати рідкісні, але руйнівні ризики.

Через війну відповідальними особами може бути сформований план обробки ризиків, який чітко визначає пріоритет і часовий інтервал, відповідно до якими слід реалізувати метод обробки кожного ризику. **Пріоритети** можуть бути розставлені за результатами **ранжирування ризиків** та **аналізу витрат та вигод** (англ. cost-benefit analysis). У разі, якщо в організації вже були впроваджені будь-які заходи захисту, буде розумно проаналізувати їхню актуальність та вартість володіння, при цьому слід враховувати взаємозв'язки між заходами захисту та загрозами, для захисту від яких ці заходи застосовувалися.

Після закінчення плану обробки ризиків слід визначити залишкові ризики. Для цього можуть знадобитися оновлення або повторне проведення оцінки ризиків з урахуванням очікуваних ефектів від запропонованих способів обробки ризиків.

Далі розглянемо докладніше можливі опції обробки ризиків.

2.2.3.1. Модифікація ризиків

Модифікація ризиків має на увазі таке управління ризиками шляхом застосування або зміни заходів захисту, що призводить до оцінки залишкового ризику як прийнятного. При використанні опції модифікації ризиків вибираються виправдані та релевантні заходи захисту, які відповідають вимогам, визначеним на етапах оцінки та обробки ризиків. Слід враховувати різноманітні обмеження, такі як вартість володіння засобами захисту (з урахуванням впровадження, адміністрування та впливу на інфраструктуру), тимчасові та фінансові рамки, потреба в персоналі, що обслуговує ці засоби захисту, вимоги щодо інтеграції з поточними та новими заходами захисту. Також потрібно порівнювати вартість зазначених витрат з вартістю активу, що захищається. До заходів захисту можна віднести: корекцію, усунення, запобігання, мінімізацію негативного впливу,

Результатом кроку «Модифікація ризиків» має стати список можливих заходів захисту з їх вартістю, пропонованими перевагами та пріоритетом впровадження.

2.2.3.2. Збереження ризику

Збереження ризику означає, що за результатами оцінки небезпеки ризику прийнято рішення, що подальші дії його обробці не потрібні, тобто, оцінний рівень очікуваного ризику відповідає критерію ухвалення ризику. Зазначимо, що ця опція суттєво відрізняється від хибної практики ігнорування ризику, за якої вже ідентифікований та оцінений ризик ніяк не обробляється, тобто, рішення про його прийняття офіційно не приймається, залишаючи ризик у «підвішеному» стані.

2.2.3.3. Уникнення (зменшення) ризику

При виборі даної опції приймається рішення не вести певну діяльність чи змінити умови її ведення те щоб уникнути ризику, асоційованого з цією діяльністю. Це рішення може бути ухвалене у разі високих ризиків або перевищення вартості впровадження заходів захисту над очікуваними перевагами. Наприклад, компанія може відмовитися від надання користувачам певних онлайн-послуг щодо персональних даних, виходячи з результатів аналізу можливих ризиків витоку такої інформації та вартості впровадження адекватних заходів захисту.

2.2.3.4. Передача (страхування) ризику

Ризик можна передати тій організації, яка зможе керувати ним найефективніше. Таким чином, на підставі оцінки ризиків приймається рішення про передачу певних ризиків іншій особі, наприклад, шляхом страхування кіберризиків (послуга, що набирає популярності в Україні, проте досі в рази відстає від обсягу цього ринку, наприклад, у США) або шляхом передачі обов'язку з моніторингу та реагування на інциденти ІБ провайдеру послуг MSSP (Managed Security Service Provider) або MDR (Managed Detection and Response), тобто, у комерційний SOC. При виборі опції передачі ризику слід врахувати, як і сама передача ризику може бути ризиком, і навіть те, що можна перекласти в іншу компанію відповідальність управління ризиком, але не можна перекласти її у відповідальність за негативні наслідки можливого інциденту.

2.2.4. Прийняття ризику

Вхідними даними цього етапу будуть розроблені на попередньому етапі плани обробки ризиків та оцінка залишкових ризиків. Плани обробки ризиків повинні описувати те, як оцінені ризики будуть опрацьовані для досягнення критеріїв прийняття ризиків. Відповідальні особи аналізують та погоджують запропоновані плани обробки ризиків та фінальні залишкові ризики, а також вказують усі умови, за яких це погодження виноситься. У спрощеній моделі проводиться банальне порівняння величини залишкового ризику раніше визначеним прийнятним рівнем. Проте слід враховувати, що в деяких випадках може знадобитися перегляд критеріїв прийняття ризиків, які не враховують нові обставини чи умови. У такому разі відповідальні особи можуть бути змушені прийняти такі ризики,

У результаті формується список прийнятих ризиків з обґрунтуванням до тих, які не відповідають раніше певним критеріям прийняття ризиків.

2.2.5. Використання розробленого плану обробки ризиків. Комунікування ризиків ІБ

На даному етапі здійснюється безпосереднє втілення в життя розробленого плану обробки ризиків: відповідно до прийнятих рішень закуповуються та налаштовуються засоби захисту та обладнання, укладаються **договори кібер-страхування** та **реагування на інциденти**, ведеться юридична робота з контрагентами. Паралельно до керівництва та стейкхолдерів доводиться інформація про виявлені ризики ІБ та вживані заходи щодо їх обробки з метою досягнення загального розуміння діяльності, що проводиться.

Розробляються плани комунікації ризиків ІБ для ведення скоординованої діяльності у звичайних та екстрених ситуаціях (наприклад, на випадок великого інциденту ІБ).

2.2.6. Безперервний моніторинг та перегляд ризиків

Слід враховувати, що ризики можуть непомітно змінюватися з часом: змінюються активи та їхня цінність, з'являються нові загрози та вразливості, змінюються ймовірність реалізації загроз та рівень їхнього негативного впливу. Отже, необхідно вести безперервний моніторинг змін, що відбуваються, у тому числі із залученням зовнішніх контрагентів, що спеціалізуються на аналізі актуальних загроз ІБ. Потрібно проводити регулярний перегляд як ризиків ІБ, так і застосовуваних способів їх обробки на предмет актуальності та адекватності ситуації, що потенційно змінилася. Особливу увагу слід приділяти цьому процесу в моменти істотних змін у роботі компанії та бізнес-процесів, що здійснюються (наприклад, при злиттях/поглинаннях, запусках нових сервісів, зміні структури володіння компанією тощо).

2.2.7. Підтримка та покращення процесу управління ризиками ІБ

Аналогічно безперервному моніторингу ризиків слід постійно підтримувати та покращувати сам процес управління ризиками для того, щоб контекст, оцінка та план обробки ризиків залишалися релевантними поточній ситуації та обставинам. Усі зміни та покращення потрібно узгоджувати із зацікавленими сторонами. Критерії оцінки та прийняття ризиків, оцінка вартості активів, наявні ресурси, активність конкурентів та зміни у законодавстві та контрактних зобов'язаннях повинні відповідати актуальним бізнес-процесам та поточним цілям компанії. У разі потреби потрібно змінювати чи вдосконалювати поточний підхід, методологію та інструменти управління ризиками ІБ.

2.3 IEC 31010:2019

Розглянемо тепер стисло стандарт **IEC 31010:2019 «Risk management – Risk assessment techniques» («Менеджмент ризику – Методи оцінки ризику»). ДСТУ IEC/ISO 31010:2013 Керування ризиком. Методи загального оцінювання ризику (IEC/ISO 31010:2019, IDT)**

Цей стандарт входить у серію стандартів з управління бізнес-ризиками без прив'язки безпосередньо до ризиків ІБ. «Найголовнішим» стандартом є документ **ISO 31000:2018 ”Risk management – Guidelines” («Менеджмент ризику – Керівництва»)**, **ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та настанови (ISO 31000:2018, IDT)**, який описує фреймворк, принципи та процес управління ризиками. Описаний у цьому документі процес ризик-менеджменту аналогічний розглянутому вище: визначаються контекст, межі та критерії, проводиться оцінка ризиків (що складається з ідентифікації, аналізу, оцінки небезпеки ризиків), далі йде обробка ризиків з подальшою комунікацією, звітністю, моніторингом та переглядом.

Стандарт же IEC 31010:2019 примітний тим, що в ньому наведено понад 40 різноманітних технік оцінки ризику, до кожної дано пояснення, зазначено спосіб застосування для всіх підпроцесів оцінки ризику (ідентифікація ризику, визначення джерел та причин ризику, аналіз заходів захисту, аналіз наслідків,

ймовірностей, взаємозв'язків та взаємодій, вимірювання та оцінка рівня ризику, вибір заходів захисту, звітність), а для деяких технік наведено і практичні приклади використання.

2.4 NIST Risk Management Framework

Першим набором документів буде **фреймворк управління ризиками (Risk Management Framework) американського національного інституту стандартів та технологій (NIST)**. Цей інститут випускає документи з ІБ у рамках серії стандартів FIPS (Federal Information Processing Standards, Федеральні стандарти обробки інформації) та рекомендацій SP (Special Publications, Спеціальні публікації) 800 Series. Ця серія публікацій відрізняється логічною взаємопов'язаністю, детальністю, єдиною термінологічною базою. Серед документів, що стосуються управління ризиками ІБ, слід зазначити публікації NIST SP 800-39, 800-37, 800-30, 800-137 та 800-53/53a.

Створення цього набору документів було наслідком ухвалення Федерального закону США про управління інформаційною безпекою (FISMA, Federal Information Security Management Act, 2002 р.) та Федерального закону США про модернізацію інформаційної безпеки (FISMA, Federal Information Security Modernization Act, 2014 р.). Незважаючи на декларовану «прив'язку» стандартів та публікацій NIST до законодавства США та обов'язковість їх виконання для американських державних органів, ці документи цілком можна розглядати і як відповідні для будь-якої компанії, яка прагне покращити управління ІБ, незалежно від юрисдикції та форми власності.

2.5 NIST SP 800-39

Отже, документ **NIST SP 800-39 « Управління ризиком інформаційної безпеки: Рівень організації, місії, інформаційної системи»** пропонує вендоронезалежний, структурований, але гнучкий підхід до управлінню ризиками ІБ у контексті операційної діяльності компанії, активів, фізичних осіб та контрагентів. При цьому ризик-менеджмент повинен бути цілісним процесом, що стосується всієї організації, в якій практикується ризик-орієнтоване прийняття рішень на всіх рівнях. Управління ризиком визначається в даному документі як всеосяжний процес, що включає етапи визначення (frame), оцінки (assess), обробки (respond) і моніторингу (monitor) ризиків. Розглянемо ці етапи докладніше.

1. На **етапі визначення ризиків** організації слід виявити:

– припущення ризики, тобто, ідентифікувати актуальні загрози, уразливість, наслідки, ймовірність виникнення ризиків;

– обмеження ризиків, тобто, можливості здійснення оцінки, реагування та моніторингу;

– ризик-толерантність, тобто, терпимість до ризиків – прийнятні типи та рівні ризиків, а також допустимий рівень невизначеності в питаннях управління ризиками;

– пріоритети та можливі компроміси, тобто, Необхідно пріоритизувати бізнес-процеси, вивчити компроміси, куди може піти організація під час обробки

ризиків, і навіть тимчасові обмеження та чинники невизначеності, які супроводжують цей процес.

2. На **етапі оцінки ризиків** організації слід виявити:

– небезпеки ІБ, тобто, конкретні дії, осіб чи сутності, які можуть бути загрозами для самої організації або можуть бути спрямовані на інші організації;

– внутрішні та зовнішні вразливості, включаючи організаційні вразливості у бізнес-процесах управління компанією, архітектурі ІТ-систем тощо;

– збитки організації з урахуванням можливостей експлуатації вразливостей загрозами;

– ймовірність виникнення шкоди.

Через війну організація отримує детермінанти ризику, тобто, рівень шкоди та ймовірність виникнення шкоди для кожного ризику.

Для **забезпечення процесу оцінки ризиків** організація заздалегідь визначає:

– інструменти, техніки та методології, що використовуються для оцінки ризику;

– припущення щодо оцінки ризиків;

– обмеження, що можуть вплинути на оцінки ризиків;

– ролі та відповідальність;

– способи збору, обробки та передачі інформації про оцінку ризиків у межах організації;

– методи проведення оцінки ризиків у організації;

– частоту проведення оцінки ризиків;

– способи отримання інформації про загрози (джерела та методи).

3. На **етапі реагування на ризик** організація виконує такі роботи:

– розроблення можливих планів реагування на ризик;

– оцінку можливих планів реагування на ризик;

– визначення планів реагування на ризик, допустимих з погляду ризик-толерантності організації;

– реалізацію прийнятих планів реагування на ризик.

Для забезпечення можливості реагування на ризики організація визначає типи можливої обробки ризиків (прийняття, уникнення, мінімізація, поділ або передача ризику), а також інструменти, технології та методології для розробки планів реагування, способи оцінки планів реагування та методи оповіщення про вжиті заходи реагування в рамках організації та/або зовнішніх контрагентів.

4. На **етапі моніторингу ризиків** вирішуються такі завдання:

– перевірка реалізації прийнятих планів реагування на ризик та виконання нормативних вимог ІБ;

– визначення поточної ефективності заходів реагування на ризики;

– визначення значущих для ризик-менеджменту змін у ІТ-системах та середовищах, включаючи ландшафт загроз, уразливості, бізнес-функції та процеси, архітектуру ІТ-інфраструктури, взаємини з постачальниками, ризик-толерантність організації та ін.

Організації описують методи оцінки нормативної відповідності та ефективності заходів реагування на ризики, а також те, як контролюються зміни, здатні вплинути на ефективність реагування на ризики.

Управління ризиками ведеться на рівнях організації, бізнес-процесів та інформаційних систем, при цьому слід забезпечувати взаємозв'язок та обмін інформацією між даними рівнями з метою безперервного підвищення ефективності здійснюваних дій та комунікації ризиків усім стейкхолдерам. На верхньому рівні (рівні організації) здійснюється ухвалення рішень щодо визначення ризиків, що безпосередньо впливає на процеси, що ведуть на нижчих рівнях (бізнес-процесів та інформаційних систем), а також на фінансування цих процесів.

На рівні організації здійснюються вироблення та впровадження функцій управління, що узгоджуються з бізнес-цілями організації та з нормативними вимогами: створення функції ризик-менеджменту, призначення відповідальних, впровадження стратегії управління ризиками та визначення ризик-толерантності, розробка та реалізація інвестиційних стратегій у ІТ та ІБ.

На рівні бізнес-процесів здійснюються визначення та створення ризик-орієнтованих бізнес-процесів та організаційної архітектури, яка має бути заснована на сегментації, резервуванні ресурсів та відсутності єдиних точок відмови. Крім того, на цьому рівні здійснюється розробка архітектури ІБ, яка забезпечить ефективне виконання вимог ІБ та впровадження всіх необхідних заходів та засобів захисту.

На рівні інформаційних систем слід забезпечити виконання рішень, прийнятих на вищих рівнях, а саме забезпечити управління ризиками ІБ на всіх етапах життєвого циклу систем: ініціалізації, розробки чи придбання, впровадження, використання та виведення з експлуатації. У документі наголошується на важливості стійкості (resilience) ІТ-систем, яка є показником життєздатності бізнес-функцій компанії.

Зазначимо, що у додатку «Н» до аналізованого документа наводиться опис кожного із способів обробки ризиків, перелічених у етапі реагування ризик. Так, зазначено, що в організації повинна існувати як загальна стратегія вибору конкретного способу обробки ризику в тій чи іншій ситуації, так і окремі стратегії кожного способу обробки ризиків. Вказано **основні принципи вибору того чи іншого підходу до обробки ризиків**:

- прийняття (acceptance) ризику має суперечити обраної стратегії ризик-толерантності організації та її можливості відповідати за можливі наслідки прийнятого ризику;
- уникнення (avoidance) ризику є найчастіше найнадійнішим способом обробки ризиків, проте може йти врозріз з бажанням компанії широко застосовувати ІТ-системи та технології, тому рекомендованим підходом є доцільний та всебічно зважений вибір конкретних технологій та ІТ-сервісів;
- поділ (share) та передача (transfer) ризиків – це відповідно частковий або повний поділ відповідальності за наслідки реалізованого ризику з внутрішнім або зовнішнім партнером відповідно до прийнятої стратегії, кінцева мета якої – успішність бізнес-процесів та місії організації;

– мінімізація (або пом'якшення) (mitigation) ризиків передбачає застосування стратегії мінімізації ризиків ІБ на всіх трьох рівнях організації та безпосереднє залучення систем ІБ для пом'якшення можливих наслідків реалізації ризиків. Організації слід вибудовувати бізнес-процеси відповідно до принципів захисту інформації, архітектурні рішення повинні підтримувати можливість ефективної мінімізації ризиків, мінімізація ризиків у конкретних системах має бути реалізована із застосуванням засобів та систем захисту інформації, а політики, процеси та засоби ІБ мають бути досить універсальними та гнучкими для застосування їх у динамічному та різнорідному середовищі організації, з урахуванням безперервно мінливого ландшафту загроз ІБ.

У документі також приділено велику увагу організаційній культурі та довірі постачальникам/контрагентам як факторам успішного управління ризиками. Зокрема, йдеться, що організаційна культура і топ-менеджери компанії безпосередньо впливають на обрані рішення з обробки ризиків, тому загальна стратегія ризик-менеджменту повинна враховувати ризик-апетит компанії і відображати способи управління ризиками, що реально практикуються. Моделі побудови довіри з контрагентами і постачальниками описані в додатку «G» стандарту: перераховані моделі, що базуються на перевірках контрагентів (наприклад, шляхом проведення аудитів), на довірі, що історично склалася (коли за багаторічну історію взаємовідносин контрагент не допускав порушень), на довірі третій стороні (яка проводить незалежну оцінку контрагентів), на мандатній довірі (у разі, коли регуляторними нормами встановлюються вимоги довірі такому постачальнику), і навіть гібридна модель.

2.6 NIST SP 800-37

Тепер перейдемо до документа **NIST SP 800-37 «Risk Management Framework for Information Systems and Organizations»: «Фреймворк управління ризиками для інформаційних систем та організацій: життєвий цикл систем для забезпечення безпеки та конфіденційності»).**

Актуальний документ має ревізію №2 і був оновлений у грудні 2018 для того, щоб врахувати сучасний ландшафт загроз та акцентувати увагу на важливості управління ризиками на рівні керівників компаній, підкреслити зв'язок між **фреймворком управління ризиками (Risk Management Framework, RMF**) та **фреймворком кібербезпеки (Cybersecurity Framework, CSF)**, вказати на важливість інтеграції **процесів керування конфіденційністю (англ. privacy)** та **управління ризиками ланцюжків поставок (англ. supply chain risk management, SCRM)**, а також логічно пов'язати список запропонованих **заходів захисту (контролів, англ. controls)** з документом NIST SP 800-53. Крім цього, виконання положень NIST SP 800-37 можна використовувати за необхідності провести взаємну оцінку процедур ризик-менеджменту компаній у випадках, коли цим компаніям потрібно обмінюватись даними або ресурсами. За аналогією з NIST SP 800-39 розглядається управління ризиками на рівнях організації, місії, інформаційних систем.

У NIST SP 800-37 зазначено, що Risk Management Framework (RMF) в цілому вказує на важливість розробки та впровадження можливостей щодо

забезпечення безпеки та конфіденційності в ІТ-системах протягом усього **життєвого циклу (SDLC)**, безперервної підтримки ситуаційної обізнаності про стан захисту ІТ-систем із застосуванням процесів **безперервного моніторингу (continuous monitoring, CM)** та надання інформації керівництву для прийняття зважених ризик-орієнтованих рішень. У **RMF виділено такі типи ризиків**:

– програмний ризик;

– ризик невідповідності законодавству;

– фінансовий ризик;

– юридичний ризик;

– бізнес-ризик;

– політичний ризик;

– ризик безпеки та конфіденційності (включаючи ризик ланцюжка поставок);

– проектний ризик;

– репутаційний ризик;

– ризик безпеки життєдіяльності;

– ризик стратегічного планування.

Крім цього, **Risk Management Framework**:

- надає повторюваний процес для ризик-орієнтованого захисту інформації та інформаційних систем;
- наголошує на важливості підготовчих заходів для управління безпекою та конфіденційністю;
- забезпечує категоризацію інформації та інформаційних систем, а також вибору, впровадження, оцінки та моніторингу засобів захисту;
- пропонує використовувати засоби автоматизації для управління ризиками та заходами захисту у режимі, близькому до реального часу, а також актуальні тимчасові метрики для надання інформації керівництву для прийняття рішень;
- пов'язує процеси ризик-менеджменту на різних рівнях та вказує на важливість вибору відповідальних за вживання захисних заходів.

У документі вказано **7 етапів застосування RMF**:

1. Підготовка, тобто, визначення цілей та їхня пріоритизація з точки зору організації та ІТ-систем.
2. Категоризація систем та інформації на основі аналізу можливого негативного впливу внаслідок втрати інформації (крім негативного впливу, NIST SP 800-30 також вказує ще 3 фактори ризику, що враховуються при проведенні оцінки ризику: загрози, уразливість, ймовірність події).
3. Вибір базового набору заходів захисту та їх уточнення (адаптація) зниження ризику до прийнятного рівня з урахуванням оцінки ризику.
4. Впровадження заходів захисту та опис того, як саме застосовуються заходи захисту.
5. Оцінка впроваджених заходів захисту для визначення коректності їх застосування, працездатності та продукування ними результатів, що відповідають вимогам безпеки та конфіденційності.

6. Авторизація систем або заходів захисту на основі висновку щодо прийнятності ризиків.

7. Безперервний моніторинг систем та застосованих заходів захисту для оцінки ефективності застосованих заходів, документування змін, проведення оцінки ризиків та аналізу негативного впливу, створення звітності щодо стану безпеки та конфіденційності.

Далі у публікації NIST SP 800-37 перераховуються завдання, які слід виконати кожному з етапів застосування RMF. Для кожного із завдань вказується назва задачі (контролю), перераховуються вхідні та вихідні (результуючі) дані процесу з прив'язкою до категорій відповідних контролів CSF, наводиться список відповідальних та допоміжних ролей, додатковий опис задачі, а також при необхідності даються посилання на пов'язані документи NIST.

Далі перерахуємо завдання для кожного з етапів застосування RMF.

Завдання етапу «**Підготовка**» на **рівні організації** включають:

- визначення ролей управління ризиками;
- створення стратегії управління ризиками, з урахуванням ризик-толерантності організації;
- проведення оцінки ризиків;
- вибір цільових значень заходів захисту та/або профілів із документа Cybersecurity Framework;
- визначення для ІТ-систем загальних заходів захисту, які можуть бути успадковані з більш високих рівнів (наприклад, з рівня організації чи бізнес-процесів)
- пріоритизацію ІТ-систем;
- розробку та впровадження стратегії безперервного моніторингу ефективності заходів захисту.

Завдання етапу «**Підготовка**» на **рівні ІТ-систем** включають:

- визначення бізнес-функцій та процесів, які підтримує кожна ІТ-система;
- ідентифікацію осіб (стейкхолдерів), зацікавлених у створенні, впровадженні, оцінці, функціонуванні, підтримці, виведенні з експлуатації систем;
- визначення активів, які потребують захисту;
- визначення межі авторизації для системи;
- виявлення типів інформації, що обробляються/передаються/зберігаються в системі;
- ідентифікацію та аналіз життєвого циклу всіх типів інформації, що обробляються/передаються/зберігаються в системі;
- проведення оцінки ризиків на рівні ІТ-систем та оновлення списку результатів оцінки;
- визначення вимог щодо безпеки та конфіденційності для систем та середовищ функціонування;
- визначення розташування систем у загальній архітектурі компанії;
- розподіл точок застосування вимог щодо безпеки та конфіденційності для систем та середовищ функціонування;

– формальну реєстрацію IT-систем у відповідних департаментах та документах.

Завдання етапу «**Категоризація**» включають:

– документування параметрів системи;

– категоризацію системи та документування результатів категоризації за вимогами безпеки;

– перегляд та узгодження результатів та рішень щодо категоризації за вимогами безпеки.

Завдання етапу «**Вибір набору заходів захисту**» включають:

– вибір заходів захисту для системи та середовища її функціонування;

– уточнення (адаптація) обраних заходів захисту для системи та середовища її функціонування;

– розподіл точок застосування заходів забезпечення безпеки та конфіденційності до системи та середовища її функціонування;

– документування запланованих заходів забезпечення безпеки та конфіденційності системи та середовища її функціонування у відповідних планах;

– створення та впровадження стратегії моніторингу ефективності вживаних заходів захисту, яка логічно пов'язана із загальною організаційною стратегією моніторингу та доповнює її;

– перегляд та узгодження планів забезпечення безпеки та конфіденційності системи та середовища її функціонування.

Завдання етапу «**Впровадження заходів захисту**» включають:

– впровадження заходів захисту відповідно до планів забезпечення безпеки та конфіденційності;

– документування змін до запланованих заходів захисту постфактум, виходячи з реального результату впровадження.

Завдання етапу «**Оцінка впроваджених заходів захисту**» включають:

– вибір оцінювача або команди з оцінки, відповідних типу оцінки, що проводиться;

– розроблення, перегляд та узгодження планів щодо оцінки впроваджених заходів захисту;

– проведення оцінки заходів захисту відповідно до процедур оцінки, описаних у планах оцінки;

– підготовку звітів з оцінки, що містять знайдені недоліки та рекомендації щодо їх усунення;

– виконання коригувальних дій із заходами захисту та переоцінку відкоригованих заходів;

– підготовку плану дій на підставі знайдених недоліків та рекомендації зі звітів з оцінки.

Завдання етапу «**Авторизація**» включають:

– збір авторизаційного пакета документів та відправлення його відповідальній особі на авторизацію;

– аналіз та визначення ризику використання системи або застосування заходів захисту;

– визначення та впровадження кращого плану дій при реагуванні на виявлений ризик;

– визначення прийнятності ризику використання системи чи застосування заходів захисту;

– повідомлення про результати авторизації та про будь-яку нестачу заходів захисту, що становить значний ризик для безпеки або конфіденційності.

Завдання етапу «**Безперервний моніторинг**» включають:

– моніторинг інформаційної системи та середовища її функціонування на наявність змін, що впливають на стан безпеки та конфіденційності системи;

– оцінку заходів захисту відповідно до стратегії безперервного моніторингу;

– реагування на ризик на основі результатів безперервного моніторингу, оцінки ризику, плану дій;

– оновлення планів, звітів щодо оцінки, планів дій на підставі результатів безперервного моніторингу;

– повідомлення про стан безпеки та конфіденційності системи відповідній посадовці відповідно до стратегії безперервного моніторингу;

– перегляд стану безпеки та конфіденційності системи для визначення прийнятності ризику;

– розробку стратегії виведення системи з експлуатації та виконання відповідних дій після закінчення терміну її служби.

2.7 NIST SP 800-30

Спеціальна публікація **NIST SP 800-30 Guide for Conducting Risk Assessments (Посібник з проведення оцінок ризику)** присвячена процедурі проведення оцінки ризику, яка є фундаментальним компонентом процесу управління ризиком в організації відповідно до NIST SP 800-39, поряд з визначенням, обробкою та моніторингом ризиків. Процедури оцінки ризиків використовуються для ідентифікації, оцінки та пріорітизації ризиків, що породжуються використанням інформаційних систем, для операційної діяльності організації, її активів та працівників. **Цілями оцінки ризиків** є інформування осіб, які приймають рішення, та підтримка процесу реагування на ризик шляхом ідентифікації:

– актуальних загроз як самої організації, і опосередковано іншим організаціям;

– внутрішніх та зовнішніх уразливостей;

– потенційних збитків організації з урахуванням можливостей експлуатації вразливостей загрозами;

– ймовірності виникнення цієї шкоди.

Кінцевим наслідком є обчислення детермінанти (значення) ризику, тобто, функції від розміру шкоди та ймовірності виникнення шкоди. **Оцінку ризику можна проводити на всіх трьох рівнях управління ризиками** (рівні організації, місії, інформаційних систем) за аналогією з підходом, що

застосовується в NIST SP 800-39 та NIST SP 800-37. Наголошується, що **оцінка ризиків** – це безперервний процес, що стосується всіх рівнів управління ризиками в організації, а також вимагає включення в **життєвий цикл розробки систем (SDLC)** і проводиться з частотою, адекватною цілям і обсягу оцінки.

Процес оцінки ризиків включає:

- підготовку до оцінки ризиків;
- проведення оцінки ризиків;
- комунікування результатів оцінки та передачу інформації всередині організації;
- підтримка досягнутих результатів.

У документі йдеться про важливість складання методології оцінки ризику, що розробляється організацією на етапі визначення ризиків. Вказано, що організація може вибрати одну або кілька методологій оцінки ризику, залежно від наявних ресурсів, фази SDLC, складності та зрілості бізнес-процесів, критичності/важливості інформації, що обробляється. При цьому створенням коректної методології організація підвищує якість і відтворюваність оцінок ризику, що реалізуються.

Методологія оцінки ризику зазвичай включає:

- опис процесу оцінки ризику;
- модель ризиків, що описує оцінювані фактори ризику та взаємозв'язку між ними;
- спосіб оцінки ризиків (наприклад, якісний або кількісний), що описує значення, які можуть набувати факторів ризику, і те, як комбінації цих факторів можуть бути оброблені;
- спосіб аналізу (наприклад, загрозливо-центричний, орієнтований на активи чи вразливості), що описує, як ідентифікуються та аналізуються комбінації факторів ризику.

Модель ризиків описує оцінювані фактори ризику та взаємозв'язку між ними. **Фактори ризику** – це характеристики, які використовуються в моделях ризику як вхідні дані для визначення рівнів ризиків при проведенні оцінки ризиків. Крім цього, фактори ризику використовуються при комунікуванні ризиків для виділення тих факторів, які відчутно впливають на рівні ризиків у певних ситуаціях та контекстах. **Типові фактори ризику** включають:

- загрози;
- вразливості;
- негативний вплив;
- ймовірність;
- попередні умови.

При цьому деякі фактори ризику можуть бути декомпозовані до більш детальних характеристик, наприклад, загрози можна декомпозувати до **джерел загроз (англ. threat sources)** та **подій загроз (англ. threat events).**

Загроза – це будь-яка обставина чи подія, що має потенціал негативного впливу на бізнес-процеси чи активи, співробітників, інші організації шляхом здійснення несанкціонованого доступу, руйнування, розголошення чи

модифікації інформації та/або відмови в обслуговуванні. Події загроз породжуються джерелами загроз. **Джерелом загроз** може бути навмисна дія, спрямована на експлуатацію вразливості, або ненавмисну дію, внаслідок якої вразливість була проексплуатована випадково. В цілому, **типи джерел загроз** включають:

- ворожі кібератаки чи фізичні атаки;
- людські помилки;
- структурні помилки в активах, підконтрольних організації;
- природні чи техногенні аварії чи катастрофи.

Детальність визначення подій загроз залежить від глибини побудови моделі ризиків. У разі детального розгляду моделі ризиків можна будувати сценарії загроз, які є набором з кількох подій загроз, що призводять до негативних ефектів, атрибутованих до певного джерела загроз (або кількох джерел) та впорядкованих за часом; при цьому розглядається потенційна ймовірність послідовної експлуатації кількох уразливостей, що призводить до успішної реалізації атаки. Події загроз у кібер- або фізичних атаках характеризуються набором **тактик, технік та процедур (англ. tactics, techniques, and procedures, TTPs),** про які ми вже говорили раніше.

Розглянутий документ також говорить про таке поняття, як «**зміщення загрози**» (англ. threat shifting), під яким розуміється зміна атакуючими своїх TTPs залежно від заходів захисту, вжитих компанією та виявлених атакуючими. Зміщення загрози може бути здійснено в тимчасовому домені (наприклад, спроби атакувати в інший час або розтягнути атаку в часі), цільовому домені (наприклад, вибір менш захищеної цілі), ресурсному домені (наприклад, використання атакуючими додаткових ресурсів для злому цілі), домені планування або методу атаки (наприклад, використання іншого інструментарію хакера або спроби атакувати іншими методами). Крім цього, підкреслюється, що атакуючі часто воліють шлях найменшого опору задля досягнення своєї цілі, тобто, вибирають найслабшу ланку в ланцюзі захисту.

Вразливість – це слабкість в інформаційній системі, процедурах забезпечення безпеки, внутрішніх способах захисту або особливостях конкретної реалізації/впровадження тієї чи іншої технології чи системи. Уразливість характеризується своєю небезпекою у тих розрахункової важливості її виправлення; при цьому небезпека може бути визначена залежно від очікуваного негативного ефекту експлуатації цієї вразливості. Більшість уразливостей в інформаційних системах організації виникають або через не застосовані (випадково чи навмисно) заходи ІБ, або застосовані невірно. Важливо також пам'ятати і про еволюцію загроз і самих систем, що захищаються – і в тих, і в інших згодом відбуваються зміни, які слід враховувати при проведенні переоцінки ризиків. Крім уразливостей технічного характеру в IT-системах,

Попередня умова (англ. predisposing condition) у контексті оцінки ризиків – це умова, що існує в бізнес-процесі, архітектурі або IT-системі, що впливає (знижує або збільшує) на ймовірність заподіяння шкоди загрозою. Логічними синонімами будуть терміни «схильність» (англ. susceptibility) або

«відкритість» (англ. exposure) ризику, що означають, що вразливість може бути проексплуатована загрозою заподіяння шкоди. Наприклад, SQL-сервер потенційно схильний до вразливості SQL-ін'єкції. Окрім технічних попередніх умов, слід враховувати і організаційні: так, місце розташування офісу в низині збільшує ризик підтоплення, а відсутність комунікації між співробітниками під час розробки IT-системи збільшує ризик її злому надалі.

Ймовірність виникнення загрози (англ. likelihood of occurrence) – фактор ризику, що розраховується на основі аналізу ймовірності того, що певна вразливість (або група вразливостей) може бути проексплуатована певною загрозою, з урахуванням ймовірності того, що загроза завдасть реальної шкоди. Для навмисних загроз оцінка ймовірності виникнення зазвичай оцінюється на підставі намірів, можливостей та цілей зловмисника. Для ненавмисних загроз оцінка ймовірності виникнення, як правило, залежить від емпіричних та історичних даних. При цьому можливість виникнення оцінюється на певну часову перспективу – наприклад, на наступний рік або на звітний період. У разі, якщо загроза практично повністю буде ініційована або реалізована протягом певного часового періоду, в оцінці ризиків слід враховувати очікувану частоту її. При оцінці ймовірності виникнення загрози слід враховувати стан управління та бізнес-процесів організації, попередні умови, наявність та ефективність існуючих заходів захисту. Імовірність негативного впливу означає можливість того, що при реалізації загрози буде завдано будь-якої шкоди, незалежно від її величини.

При **визначенні загальної ймовірності виникнення подій загроз** можна використовувати такі три етапи:

1. Оцінка ймовірності того, що подія загрози буде кимось ініційована (у разі навмисної загрози) або станеться сама (у разі ненавмисної).
2. Оцінка ймовірності того, що загроза, що виникла, призведе до шкоди або завдасть шкоди організації, активам, співробітникам.
3. Загальна можливість розраховується як комбінація перших двох отриманих оцінок.

Окрім цього підходу, у документі дається рекомендація не шукати абсолютно всіх взаємопов'язаних загроз і вразливостей, а сконцентруватися на тих з них, які дійсно можуть бути використані в атаках, а також на бізнес-процесах та функціях з недостатніми заходами захисту.

Рівень негативного впливу (англ. impact) події загрози – це величина шкоди, яка очікується від несанкціонованого розголошення, доступу, зміни, втрати інформації чи недоступності інформаційних систем. Організації явно визначають:

1. Процес, який використовується визначення негативного впливу.
2. Припущення, що використовуються визначення негативного впливу.
3. Джерела та методи отримання інформації про негативний вплив.
4. Логічне обґрунтування, використане визначення негативного впливу.

Крім цього, при розрахунку негативного впливу організації повинні враховувати цінність активів та інформації: можна використовувати прийняту в

компанії систему категорування інформації за рівнем значущості або результати оцінок негативного впливу на конфіденційність (Privacy Impact Assessments).

При оцінці ризиків важливим фактором є **ступінь неточності** (англ. uncertainty), що виникає через наступні, загалом, природні обмеження, такі як неможливість з точністю спрогнозувати майбутні події; недостатні наявні відомості про загрози; невідомі вразливості; нерозпізнані взаємозалежності.

З урахуванням вищесказаного **модель ризику** можна описати як наступну логічну структуру:

джерело загрози (з певними характеристиками) з певною *часткою ймовірності* ініціює *подію загрози*, яка *експлуатує вразливість* (що має певну частку небезпеки, з урахуванням попередніх умов та успішного обходу захисних заходів), внаслідок чого створюється *негативний вплив* (з певною величиною ризику як функції від розміру шкоди та ймовірності) виникнення шкоди), що породжує *ризик*.

Документ дає також рекомендації щодо використання процесу **агрегування ризиків** (англ. risk aggregation) з метою об'єднання кількох роз'єднаних або низькорівневих ризиків в один загальніший: наприклад, ризики окремих IT-систем можуть бути агреговані в загальний ризик для всієї підтримуваної ними бізнес-системи. При такому об'єднанні слід враховувати, що деякі ризики можуть реалізовуватися одночасно чи частіше, ніж це прогнозувалося. Також слід враховувати взаємозв'язки між роз'єднаними ризиками і об'єднувати їх, або, навпаки, роз'єднувати.

У NIST SP 800-30 також описані основні **способи оцінки ризиків**: кількісний (англ. quantitative), якісний (англ. qualitative) та напівкількісний (англ. semi-quantitative).

Кількісний аналіз оперує конкретними цифрами (вартістю, часом простою, витратами тощо) і найкраще підходить для проведення аналізу вигод та витрат (англ. Cost-benefit analysis), проте є досить ресурсомістким.

Якісний аналіз застосовує описові характеристики (наприклад, високий, середній, низький), що може призвести до некоректних висновків через малу кількість можливих оцінок та суб'єктивність їх виставлення.

Напівкількісний спосіб є проміжним варіантом, що пропонує використовувати більший діапазон можливих оцінок (наприклад, за шкалою від 1 до 10) для більш точної оцінки та аналізу результатів порівняння. Застосування конкретного способу оцінки ризиків залежить як від сфери діяльності організації (наприклад, у банківській сфері може застосовуватися суворіший кількісний аналіз), так і від стадії життєвого циклу системи (наприклад, на початкових етапах циклу може проводитися лише якісна оцінка ризиків, а на більш зрілих) – вже кількісна).

Нарешті, у документі також описано три основні **способи аналізу** факторів ризиків: загрозливо-центричний (англ. threat-oriented), орієнтований на активи (англ. asset/impact-oriented) або вразливість (англ. vulnerability-oriented).

Загрозо-центричний спосіб сфокусований на створенні сценаріїв загроз та починається з визначення джерел загроз та подій загроз; далі, вразливості

ідентифікуються у тих загроз, а негативний вплив пов'язують із намірами зловмисника.

Спосіб, **орієнтований на активи**, передбачає виявлення подій загроз і джерел загроз, здатних вплинути на активи; на чільне місце ставиться потенційний збиток активам.

Застосування способу, **орієнтованого на вразливість**, починається з аналізу набору попередніх умов та недоліків/слабкостей, які можуть бути проексплуатовані; далі визначаються можливі події загроз та наслідки експлуатації ними знайдених уразливостей. Документ містить рекомендації щодо комбінування описаних способів аналізу для отримання більш об'єктивної картини загроз при оцінці ризиків.

Отже, як ми вже вказали вище, NIST SP 800-30 **процес оцінки ризиків** розбивається на 4 кроки:

- підготовка до оцінки ризиків;
- проведення оцінки ризиків;
- комунікування результатів оцінки та передача інформації всередині організації;
- підтримка досягнутих результатів.

Розглянемо докладніше завдання, які виконуються на кожному з етапів.

1. Підготовка до оцінки ризиків

У межах підготовки до оцінки ризиків виконуються такі:

1.1. Ідентифікація цілі оцінки ризиків: яка інформація очікується в результаті оцінки, які рішення будуть продиктовані результатом оцінки.

1.2. Ідентифікація області (англ. scope) оцінки ризиків у контексті застосування до конкретної організації, тимчасового проміжку, відомостей про архітектуру та технології, що використовуються.

1.3. Ідентифікація специфічних припущень та обмежень, з урахуванням яких проводиться оцінка ризиків. В рамках цього завдання визначаються припущення та обмеження в таких елементах, як джерела загроз, події загроз, уразливості, попередні умови, ймовірність виникнення, негативний вплив, ризик-толерантність та рівень неточності, а також обраний спосіб аналізу.

1.4. Ідентифікація джерел попередньої інформації, джерел загроз та вразливостей, а також інформації про негативний вплив, яка використовуватиметься для оцінки ризиків. У цьому процесі джерела інформації можуть бути як внутрішніми (такими, як звіти щодо інцидентів та аудитів, журнали безпеки та результати моніторингу), так і зовнішніми (наприклад, звіти CERTів, результати досліджень та інша загальнодоступна релевантна інформація).

1.5. Ідентифікація моделі ризиків, способу оцінки ризиків та підходу до аналізу, які використовуватимуться в оцінці ризиків.

2. Проведення оцінки ризиків

У межах оцінки ризиків виконуються такі:

2.1. Ідентифікація та характеризування актуальних джерел загроз, включаючи можливості, наміри та цілі навмисних загроз, а також можливі ефекти від ненавмисних загроз.

2.2. Ідентифікація потенційних подій загроз, релевантності цих подій та джерел загроз, які можуть ініціювати події загроз.

2.3. Ідентифікація вразливостей та попередніх умов, які впливають на ймовірність того, що актуальні події загроз призведуть до негативного впливу. Її метою є визначення того, наскільки аналізовані бізнес-процеси та інформаційні системи вразливі перед ідентифікованими раніше джерелами загроз та наскільки ідентифіковані події загроз дійсно можуть бути ініційовані цими джерелами загроз.

2.4. Визначення ймовірності того, що актуальні події загроз призведуть до негативного впливу, з урахуванням характеристик джерел загроз, уразливостей та попередніх умов, а також схильності організації до цих загроз, беручи до уваги впроваджені заходи захисту.

2.5. Визначення негативного впливу, породженого джерелами загроз, з урахуванням характеристик джерел загроз, уразливостей та попередніх умов, а також схильності організації до цих загроз, беручи до уваги впроваджені заходи захисту.

2.6. Визначення ризику від реалізації актуальних подій загроз, беручи до уваги рівень негативного впливу від цих подій та ймовірність настання цих подій. У Додатку «І» до цього стандарту наведено таблицю І-2 для розрахунку рівня ризику залежно від рівнів ймовірності та негативного впливу.

3. Комунікування результатів оцінки ризиків та передачі інформації

У рамках комунікування результатів оцінки ризиків та передачі інформації виконуються такі завдання:

3.1. Комунікування результатів оцінки ризиків особам, які приймають рішення, для реагування на ризики.

3.2. Передача заінтересованим особам інформації щодо ризиків, виявлених в результаті оцінки.

4. Підтримка досягнутих результатів

У межах підтримки досягнутих результатів виконуються такі задачі:

4.1. Проведення безперервного моніторингу факторів ризику, які впливають на ризики в операційній діяльності організації, її активи, співробітників, інші організації. Цю задачу присвячено стандарт NIST SP 800-137, який ми розглянемо далі.

4.2. Актуалізація оцінки ризиків з використанням результатів безперервного моніторингу факторів ризику.

Як бачимо, документ NIST SP 800-30 пропонує досить детальний підхід до моделювання загроз та розрахунку ризиків. Цінними є також додатки до цього стандарту, що містять приклади розрахунків по кожній із підзадач оцінки ризиків, а також переліки можливих джерел загроз, подій загроз, уразливостей та попередніх умов.

2.8 NIST SP 800-137

Перейдемо тепер до огляду документа **NIST SP 800-137 «Information Security Continuous Monitoring for Federal Information Systems and Organizations» («Безперервний моніторинг інформаційної безпеки для федеральних інформаційних систем та організацій»).**

Завданням побудови стратегії безперервного моніторингу інформаційної безпеки є оцінка ефективності заходів захисту та статусу безпеки систем з метою реагування на виклики, що постійно змінюються, та завдання у сфері інформаційної безпеки. Система безперервного моніторингу ІБ допомагає надавати ситуаційну поінформованість про стан безпеки інформаційних систем компанії на підставі інформації, зібраної з різних ресурсів (таких як активи, процеси, технології, співробітники), а також наявні можливості щодо реагування на зміни ситуації. Ця система є однією з тактик у загальній стратегії управління ризиками.

Як і інші документи серії SP, у цій публікації наведено рекомендований **процесний підхід до вибудовування системи моніторингу ІБ**, що складається з:

- визначення стратегії безперервного моніторингу ІБ (включає в себе вибудовування стратегії на рівні організації, бізнес-процесів та інформаційних систем; призначення ролей та відповідальних; вибір тестового набору систем для збору даних);
- розробки програми безперервного моніторингу ІБ (включає визначення метрик для оцінки та контролю; вибір частоти проведення моніторингу та оцінки; розробку архітектури системи моніторингу);
- запровадження програми безперервного моніторингу ІБ;
- аналізу знайдених недоліків та звіту про них (включає аналіз даних; звітність з оцінки заходів захисту; звітність з моніторингу статусу захисту);
- реагування на виявлені недоліки;
- перегляду та оновлення стратегії та програми безперервного моніторингу ІБ.

У документі також надаються такі рекомендації щодо **вибору інструментів** забезпечення безперервного моніторингу ІБ:

- підтримка ними великої кількості джерел;
- використання відкритих та загальнодоступних специфікацій (наприклад, SCAP – Security Content Automation Protocol);
- інтеграція з іншим програмним забезпеченням, таким як системи Help Desk, системи управління інвентаризацією та конфігураціями, системами реагування на інциденти;
- підтримка процесу аналізу відповідності застосовним законодавчим нормам;
- гнучкий процес створення звітів, можливість «провалюватися» (англ. drill-down) у глибину даних, що розглядаються;
- підтримка систем Security Information and Event Management (SIEM) та систем візуалізації даних.

2.9 Системи класу Incident Response Platform

Як ми знаємо, на даний момент кількість інцидентів ІБ, особливо у великих компаніях, досить велика, і при реагуванні на них рахунок йде буквально на хвилини. При цьому далеко не всі можуть дозволити собі найняти велику кількість висококласних спеціалістів.

Виникає питання: як допомогти аналітикам ІБ (передусім на L1 та L2) при реагуванні на інциденти та зняти з них рутинне навантаження щодо виконання однотипних операцій?

Уявімо ситуацію, коли SIEM-система показує, що відбувається можлива атака на фінансову систему дистанційного банківського обслуговування. Зловмисники можуть викрасти гроші з рахунків фірми з хвилини на хвилину і після цього повернути кошти буде важко.

Аналітик SOC, побачивши такий інцидент, повинен за сценарієм реагування зібрати великий **обсяг допоміжної інформації:**

– ім'я атакованого сервера;

– назва фінансової системи;

– уточнити прізвище та контактні дані відповідального;

– отримати у нього додаткову інформацію.

Якщо не залишилося сумнівів у тому, що цей інцидент – »бойовий», а не хибнопозитивний, **то аналітику потрібно якнайшвидше**:

– ізолювати атакований сервер від мережі компанії;

– заблокувати скомпрометований обліковий запис,

Як бачимо, завдань – багато, і всі їх слід виконати за суворо відведений нормативами та KPI час, наприклад, за 10 хвилин. І саме тут допоможе нашому аналітику може прийти платформа **Incident Response Platform (IRP) – система автоматизації реагування на інциденти інформаційної безпеки**. Система IRP допомагає:

– виконати ряд рутинних операцій зі збору додаткової інформації;

– здійснити невідкладні дії зі стримування (англ. contain) та усунення (англ. eradicate) загрози;

– відновити (англ. recover) атаковану систему;

– оповістити зацікавлених осіб;

– зібрати та структурувати дані про розслідувані інциденти інформаційної безпеки.

Крім того, IRP дозволяє роботизувати та автоматизувати однотипні дії оператора-фахівця ІБ, які він робить при реагуванні на інциденти інформаційної безпеки, що допомагає знизити навантаження співробітника щодо виконання рутинних операцій. Давайте докладніше зупинимося на задачах реагування на інциденти інформаційної безпеки, що виконуються системами IRP.

Процеси реагування на інциденти ІБ

Для того, щоб зрозуміти, як і де коректно застосовувати та впроваджувати системи IRP, нам слід побачити процес реагування на інциденти інформаційної безпеки загалом та подумати, як можна його автоматизувати. Для цього звернімося до документа **NIST SP 800-61 «Computer Security Incident Handling**

Guide» («Посібник з обробки інцидентів комп'ютерної безпеки»). Відповідно до нього, **реагування на інциденти ІБ** складається з кількох взаємопов'язаних процесів:

1. Підготовка
2. Детектування
3. Аналіз
4. Стримування/локалізація
5. Усунення
6. Відновлення
7. Пост-інцидентні дії

Розглянемо ці процеси докладніше у тих застосування IRP-систем їх автоматизації.

1. Підготовка

Етап підготовки є попереднім та одним із ключових. На даному етапі слід зробити всю організаційну роботу, щоб дії команди реагування на інциденти ІБ були документально підтверджені та узгоджені. Політики, процедури та інструкції з реагування повинні бути максимально чіткими, докладними та зручними, щоб у разі високопріоритетного інциденту у аналітиків команди реагування було чітке розуміння того, що слід зробити в тій чи іншій ситуації. Слід регулярно проводити тренування з відпрацювання кроків, визначених у написаних документах, а також навчати персонал компанії та команду реагування коректним технічним та організаційним діям під час інциденту.

На етапі підготовки також створюються та налаштовуються playbooks або runbooks – сценарії реагування, відповідно до яких команда реагування та IRP-система будуть робити заздалегідь задані дії в залежності від деталей інциденту. Наприклад, у разі настання високопріоритетного інциденту ІБ на особливо критичній системі відповідно до playbook, член групи реагування повинен зв'язатися з керівником та відповідальною за систему особою, а IRP-платформа повинна дати команду на ізоляцію цієї системи від мережі компанії для проведення подальших розглядів.

Крім того, на етапі підготовки слід забезпечити групу реагування на інциденти всім необхідним програмним та апаратним забезпеченням (тобто видати ноутбуки, смартфони, встановити на них необхідні утиліти), а також виконати превентивні дії щодо запобігання інцидентам (захистити мережу та пристрої компанії, встановити засоби захисту інформації, провести навчання співробітників основам ІБ). У цей час платформа IRP налаштовується для ефективного застосування: до неї підключаються IT-системи та засоби захисту, з якими належить взаємодіяти при реагуванні на інциденти. Як правило, забезпечують підключення тих систем, які здатні надати фахівцю додаткову інформацію в контексті інциденту, наприклад, відомості про порушених інцидентом користувачів (контактні дані, посада, структурний підрозділ, повноваження) та пристрої (тип операційної системи, встановлене ПЗ, виконувана функція). Крім цього, підключаються і засоби захисту, які в рамках реагування на інцидент виконуватимуть завдання зі стримування та усунення загроз, наприклад, засоби захисту кінцевих точок, міжмережевих екранів та системи управління мережею.

Таким чином, до моменту виникнення інциденту інформаційної безпеки в компанії слід приходити у всеозброєнні: фахівці з реагування та система IRP повинні знаходитись у повній бойовій готовності. Це є запорукою того, що навіть якщо інцидент трапиться, його можна буде швидко локалізувати, і його наслідки не будуть надмірно руйнівними.

2. Детектування

На етапі детектування слід визначити список можливих типів інцидентів ІБ та сформулювати перелік ознак можливих інцидентів. Ознаки можна умовно поділити на прекурсори та індикатори інцидентів інформаційної безпеки:

- *прекурсор* – це ознака того, що інцидент ІБ може статися у майбутньому;
- *індикатор* – це ознака того, що інцидент уже стався або відбувається прямо зараз.

Прикладами прекурсорів інциденту інформаційної безпеки можуть бути зафіксоване інтернет-сканування відкритих портів веб-серверів компанії або виявлення вразливості в IT-системі. Прикладами індикаторів інциденту інформаційної безпеки можуть бути поява повідомлень від засобів захисту (антивіруса, міжмережевого екрану тощо) про можливу атаку, несанкціоноване видалення або модифікація даних, появу помилок та збоїв у роботі IT-систем. Слід уважно ставитися до аномалій у мережевому трафіку: несподівані сплески певного типу трафіку (наприклад, DNS) можуть свідчити про шкідливу активність. Нетипова поведінка користувачів також слід аналізувати: віддалене підключення в неробочий час із незвичайної локації може бути ознакою компрометації облікового запису.

3. Аналіз

Під час етапу аналізу інциденту основне навантаження лягає на досвід і експертизу аналітика – він має прийняти рішення, чи був зафіксований інцидент «бойовим», чи все ж таки це було хибнопозитивне спрацювання. Слід провести ідентифікацію та первинну обробку (тріаж, англ. triage): визначити тип інциденту та категорувати його. Далі визначаються **індикатори копрометації (англ. Indicators of Compromise, IoCs)**, аналізується можливий масштаб інциденту та порушені ним компоненти інфраструктури, проводиться обмежене форензик-обстеження для уточнення типу інциденту та можливих подальших кроків щодо реагування.

На цьому етапі безцінну допомогу надасть IRP-платформа завдяки тому, що вона може надати важливу контекстну інформацію, що стосується інциденту. Наведемо приклад: SIEM-система повідомляє про те, що веб-сервер компанії зазнав атаки, при цьому вразливість, що використовувалася, застосовна тільки до ОС Windows. Аналітик, подивившись у консоль IRP, відразу побачить, що атакований веб-сервер працює на ОС Linux, отже атака не могла бути успішною. Інший приклад: антивірусна система на одному з ноутбуків повідомила про вірусне зараження і про звернення до певних IP-адрес. Аналітик, скориставшись даними IRP-системи, побачить, що аналогічна мережна активність спостерігається і на кількох інших пристроях у мережі компанії, що говорить не про одиничний вірус, а про масоване зараження. Інциденту буде надано більш пріоритетний статус, він буде ескалований відповідно до матриці ескалації, і на його усунення будуть направлені додаткові ресурси. Платформа IRP допоможе

запротоколувати всі дії, виконані в рамках реагування, а також автоматизує дії щодо комунікування та ескалації інциденту.

4. Стримування/локалізація

На етапі стримування (або локалізації) інциденту головним завданням є оперативна мінімізація потенційної шкоди від інциденту ІБ та надання тимчасового вікна для ухвалення рішення щодо усунення загрози. Цього можна досягти, наприклад, оперативно включивши суворіші заборонні правила на міжмережевому екрані для зараженого пристрою, ізолювавши заражений хост від локальної мережі компанії, відключивши частину сервісів та функцій, або, нарешті, повністю вимкнувши заражений пристрій.

На даному етапі використовуються відомості про інцидент, отримані на етапі аналізу, а також дані про те, яку функцію виконує порушений інцидентом ІТ-актив, оскільки, наприклад, вимкнення критично важливого сервера може призвести до істотніших негативних наслідків для компанії, ніж просте перезавантаження некритичного сервісу на ньому. У цій ситуації IRP-платформа знову ж таки підкаже, які функції виконує сервер, як і коли його можна вимикати або ізолювати (за умови, що на етапі підготовки дана інформація була занесена до IRP). Крім цього, у playbooks IRP-системи на етапі підготовки також мають бути закладені сценарії стримування, які застосовуються для кожного конкретного типу інциденту. Наприклад, у випадку DDoS-атаки, можливо, немає сенсу вимикати атаковані сервера, а у разі вірусного зараження усередині одного сегмента мережі можна не ізолювати пристрої в іншому сегменті. На етапі стримування також проводиться аналіз подробиць атаки: яка система була першою атакована, якими тактиками, техніками та процедурами користувалися атакуючі, які командні сервери використовуються в цій атаці і т.д. Вказану інформацію допоможе зібрати IRP-система: інтеграція з **джерелами кіберрозвідки (англ. Threat Intelligence feeds)** та спеціалізованими пошуковими системами (наприклад,VirusTotal, Shodan, Censys і т.д.) дасть більш чітку і збагачену картину інциденту, що відбудеться, що допоможе ефективніше впоратися з ним. У деяких випадках може знадобитися отримати форензик-дані для подальшого проведення комп'ютерної криміналістичної експертизи, і IRP-платформа допоможе зібрати таку інформацію з атакованих пристроїв.

5. Усунення

На етапі усунення інциденту проводяться вже активні дії з видалення загрози з мережі та запобігання повторній атакі: видаляється шкідливе ПЗ, змінюються зламані облікові записи (їх можна тимчасово заблокувати, змінити пароль або, наприклад, перейменувати), встановлюються оновлення та патчі для проексплуатації налаштування засобів захисту (наприклад, для блокування IP-адреси зломщиків). Зазначені дії виконуються для всіх порушених інцидентом сутностей – і для пристроїв, і для облікових записів, і для програм.

Надзвичайно важливо ретельно усунути вразливості, які використовувалися зловмисниками, оскільки найчастіше, успішно зламавши якусь компанію, хакери повертаються в надії використовувати ті самі недоліки її захисту. При виконанні цього процесу платформа IRP дасть необхідні команди засобам захисту і збере дані про всі зачеплені інцидентом пристрої. Таким чином, швидкість реагування на інцидент інформаційної безпеки щодо усунення самої

загрози істотно зростає при використанні IRP-системи, яка буде чудовою підмогою аналітику ІБ.

6. Відновлення

На етапі відновлення слід перевірити надійність вжитих заходів захисту, повернути системи в нормальний режим роботи (business as usual), можливо, відновивши якісь системи з резервних копій або встановивши і налаштувавши їх заново. На даному етапі системи IRP допоможуть не забути всі пристрої і хронологію подій, що брали участь в інциденті, оскільки ці дані зберігаються і накопичуються в IRP протягом усього циклу розслідування інциденту.

7. Пост-інцидентні дії

На етапі пост-інцидентних дій (англ. post-incident activities) слід проаналізувати причини інциденту (англ. root cause analysis) для того, щоб звести до мінімуму ймовірність повторного аналогічного інциденту в майбутньому, а також оцінити коректність та своєчасність дій персоналу та засобів захисту, і, можливо, оптимізувати якісь процедури реагування та політики ІБ. У разі серйозного інциденту слід провести позачергове сканування інфраструктури на наявність уразливостей, пен-тесту та/або позапланового аудиту інформаційної безпеки. Логічно використовувати агреговану базу знань для ведення накопиченого досвіду реагування, що також можна зробити в IRP-платформі, в якій вже зберігається докладна інформація про інциденти ІБ, що відбулися, і про вжиті заходи реагування. У деяких випадках потрібне складання офіційного звіту щодо інциденту, особливо якщо він був серйозним або торкнувся важливих даних. Як бачимо, IRP – це ще й універсальне сховище відомостей про інциденти інформаційної безпеки з можливістю роботизування рутинних дій фахівця з інформаційної безпеки.

Висновки з застосування IRP

Підведемо підсумок. Системи IRP є автоматизованими засобами реагування на інциденти інформаційної безпеки, що реалізують контрзаходи для протидії загрозам інформаційної безпеки відповідно до заздалегідь заданих сценаріїв реагування. Сценарії реагування називаються playbooks або runbooks і є набором автоматизованих завдань з детектування загроз і аномалій в інфраструктурі, реагування і стримування загроз в режимі реального часу. Сценарії реагування діють на основі налаштовуваних правил і типів інцидентів, виконуючи ті чи інші дії в залежності від даних, що надходять із засобів захисту або інформаційних систем. Платформи IRP допомагають проводити структуроване та журнальне реагування на інциденти інформаційної безпеки на підставі правил та політик. Узагальнюючи сказане, можна зробити висновок, що система IRP – це платформа реагування на інциденти кібербезпеки, призначена для захисту інформації шляхом систематизації даних про інциденти інформаційної безпеки та роботизацію дій оператора-аналітика ІБ. Завдяки IRP-платформам команди реагування на інциденти інформаційної безпеки можуть суттєво заощадити час та зусилля при розслідуванні інцидентів ІБ, що підвищує операційну ефективність діяльності департаментів ІБ та SOC-центрів.

Розділ 16. Аудит інформаційної та/або кібербезпеки

16.1. Етапи проведення аудиту.

16.2. Аудит на основі аналізу ризиків.

16.3. Аудит на основі стандартів інформаційної безпеки (ІБ).

16.4. Аудит на основі експертних досліджень інформаційних систем (ІС).

16.5. Забезпечення безперервності бізнес-процесів: Поняття бізнес-процесу. Модель бізнес-процесу.

16.6. Розробка політик інформаційної безпеки під час забезпечення бізнес-процесів.

16.7. Дотримання політик інформаційної безпеки під час забезпечення бізнес-процесів.

16.1. Етапи проведення аудиту

Аудит інформаційної безпеки – системний процес отримання об'єктивних якісних та кількісних оцінок про поточний стан інформаційної безпеки автоматизованої системи відповідно до певних критеріїв та показників безпеки.

Інформаційна безпека (ІБ) – стан збереження інформаційних ресурсів та захищеності законних прав особистості та суспільства в інформаційній сфері.

Аудит дозволяє оцінити поточну безпеку функціонування інформаційної системи, оцінити та прогнозувати ризики, керувати їх впливом на бізнес-процеси фірми, коректно та обґрунтовано підійти до питання забезпечення безпеки її інформаційних активів, стратегічних планів розвитку, маркетингових програм, фінансових та бухгалтерських відомостей, вмісту корпоративних баз. даних. Зрештою, грамотно проведений аудит безпеки інформаційної системи дозволяє досягти максимальної віддачі від коштів, що інвестуються у створення та обслуговування системи безпеки фірми.

В Україні використовується наступний стандарт: **ДСТУ ISO/IEC 27007:2018 Інформаційні технології. Методи захисту. Настанова щодо аудиту систем управління інформаційною безпекою (ISO/IEC 27007:2017, IDT)** – Цей документ містить вказівки щодо управління програмою аудиту системи управління інформаційною безпекою (СУІБ), щодо проведення аудитів та компетентності аудиторів СУІБ, на додаток до вказівок, що містяться в ISO 19011. Цей документ стосується тих, хто потребує розуміння чи проведення внутрішніх чи зовнішніх аудитів СУІБ або управління програмою аудиту СУІБ.

Крім того, важливу роль стандартизації критеріїв грає асоціація **ISACA** (Information Systems Audit and Control Association). Ця асоціація заснована в 1969 році і в даний час об'єднує близько 20 тисяч членів із понад 100 країн. Вона підтримує діяльність більш як 12 тисяч аудиторів інформаційних систем. На допомогу професійним аудиторам, адміністраторам та зацікавленим користувачам асоціацією ISACA із залученням фахівців із провідних світових

консалтингових компаній було розроблено стандарт **CoBIT**. Цей стандарт в даний час доступний для застосування всіма бажаючими, причому ISACA (www.isaca.org) сприяє створенню організаціями свого персонального варіанту застосування стандарту (так званого **myCoBit**).

Основні напрямки діяльності в галузі аудиту безпеки інформації

Основні напрями аудиту інформаційної безпеки деталізуються такі: атестацію; контроль захищеності інформації; спеціальні дослідження технічних засобів та проектування об'єктів у захищеному виконанні.

1. Атестація об'єктів інформатизації щодо вимог безпеки інформації:

– атестація автоматизованих систем, засобів зв'язку, обробки та передачі інформації;

– атестація приміщень, призначених для проведення конфіденційних переговорів;

– атестація технічних засобів, встановлених у виділених приміщеннях.

2. Контроль захищеності інформації обмеженого доступу:

– виявлення технічних каналів витоку інформації та способів несанкціонованого доступу до неї;

– контроль ефективності засобів захисту інформації.

3. Спеціальні дослідження технічних засобів на наявність побічних електромагнітних випромінювань та наведень (ПЕМВН):

– персональні ЕОМ, засоби зв'язку та обробки інформації;

– локальні обчислювальні системи;

– оформлення результатів досліджень відповідно до вимог відповідних органів.

4. Проектування об'єктів у захищеному виконанні:

– розробка концепції інформаційної безпеки;

– проектування автоматизованих систем, засобів зв'язку, обробки та передачі в захищеному виконанні;

– проектування приміщень, призначених для проведення конфіденційних переговорів.

Види та цілі аудиту

Розрізняють зовнішній та внутрішній аудит.

Зовнішній аудит – це, як правило, разовий захід, який проводиться за ініціативою керівництва організації або акціонерів. Зовнішній аудит рекомендується (а для низки фінансових установ та акціонерних товариств потрібно) проводити регулярно. Цей вид аудиту проводиться в основному "поза" компанією та, як правило, спеціалізованими організаціями. У цьому випадку аналізуються заходи ризику від зовнішніх атак, атак із боку (навіть якщо організація захищена міжмережевими екранами). Під час проведення зовнішнього аудиту експерт здійснює:

– сканування портів, пошук уразливостей у мережевому та прикладному програмному забезпеченні,;

– спроби взаємодії з web-, поштовими та файловими серверами;

– спроби вторгнення в локальні мережі організації.

За бажанням керівництва організації, може бути здійснений спеціальний вид зовнішнього аудиту, так званий **Ethical Hacking**. У цьому випадку спеціальна організація (у світі це широко поширена практика, такі підрозділи мають спеціальну назву: “tiger team”) здійснює певні замовником види атак на сервери, сайти та хости організації.

Внутрішній аудит є безперервною діяльністю, що здійснюється на підставі документа, який зазвичай має назву «Положення про внутрішній аудит», і відповідно до плану, підготовка якого здійснюється підрозділом внутрішнього аудиту і затверджується керівництвом організації. Аудит безпеки інформаційних систем є однією із складових IT-аудиту. Внутрішній аудит зазвичай проводиться спеціальною командою з числа персоналу організації. Його завданням є оцінка ризику існуючої технології застосування інформаційної системи. Цей вид аудиту виконується із залученням засобів автоматизації аудиту, які реалізують будь-який стандарт.

Внутрішній аудит проводиться усередині мережного простору, обмеженого міжмережевим екраном організації. Він також включає сканування портів і вразливостей внутрішніх хостів організації. Крім того, аналізується організація та виконання встановленої політики безпеки, контроль та управління доступом до ресурсів, парольна політика персоналу організації та її виконання. Цей вид аудиту доповнює стандартні методики проведення аудиту вичерпнішим розглядом мережевих уразливостей.

Цілями проведення аудиту безпеки є:

– отримання об'єктивних доказів, аналіз ризиків, пов'язаних з можливістю здійснення загроз безпеці щодо ресурсів інформаційних систем (ІС);

– оцінка поточного рівня захищеності ІС;

– локалізація «вузьких місць» у системі захисту ІС;

– оцінка відповідності ІС існуючим стандартам у сфері інформаційної безпеки (ІБ);

– інвентаризація ресурсів інформаційної системи та визначення матеріалів для розробки організаційних документів, формулярів завдань та ресурсів, списків користувачів, оптимізації прав користувачів тощо;

– інвентаризація всіх видів створюваної, оброблюваної, прийнятої, переданої та ін. інформації, визначення (при необхідності уточнення) вимог забезпечення основних властивостей безпеки (конфіденційності, цілісності, доступності, спостереження) для кожного виду інформації;

– збирання даних для оцінки ефективності вживаних заходів та засобів захисту інформації;

– аналіз ефективності заходів захисту;

– аналіз складу та характеристик ресурсів (технічних та програмних), технологій обробки та передачі інформації в системі;

– аналіз телекомунікаційної складової інформаційної системи, включаючи топологію мережі, характеристики технічних та програмних засобів телекомунікацій;

– аналіз порядку допуску працівників до роботи з інформаційною системою;

– виявлення “мертвих душ” (облікових записів співробітників, звільнених із роботи, чиї облікові записи з якоїсь причини були видалені);

– аналіз існуючого порядку придбання, встановлення, оновлення та налаштування програмних засобів.

– розробка пропозицій щодо вдосконалення системи захисту інформації;

– вироблення рекомендацій щодо впровадження нових та підвищення ефективності існуючих механізмів безпеки ІС;

В результаті аудиту необхідно отримати:

– характеристику інформаційної системи як об'єкта захисту;

– формуляри робочих місць користувачів;

– формуляри завдань, які вирішуються в інформаційній системі;

– перелік завдань, які вирішуються в інформаційній системі;

– перелік видів інформації, що використовується під час вирішення завдань.

Представлені Аудитору рапорти про **інциденти системи інформаційної безпеки (СІБ)** повинні містити документацію про т.з. "слабких точках" СІБ.

До додаткових завдань, що стоять перед внутрішнім аудитором, крім надання допомоги зовнішнім аудиторам, можуть також входити:

– розробка політик безпеки та інших організаційно-розпорядчих документів щодо захисту інформації та участь у їх впровадженні в роботу організації;

– постановка завдань для IT – персоналу, що стосуються забезпечення захисту інформації;

– участь у навчанні користувачів та обслуговуючого персоналу ІС з питань забезпечення інформаційної безпеки;

– участь у розборі інцидентів, пов'язаних з порушенням інформаційної безпеки;

– інші завдання.

Основні етапи аудиту безпеки

Роботи з аудиту безпеки ІС включають ряд послідовних етапів, які в цілому відповідають етапам проведення комплексного IT-аудиту автоматизованої системи, що включає в себе:

– ініціювання процедури аудиту;

– збирання інформації аудиту;

– аналіз даних аудиту;

– вироблення рекомендацій;

– підготовку аудиторського звіту

Розглянемо ці етапи більш детально.

Ініціація процедури аудиту

Аудит повинен ініціюватися керівництвом компанії, а не відділом аудиту (аудитором). Це пов'язано з тим, що в ході аудиту буде задіяна велика кількість співробітників із різних підрозділів, при цьому дії людей мають бути скоординовані. На етапі ***ініціювання процедури аудиту*** мають бути вирішені такі організаційні питання:

– права та обов'язки аудитора мають бути чітко визначені та документально закріплені у його посадових інструкціях, а також у положенні про внутрішній (зовнішній) аудит;

– аудитором має бути підготовлений та погоджений з керівництвом план проведення аудиту;

– у положенні про внутрішній аудит має бути закріплено, зокрема, що співробітники компанії зобов'язані сприяти аудитору та надавати всю необхідну для проведення аудиту інформацію.

Для проведення обстеження формується спеціальна робоча група. До її складу входять фахівців відділів IT, а також інформаційної безпеки. Після цього видається наказ на підприємстві, у якому даються вказівки начальникам підрозділів про надання групі необхідної допомоги.

На етапі ініціювання процедури аудиту мають бути визначені межі проведення обстеження. План та межі проведення аудиту обговорюються на робочих зборах, у яких беруть участь аудитори, керівництво компанії та керівники структурних підрозділів.

Збір інформації аудиту

Етап ***збору інформації аудиту*** є найбільш складним та тривалим. Це пов'язано в основному з відсутністю необхідної документації на інформаційну систему та необхідністю щільної взаємодії аудитора з багатьма посадовими особами організації. Для отримання інформації аудитор проводить спеціальні інтерв'ю, а також досліджує інформаційну систему за допомогою спеціалізованого інструментарію.

Щоб зібрати необхідний обсяг якісної інформації для аналізу, необхідно отримати опис організаційної структури користувачів системи та обслуговуючих підрозділів. Для збору цих даних можна використовувати схеми організаційної структури користувачів та відповідних підрозділів.

В ході інтерв'ю аудитор повинен отримати відповіді на запитання про те, хто є власником інформації, хто є користувачем інформації, хто є провайдером послуг, які послуги та яким чином надаються кінцевим користувачам, які види програм функціонують у системі, скільки користувачів задіюють ці програми.

Крім того, аудитору потрібна інформація про структуру самої системи. У ході опитування аудитор повинен дізнатися, з яких компонентів складається система, якою є їх функціональність, де проходять межі корпоративної системи, як вона взаємодіє з іншими елементами IT-інфраструктури.

При цьому аудитору потрібна структурна схема системи, інформаційних потоків, опис структури інформаційного забезпечення, розміщення компонентів системи. На жаль, як правило, підготовка значної частини документації здійснюється під час аудиту.

Аналіз даних аудиту

Методи аналізу даних, що використовуються аудиторами, визначаються обраними підходами до проведення аудиту, які можуть істотно відрізнятися.

Перший підхід, найскладніший, базується на аналізі ризиків. Спираючись на методи аналізу ризиків, аудитор визначає для обстежуваної ІС індивідуальний набір вимог безпеки, що найбільше враховує особливості даної ІС, середовища її функціонування та існуючі в цьому середовищі загрози безпеці.

Другий підхід, найпрактичніший, спирається на використання стандартів інформаційної безпеки. Стандарти визначають базовий набір вимог безпеки для широкого класу ІС, що формується внаслідок узагальнення світової практики. Стандарти можуть визначати різні набори вимог безпеки, залежно від рівня захищеності ІС, який потрібно забезпечити, її приналежності (комерційна організація чи державна установа), а також призначення (фінанси, промисловість, зв'язок тощо). Від аудитора у разі потрібно правильно визначити набір вимог стандарту, відповідність яким потрібно забезпечити.

Третій підхід, найефективніший, передбачає комбінування перших двох. Базовий набір вимог безпеки, що пред'являються ІС, визначається стандартом. Додаткові вимоги, які максимально враховують особливості функціонування даної ІС, формуються на основі аналізу ризиків.

Вироблення рекомендацій аудиту

Рекомендації, що видаються аудитором за результатами аналізу стану ІС, визначаються підходом, особливостями обстежуваної ІС, станом справ з інформаційною безпекою і ступенем деталізації, що використовується при проведенні аудиту. У будь-якому разі, рекомендації аудитора повинні бути конкретними та застосовними до цієї ІС, економічно обґрунтованими, аргументованими (підкріпленими результатами аналізу) та відсортованими за ступенем важливості. При цьому заходи щодо захисту організаційного рівня практично завжди мають пріоритет над конкретними програмно-технічними методами захисту. Водночас наївно очікувати від аудитора, як результат проведення аудиту, видачі технічного проекту підсистеми інформаційної безпеки, або детальних рекомендацій щодо впровадження конкретних програмно-технічних засобів захисту інформації.

Підготовка аудиторського звіту

Аудиторський звіт є основним результатом аудиту. Його якість характеризує якість роботи аудитора. Він повинен, принаймні, містити:

– опис цілей проведення аудиту;

– характеристику обстежуваної ІС;

– вказівку меж проведення аудиту та використовуваних методів;

– результати аналізу даних аудиту;

– висновки, що узагальнюють ці результати та містять оцінку рівня захищеності автоматизованої системи (АС) або відповідність її вимогам стандартів;

– рекомендації аудитора щодо усунення існуючих недоліків та вдосконалення системи захисту.

16.2. Аудит на основі аналізу ризиків

Базовим поняттям аудиту на основі аналізу ризиків є **Система менеджменту інформаційної безпеки (СМІБ, ISMS)** – частина загальної системи менеджменту, що ґрунтується на оцінці ділових ризиків з метою створити, впровадити, експлуатувати, постійно контролювати, аналізувати, підтримувати в робочому стані і покращувати захист інформації (ЗІ).

Система менеджменту складається з організаційної структури, політики, діяльності щодо планування, відповідальності, практик, процедур, процесів та ресурсів.

В якості об'єкта аудиту може виступати як інформаційно-телекомунікаційна система (ІТС) організації в цілому, так і її окремі складові, що забезпечують обробку інформації, яка підлягає захисту.

Варіанти аудиту СМІБ:

– плановий внутрішній аудит;

– позаплановий внутрішній аудит;

– пошук загроз;

– моделювання загроз.

Система менеджменту інцидентів інформаційної безпеки (СМІІБ) є базовою складовою загальної СМІБ і дозволяє виявляти, враховувати, реагувати і аналізувати події та інциденти інформаційної безпеки. Без реалізації цих процесів неможливо забезпечити рівень захищеності, адекватний сучасним стандартам і галузевим нормам. Для найбільш ефективної реалізації СМІІБ необхідно спиратись на вимоги міжнародних і галузевих стандартів, таких як **ISO/IEC 27001:2013** «Information security management systems. Requirements», **ITU-T X-1051** «Information security management systems. Requirements for telecommunications», а також **ISO/IEC 27035:2011** «Information technology. Security techniques. Information security incident management».

Оцінка рівня безпеки ІС за допомогою визначення ризиків інформаційної безпеки

Після збору необхідної інформації проводиться її аналіз з метою оцінки поточного рівня захищеності системи. У процесі такого аналізу визначаються ризики інформаційної безпеки, яким схильна компанія. Фактично ризик являє собою інтегральну оцінку того, наскільки ефективно існуючі засоби захисту здатні протистояти інформаційним атакам.

Зазвичай виділяють дві основні групи методів розрахунку ризиків безпеки.

Перша група дозволяє встановити рівень ризику шляхом оцінки ступеня відповідності певним набором вимог до інформаційної безпеки. Як джерела таких вимог можуть виступати:

– нормативно-правові документи підприємства, що стосуються питань інформаційної безпеки (політика безпеки, регламенти, накази, розпорядження);

– вимоги чинного українського законодавства;

– рекомендації міжнародних стандартів – ISO 17799, OCTAVE, CoBIT, BS 7799-2 і т. д.;

– рекомендації компаній-виробників програмного і апаратного забезпечення – Microsoft, Oracle, Cisco і т. д.

Друга група методів оцінки ризиків інформаційної безпеки базується на визначенні ймовірності реалізації атак, а також рівнів їх збитку.

Значення ризику обчислюється окремо для кожної атаки і в загальному випадку є як добуток імовірності проведення атаки а на величину можливого збитку від цієї атаки:

$$Ризик\ (a) = P\ (a) \bullet Збиток\ (a).$$

Значення шкоди визначається власником інформаційного ресурсу, а ймовірність атаки обчислюється групою експертів, які проводять процедуру аудиту. Імовірність в даному випадку розглядається як міра того, що в результаті проведення атаки порушники досягли своїх цілей і завдали шкоди компанії.

Методи обох груп можуть використовувати **кількісні** або **якісні** шкали для визначення величини ризику інформаційної безпеки.

У першому випадку **(кількісна шкала**) для ризику і всіх його параметрів беруться чисельні вираження. Наприклад, при використанні кількісних шкал ймовірність проведення атаки P (a) може виражатися числом в інтервалі [0,1], а збиток від атаки – задаватися у вигляді грошового еквівалента матеріальних втрат, які може понести організація в разі успішної атаки. При використанні якісних шкал числові значення замінюються на еквівалентні їм понятійні рівні. Кожному понятійному рівню в цьому випадку буде відповідати певний інтервал кількісної шкали оцінки. Кількість рівнів може варіюватися в залежності від застосовуваних методик оцінки ризиків.

Для обчислення рівня ризику за **якісними шкалами** застосовуються спеціальні таблиці, в яких в першому стовпці задаються понятійні рівні збитку, а в першому рядку – рівні ймовірності атаки. Осередки же таблиці, розташовані на перетині відповідних рядків і стовпців, містять рівень ризику безпеки. Розмірність таблиці залежить від кількості концептуальних рівнів ймовірності атаки і шкоди.

При розрахунку значень ймовірності атаки, а також рівня можливого збитку використовують статистичні методи, експертні оцінки або елементи теорії прийняття рішень. Статистичні методи передбачають аналіз вже накопичених даних про реально траплялися інциденти, пов’язані з порушенням інформаційної безпеки. На основі результатів такого аналізу будуються припущення про ймовірність проведення атак і рівнях збитку від них в інших ІС. Однак статистичні методи не завжди вдається застосувати через нестачу статистичних даних про раніше проведених атаках на ресурси ІС, аналогічної тій, яка виступає в якості об’єкта оцінки.

Активний аудит інформаційних систем

Одним з найпоширеніших видів аудиту є активний аудит. Він полягає у дослідженні стану захищеності ІС з точки зору зловмисника (або зловмисника, що володіє високою кваліфікацією в галузі ІТ).

Найчастіше компанії-постачальники послуг активного аудиту іменують його **інструментальним аналізом захищеності**, щоб відокремити даний вид аудиту від інших.

Сутність активного аудиту полягає в тому, що за допомогою спеціального програмного забезпечення (у тому числі систем аналізу захищеності) і спеціальних методів, здійснюється збір інформації про стан системи мережевого захисту. Під станом системи мережевого захисту розуміють лише ті параметри і налаштування, використання яких допомагає зловмисникові проникнути в мережі і нанести збитки компанії.

При здійсненні даного виду аудиту система мережевого захисту піддається якомога більшій кількості мережевих атак, які може виконати зловмисник. При цьому аудитор штучно ставиться саме в ті умови, в яких працює зловмисник. Йому надається мінімум інформації, тільки та, яку можна здобути у відкритих джерелах.

Атаки тільки моделюються і не завдають будь-якого деструктивного впливу ІС. Їх різноманітність залежить від використовуваних систем аналізу захищеності і кваліфікації аудитора.

Активний аудит умовно можна розділити на два види – зовнішній і внутрішній.

При **зовнішньому активному** аудиті фахівці моделюють дії зовнішнього зловмисника. У даному випадку проводяться наступні процедури:

–визначення доступних із зовнішніх мереж IP-адрес підприємства;

–сканування даних адрес з метою визначення працюючих сервісів і служб, а також призначення відсканованих хостів;

–визначення версій сервісів і служб хостів, що скануються;

–вивчення маршрутів проходження трафіку до хостів замовника;

–збір інформації про ІС замовника з відкритих джерел;

–аналіз отриманих даних з метою виявлення уразливостей.

Внутрішній активний аудит за складом робіт аналогічний зовнішньому, однак при його проведенні за допомогою спеціальних програмних засобів моделюються дії «внутрішнього» зловмисника.

Даний розподіл активного аудиту на «зовнішній» і «внутрішній» актуальний для підприємства в таких випадках:

–існують фінансові обмеження на придбання послуг і продуктів ЗІ;

–модель зловмисника, яка існує, не містить «внутрішніх» зловмисників;

–розслідується факт обходу системи мережевого захисту.

Найчастіше організація у своїй ІС використовує спеціалізоване програмне забезпечення (ПЗ) власної розробки, призначене для вирішення нестандартних завдань (наприклад, корпоративний інформаційний портал, різні бухгалтерські системи або системи документообігу). Подібні ПЗ унікальні, тому яких-небудь готових засобів і технологій для аналізу їх захищеності та відмовостійкості не існує. У даному випадку проводяться спеціалізовані дослідження, спрямовані на оцінку рівня захищеності конкретного ПЗ.

Також під час активного аудиту здійснюється **дослідження виробленості і стабільності системи, або стрес-тестування**. Воно спрямоване на визначення

критичних точок навантаження, при якій система внаслідок атаки на відмову в обслуговуванні або підвищеної завантаженості перестає адекватно реагувати на легітимні (визначені політикою безпеки) запити користувачів.

Стрес-тест дозволить виявити «вузькі» місця у процесі формування та передачі інформації і визначити ті умови, за яких нормальна робота системи неможлива. Таке тестування передбачає моделювання атак на відмову в обслуговуванні запитів користувача до системи і загальний аналіз її продуктивності.

Результатом активного аудиту є інформація про всі уразливості, ступені їх критичності і методи усунення, відомості про загальнодоступну інформацію (інформацію, доступну будь-якому потенційному порушнику) мережі замовника.

За результатами активного аудиту надаються рекомендації з модернізації системи мережевого захисту, які дозволяють усунути небезпечні уразливості, і таким чином підвищити рівень захищеності ІС від дій «зовнішнього» зловмисника при мінімальних витратах на ІБ.

Однак без проведення інших видів аудиту ці рекомендації можуть виявитися недостатніми для створення «ідеальної» системи мережевого захисту. Наприклад, за результатами даного виду аудиту неможливо зробити висновок про коректність, з точки зору безпеки, проекту ІС.

16.3. Аудит на основі стандартів ІБ

Аудит на основі стандартів ІБ – аудит ІБ на відповідність міжнародним стандартам, наприклад, стандарту **ISO/IEC 27001** «Інформаційні технології. Методи забезпечення безпеки. Системи менеджменту інформаційної безпеки. Вимоги», розробленому Міжнародною організацією зі стандартизації (ISO) і Міжнародною електротехнічною комісією (IEC) на основі британського стандарту **BS 7799-2:2002** «Системи управління інформаційною безпекою. Специфікація і керівництво по застосуванню».

При проведенні цього виду аудиту реальний стан ІБ компанії порівнюється з вимогами щодо безпеки, описаними в обраному стандарті.

Звіт, складений за результатами проведення даного виду аудиту, має містити таку інформацію:

– ступінь відповідності ІТС, що перевіряється, обраному стандарту;

– ступінь відповідності внутрішнім вимогам компанії з питань ІБ;

– кількість і категорії отриманих невідповідностей і зауважень;

– рекомендації з побудови або модифікації системи забезпечення ІБ, які дозволяють привести її у відповідність до даного стандарту;

– детальне посилання на основні документи підприємства, включаючи політику безпеки, опис процедур забезпечення ІБ, додаткові обов'язкові і необов'язкові стандарти і норми, які застосовуються у даній компанії;

– перелік політик, інструкцій, посібників, положень, необхідність яких визначена в стандартах та рекомендації щодо їх розробки.

Після вибору виду аудиту необхідно приділити увагу **вибору аудитора**. Аудитором повинна бути організація, що має багаторічний досвід проведення аудитів, професіоналізм виконавця, підтверджений кваліфікацією його співробітників. Помилковою є думка, що аудит може бути проведений «своїми силами», тобто співробітниками організації, оскільки це не дасть необхідного рівня об'єктивності, і навряд чи співробітники компанії мають необхідний досвід, навички та кваліфікацію.

Підводячи підсумки, необхідно зазначити, що аудит особливо необхідний компаніям які розвиваються, з огляду на те, що він забезпечить своєчасне виявлення загроз ІБ, каналів витоку інформації та відповідні заходи реагування на виявлені уразливості. Вчасно проведений аудит ІБ допоможе уникнути збитків та негативних наслідків.

Діагностичний аналіз СМІБ за вимогами ISO/IEC 27001

Одним із етапів впровадження СМІБ є первинний аналіз. Виконання даного аналізу – це основа для побудови чіткого і зрозумілого плану робіт. Тільки після проведення первинного аналізу СМІБ можна говорити про конкретний алгоритм дій, які належить реалізувати у процесі аудиту.

Результатами первинного аналізу є:

– уявлення про існуючий рівень управління ІБ підприємства;

– перелік робіт з приведення СМІБ у відповідність до стандарту ISO/IEC 27001.

Для того, щоб визначити існуючий рівень СМІБ, необхідно мати чіткі критерії – **вимоги стандарту**. Перелік вимог надає можливість провести діагностичний аналіз СМІБ з певною точністю. Відповідно до цих вимог необхідно скласти опитувальник з варіантами відповідей, який має охоплювати всі розділи і пункти стандарту, містити чіткі, зрозумілі і прості питання. Наприклад: «Чи існує документована методика управління ризиками?». У даному випадку можуть бути варіанти відповідей «Так» або «Ні». Якщо є документ з такою назвою, відповідь має бути позитивною. Разом з тим, це питання не розкриває повністю виконання вимог стандарту. Тому необхідні й так звані «складні» питання.

Складання опитувальника досить трудомісткий і тривалий процес. З огляду на це, австралійською компанією **Bridge Point розроблено типовий опитувальник** та запропоновано використовувати його фахівцям, які проводять діагностичний аналіз СМІБ за вимогами **ISO/IEC 27001**.

Переваги даного опитувальника:

1. Безкоштовно доступний на сайті компанії Bridge Point.
2. Оновлюється, а значить вдосконалюється.
3. Дозволяє з достатньо високим ступенем адекватності оцінити поточний стан СМІБ.
4. Структурований відповідно до розділів стандарту (напрямків безпеки).
5. Простий у використанні.
6. Враховує важливість (вагу, значущість) кожного питання.
7. Автоматизований, надає можливість зручно реєструвати відповіді.
8. Автоматично розраховує результати.
9. Автоматично надає результат аналізу в зручному вигляді.
10. Дозволяє фіксувати і порівнювати стан СМІБ через інтервали часу.

16.4. Аудит на основі експертних досліджень ІС

Експертний аудит можна умовно представити як порівняння стану ІБ з «ідеальним» описом, що передбачає:

– вимоги, які були висунуті керівництвом у процесі проведення аудиту;

– опис «ідеальної» системи безпеки, заснованої на акумульованому у компанії-аудитора загальновідомому та власному досвіді.

При виконанні експертного аудиту проводяться наступні види робіт:

– збір первинних даних про систему ІБ, про її функції й особливості, використовувані технології автоматизованої обробки та передачі даних (з урахуванням найближчих перспектив розвитку);

– збір інформації про наявні організаційно-розпорядчі документи щодо забезпечення ІБ і їх аналіз;

– визначення точок відповідальності систем, пристроїв і серверів ІС;

– формування переліку підсистем кожного підрозділу компанії з категоруванням критичної інформації та схемами інформаційних потоків.

Одним із найбільших за обсягом видом робіт серед тих, які проводяться при експертному аудиті, є збір даних про ІС шляхом інтерв'ювання представників замовника і заповнення ними спеціальних анкет.

Основна мета інтерв'ювання технічних фахівців – збір інформації про функціонування мережі, а керівного складу компанії – з’ясування вимог, які висуваються до системи ІБ.

16.5. Забезпечення безперервності бізнес-процесів: Поняття бізнес-процесу. Модель бізнес-процесу

Бі́знес-проце́с (англ. *Business Process*) – будь-яка діяльність, що має вхідний продукт, додає вартість до нього, та забезпечує вихідний продукт для внутрішнього або зовнішнього споживача.

Існують три види бізнес-процесів:

– **процеси управління** – бізнес-процеси, які управляють функціонуванням системи. Прикладом керувального процесу може служити корпоративне управління та стратегічний менеджмент.

– **основні** – бізнес-процеси, які складають основний бізнес компанії і створюють основний потік доходів. Прикладами операційних бізнес-процесів є постачання, виробництво, маркетинг та збут.

– **забезпечувальні** – бізнес-процеси, які обслуговують основний бізнес. Наприклад, бухгалтерський облік, кадрове, інформаційне забезпечення.

Бізнес-процес починається з попиту споживача і закінчується його задоволенням.

Таблиця 16.1 – Приблизна схема і дефініція бізнес-процесів банку

Об'єкт управління	**Бізнес-процес**
Бізнес-система	Вироблення узгоджених умов діяльності
Технологія	Розробка нових і модифікація наявних продуктів
Клієнт	Продаж активних продуктів
Постачальники фінансових ресурсів	Залучення ресурсів
Персонал	Відтворення персоналу
Технологічні засоби	Відтворення технологічних засобів
Фінанси і стійкість банку	Управління фінансами
Розпорядження на проведення операцій	Операційна діяльність

Власник бізнес-процесу

Власник бізнес-процесу (англ. *Process Owner*) – роль, яку виконує особа, яка несе постійну відповідальність й звітує за успішне проектування, розробку, виконання і ефективність усього наскрізного (крос-функціонального) бізнес-процесу. Ця функція може бути оформлена у вигляді посади на повну ставку або у вигляді додаткових обов'язків для когось з основної або допоміжної служби. Володілець процесу з лав керівництва (володільці процесів рівня підприємства й директор з бізнес-процесів) зазвичай несуть фінансову відповідальність за групи бізнес-процесів. Вони первісно зацікавлені в успішному виконані крос-функціональних бізнес-процесів, які мають ключове значення для успіху компанії.

Наявність власника – необхідна умова успішності бізнес-процесу. Бізнес-процес без власника, який має серйозний вплив в організації, подібен кораблю без штурвала, гвинта і вітрил – такий процес не буде виконуватися у найбільш ефективний і результативний спосіб.

Компоненти бізнес-процесу

Входи бізнес-процесу

Ресурси або дані, які мають бути, й тригери (різні типи подій), які ініціюють процес.

Виходи бізнес-процесу

Виходи – це результати діяння на входи механізмів, які управляються згідно з регулюваннями. В ідеалі виходи – продукція або послуги, які відповідають або перевершують очікування замовинків по термінах, якості і вартості. Це також можуть бути події, які запускають інші процеси у цій самій або у іншій організації.

Механізми бізнес-процесу

Механізми бізнес-процесу – це "інструменти", включаючи машини, системи і людей, які запускаються входами і виконують дії над входами.

Контрольні точки бізнес-процесу

Контрольні точки – це вимоги, обов'язкові дії, інструкції і обмеження, а також закони, положення, регламенти, правила і установки, які структурують і визначають дії над входами. Механізми і контрольні точки можуть бути одним й тим самим, наприклад, регламенти, фінанси і люди[2].

Моделювання та симуляція

Бізнес-процеси можуть бути унаочнені діаграмами бізнес-процесу – наприклад, у позначеннях BPMN. Бізнес-процеси можна моделювати з допомогою програмних засобів, наприклад ARIS.

Симуляція бізнес процесів в сучасних умовах займає особливе місце і в першу чергу в освітньому процесі. Симуляція застосовує методику learning by doing (навчання дією), що надає можливість:

– приймати конкретні економічні та управлінські рішення, що мають реальні наслідки для подальшої діяльності підприємства;

– отримувати орієнтири для набуття нових знань;

– навчитися виявляти причинно-наслідкові зв'язки управління економічними процесами на підприємстві в конкурентному ринковому середовищі.

Автоматизація та комп'ютеризація бізнес-процесів

Автоматизація бізнес-процесів – широкий клас завдань, що не обмежується рухом і обробкою документа, а до складу їх входять різні операції, що виконуються співробітниками, і покрокову автоматичну обробку даних. У ході бізнес-процесу можуть оброблятися різні документи і відбуватися взаємодія з зовнішніми IT-системами. Як правило, автоматизуються ключові бізнес-процеси діяльності підприємства: формування замовлень, виконання заявок клієнтів, розробка і запуск нової продукції і т. д., а також інші нескладні, але численні і рутинні процеси.

Таблиця 16.2 – Охоплення завдань автоматизації та комп'ютеризації бізнес-процесів

Специфікація	**Аудиторія**	**Суть (зміст завдань, що ставляться перед системою)**
описи типових бізнес-процесів	керівники підрозділів автоматизації; консультанти і технічні фахівці, що здійснюють впровадження комплексу	модель предметної області, закладена в основу комплексу; бізнес-процеси, в розрахунку на які комплекс був спроектований
типові технологічні інструкції		рекомендований порядок виконання операцій персоналом при використанні комплексу в складі автоматизованої системи

Ключовий процес

Ключови́й проце́с (англ. *Core or Key Process*) – бізнес-процес, який є життєво необхідним для успіху та життєдіяльності організації.

Моделювання бізнес-процесів

Моделюва́ння бі́знес-проце́сів (англ. *Business process modeling* – BPM) – формалізований і виконаний за певними правилами опис послідовності дій фахівців у формі логічних блок-схем, що визначають вибір подальших дій, виходячи з ситуативного факту. Наприклад: «якщо всі документи для формування страхового акта є в наявності, то формуємо цей документ. Якщо немає, то вживаємо заходів для отримання документів, яких не вистачає». У моделі бізнес-процесів певні послідовності окремих дій об'єднуються у відповідні процедури і сценарії бізнес-процесів. Описується взаємодія фахівців різних підрозділів в рамках одного бізнес-процесу.

Моделювання бізнес-процесів – це процесове відображення (як правило, графічне) діяльності підприємства з тим, щоб в подальшому дані процеси можна було аналізувати і вдосконалювати.

Цілі

Метою моделювання бізнес-процесів як правило є:

1. Документація бізнесу компанії:
   - Для отримання знання про бізнес.
   - Формування карти підрозділів.
   - Переведення бізнесу в інші місця.
   - Для задоволення потреб бізнес-партнерів або об'єднань (наприклад, з метою сертифікації).
   - Для навчання співробітників (передачі знань).
   - Для впровадження (підтримки системи менеджменту якості) та екологічного менеджменту.
2. Підготовка бізнес-процесів (який зазвичай починається з аналізу фактичного стану):
   - З метою впровадження нових організаційних структур.
   - Впровадження аутсорсингу.
3. Підготовка і автоматизації IT-підтримки бізнес систем.
4. Визначення показників процесу.
5. Бенчмаркінг.
6. Найкраща практика.
7. Організаційні зміни:
   - При підготовці до продажу бізнесу.
   - При підготовці до інтеграції компаній або їх частин.
   - Введення або зміна IT-систем та/або організаційних структур.
8. Участь у конкурсах (наприклад, Європейський фонд управління якістю).
9. Удосконалення внутрішніх процесів.

Використання

Моделювання бізнес-процесів, як правило, здійснюється та використовується бізнес-аналітиками і менеджерами, які прагнуть підвищити ефективність процесу та їх якість. В крупних компаніях без формалізації і опису бізнес-процесів складно забезпечити належний рівень виконавської і технологічної дисципліни. Формалізація і опис бізнес-процесів є ключовою умовою для їх автоматизації. Взаємозв'язана система бізнес-процесів зображає

весь комплекс завдань і функцій структурних підрозділів, виконання яких необхідно забезпечити в процесі діяльності компанії. Моделювання бізнес-процесів дозволяє, незалежно від актуальної чисельності персоналу компанії, на будь-якому етапі її еволюційного розвитку, дозволяє закріпити ті або інші функції не тільки за конкретними структурними підрозділами, але і за конкретними фахівцями. В міру збільшення чисельності персоналу, створення нових структурних підрозділів можна гнучко перерозподіляти функції і завдання структурних підрозділів.

Графічний опис бізнес-процесів та їх імітація це методи аналізу бізнес-процесів, ефективність яких доведена багаторічною практикою використання та численними дослідженнями.

Мови графічного моделювання

На сьогодні найвідомішими мовами (нотаціями) графічного моделювання бізнес-процесів є UML, ARIS, IDEF (IDEF0, IDEF3 у програмній інтерпретації BPwin), BPMN.

Абревіатура BPM

Моделювання бізнес-процесів відіграє величезну роль в управлінні бізнес-процесами. Необхідно відзначити, що в англійському перекладі обидва види діяльності мають однакову абревіатуру BPM (Business Process Modeling та Business Process Management, відповідно), що часто призводить до плутанини. Цей факт необхідно враховувати, тому що більшість літератури з даного предмету видано англійською мовою.

16.6. Розробка політик інформаційної безпеки під час забезпечення бізнес-процесів

Політика інформаційної безпеки виступає як документ або багаторівнева система документів, які визначають вимоги безпеки, систему заходів або порядок дій, відповідальність співробітників та механізми контролю задля забезпечення інформаційної безпеки підприємства. У документ **політики безпеки** рекомендовано вносити **наступні розділи**:

– Вступний розділ, що підтверджує стурбованість керівництва проблемами інформаційної безпеки.

– Організаційний розділ, що описує підрозділи, комісії, групи осіб, відповідальні за роботи в області інформаційної безпеки.

– Класифікаційний розділ, що описує матеріальні та інформаційні ресурси підприємства та необхідний рівень їх захисту.

– Штатний розділ, що характеризує заходи безпеки щодо персоналу.

– Розділ, що висвітлює питання фізичного захисту інформації.

– Розділ управління, що описує підхід до управління комп'ютерами та комп'ютерними мережами пересилання даних.

– Розділ, що зазначає правила розмежування доступу до інформації.

– Розділ, що описує заходи, спрямовані на забезпечення безперервної роботи підприємства (доступності інформації).

В даний час для захисту інформації потрібна не просто розробка приватних механізмів захисту, а реалізація системного підходу, що включає комплекс взаємопов'язаних заходів (використання спеціальних технічних і програмних засобів, організаційних заходів, нормативно-правових актів і т.д.). Головною метою будь-якої системи забезпечення інформаційної безпеки є створення умов функціонування підприємства, запобігання загроз його безпеки, захист законних інтересів підприємства від протиправних посягань, недопущення розкрадання фінансових засобів, розголошення, втрати, витоку, спотворення і знищення службової інформації, забезпечення в рамках виробничої діяльності всіх підрозділів підприємства.

Ефективна політика інформаційної безпеки визначає необхідний та достатній набір вимог безпеки. Вона мінімально впливає на продуктивність праці, враховує особливості бізнес-процесів підприємства, підтримується керівництвом, позитивно сприймається й виконується співробітниками підприємства.

Політика інформаційної безпеки (організаційно-технічні і режимні заходи)

Визначення політики інформаційної безпеки

При прийнятті рішень адміністратори ІС зіштовхуються з проблемою вибору варіантів рішень по організації ЗІ на основі обліку принципів діяльності організації, співвідношення важливості цілей і наявності ресурсів. Ці рішення включають визначення того, як будуть захищатися технічні й інформаційні ресурси, а також як повинні поводитися службовці в тих чи інших ситуаціях.

Політика інформаційної безпеки (ПІБ) – набір законів, правил і практичних рекомендацій і практичного досвіду, що визначають управлінські і проектні рішення в області ЗІ. На основі ПІБ будується керування, захист і розподіл критичної інформації в системі. Вона повинна охоплювати всі особливості процесу обробки інформації, визначаючи поводження ІС у різних ситуаціях.

Відповідно до запропонованого підходу політика (заходи) інформаційної безпеки реалізується відповідною структурою органів на основі нормативно-методичної бази з використанням програмно-технічних методів і засобів, що визначають архітектуру системи захисту.

Для конкретної ІС політика безпеки повинна бути індивідуальної. Вона залежить від технології обробки інформації, використовуваних програмних і технічних засобів, структури організації т.д.

Для того щоб описати ПІБ для конкретної ІС, адміністратори спочатку повинні визначити саму область обмежень і умов у зрозумілих усьому термінах. Корисно вказати чи мета причини розробки ПІБ – це допоможе домогтися дотримання політики.

Інформація, що циркулює в рамках ІС, є критично важливої. ІС дозволяє користувачам розділяти програми і дані, що збільшує ризик. Отже, кожний з комп'ютерів, що входять у мережу, має потребу в більш сильному захисті.

ПІБ переслідує дві головні цілі – продемонструвати співробітникам важливість захисту мережного середовища, описати їхня роль у забезпеченні безпеки, а також розподілити конкретні обов'язки по захисту інформації, що циркулює в мережі, так само як і самої мережі.

У відношенні політики безпеки в Internet організації може знадобитися уточнення, чи охоплює ця політика всі з'єднання, через які ведеться робота з Internet (чи прямо опосредованно) чи власне з'єднання Internet. Ця політика також може визначати, чи враховуються інші аспекти роботи в Internet, що не мають відносини до безпеки, такі як персональне використання з'єднань з Internet.

Принципи політики безпеки бізнес-процесів

Політика безпеки визначається як сукупність документованих управлінських рішень, спрямованих на захист інформації й асоційованих з нею ресурсів.

При розробці і проведенні її в життя доцільно керуватися наступними засадами:

- неможливість минати захисні засоби;
- посилення самої слабкої ланки;
- неприпустимість переходу у відкритий стан;
- мінімізація привілеїв;
- поділ обов'язків;
- багаторівневий захист;
- розмаїтість захисних засобів;
- простота і керованість інформаційної системи;
- забезпечення загальної підтримки заходів безпеки.

Пояснимо зміст перерахованих принципів.

Стосовно до межмережевих екранів *принцип неможливості минати захисні засоби* означає, що всі інформаційні потоки в мережу, що захищається, і з її повинні проходити через екран. Не повинно бути «таємних» модемних чи входів тестових ліній, що йдуть в обхід екрана.

Надійність будь-якої оборони визначається самою *слабкою ланкою*. Часто самою слабкою ланкою виявляється не чи комп'ютер програма, а людина, і тоді проблема забезпечення інформаційної безпеки здобуває нетехнічний характер.

Принцип неприпустимості переходу у відкритий стан означає, що при будь-яких обставинах (у тому числі позаштатних), СЗІ або цілком виконує свої функції, або повинна цілком блокувати доступ.

Принцип мінімізації привілеїв наказує виділяти користувачам і адміністраторам тільки ті права доступу, що необхідні їм для виконання службових обов'язків.

Принцип поділу обов'язків припускає такий розподіл ролей і відповідальності, при якому одна людина не може порушити критично важливий

для організації процес. Це особливо важливо, щоб запобігти зловмисні чи некваліфіковані дії системного адміністратора.

Принцип багаторівневого захисту наказує не покладатися на один захисний рубіж, яким би надійним він ні здавався. За засобами фізичного захисту повинні випливати програмно-технічні засоби, за ідентифікацією й автентифікацією – керування доступом і, як останній рубіж, – протоколювання й аудит. Ешелонована оборона здатна принаймні затримати зловмисника, а наявність такого рубежу, як протоколювання й аудит, істотно утрудняє непомітне виконання злочинних дій.

Принцип розмаїтості захисних засобів рекомендує організовувати різні за своїм характером оборонні рубежі, щоб від потенційного зловмисника було потрібно оволодіння різноманітними і, по можливості, несумісними між собою навичками подолання СЗІ.

Принцип простоти і керованості інформаційної системи в цілому і СЗІ особливо визначає можливість формального чи неформально доказу коректності реалізації механізмів захисту. Тільки в простій і керованій системі можна перевірити погодженість конфігурації різних компонентів і здійснити централізоване адміністрування.

Принцип загальної підтримки заходів безпеки – носить нетехнічний характер. Рекомендується із самого початку передбачити комплекс заходів, спрямований на забезпечення лояльності персоналу, на постійне навчання, теоретичне і, головне, практичне.

Види політики безпеки

Основу політики безпеки складає спосіб керування доступом, що визначає порядок доступу суб'єктів системи до об'єктів системи. Назва цього способу, як правило, визначає назва політики безпеки.

Для вивчення **властивостей способу керування доступом** створюється його формальний опис – **математична модель**. При цьому модель повинна відбивати стан всієї системи, її переходи з одного стану в інший, а також враховувати, які стани і переходи можна вважати безпечними в змісті даного керування. Без цього говорити про яких-небудь властивості системи, і тим більше гарантувати їх, щонайменше некоректно.

В даний час найкраще вивчені **два види політики безпеки**: **виборча** і **повноважна**, засновані, відповідно на виборчому і повноважному способах керування доступом. Крім того, існує набір вимог, що підсилює дію цих політик і призначений для керування інформаційними потоками в системі.

Слід зазначити, що засоби захисту, призначені для реалізації якого-небудь з названих способу керування доступом, тільки надають можливості надійного керування чи доступом інформаційними потоками.

Визначення прав доступу суб'єктів до об'єктів і/чи інформаційним потокам (повноважень суб'єктів і атрибутів об'єктів, присвоєння міток критичності і т.д.) входить у компетенцію адміністрації системи.

Основою виборчої політики безпеки є виборче керування доступом, що має на увазі, що:

– усі суб'єкти й об'єкти системи повинні бути ідентифіковані;

– права доступу суб'єкта до об'єкта системи визначаються на підставі деякого правила (властивість вибірковості).

Для опису властивостей виборчого керування доступом застосовується **модель системи на основі матриці доступу (МД),** іноді неї називають матрицею контролю доступу. Така модель одержала назву матричної.

Матриця доступу являє собою прямокутну матрицю, у якій об'єкту системи відповідає рядок, а суб'єкту стовпець. На перетинанні стовпця і рядка матриці вказується тип дозволеного доступу суб'єкта до об'єкта. Звичайно виділяють такі типи доступу суб'єкта до об'єкта, як "доступ на читання", "доступ на запис", "доступ на виконання" і ін.

Безліч об'єктів і типів доступу до них суб'єкта може змінюватися відповідно до деяких правил, що існують у даній системі. Визначення і зміна цих правил також є задачею МД.

Рішення на доступ суб'єкта до об'єкта приймається відповідно до типу доступу, зазначеним у відповідній осередку матриці доступу. Звичайно виборче керування доступом реалізує принцип "що не дозволено, те заборонено", що припускає явний дозвіл доступу суб'єкта до об'єкта. Матриця доступу – найбільш простий підхід до моделювання систем доступу.

Виборча політика безпеки найбільше широко застосовується в комерційному секторі, тому що її реалізація на практиці відповідає вимогам комерційних організацій по розмежуванню доступу і підзвітності, а також має прийнятну вартість і невеликі накладні витрати.

Основу повноважної політики безпеки складає повноважне керування доступом, що має на увазі, що:

– усі суб'єкти й об'єкти системи повинні бути однозначно ідентифіковані;

– кожному об'єкту системи привласнена мітка критичності, що визначає цінність інформації, що міститься в ньому;

– кожному суб'єкту системи привласнений рівень прозорості, що визначає максимальне значення мітки критичності об'єктів, до яких суб'єкт має доступ.

У тому випадку, коли сукупність міток має однакові значення, говорять, що вони належать до одного рівня безпеки. Організація міток має ієрархічну структуру і, таким чином, у системі можна реалізувати ієрархічно спадний потік інформації (наприклад, від рядових виконавців до керівництва). Чим важливіший об'єкт чи суб'єкт, тим вище його мітка критичності. Тому найбільш захищеними виявляються об'єкти з найбільш високими значеннями мітки критичності. Кожен суб'єкт, крім рівня прозорості, має поточне значення рівня безпеки, що може змінюватися від деякого мінімального значення до значення його рівня прозорості.

Основне призначення повноважної політики безпеки – регулювання доступу суб'єктів системи до об'єктів з різним рівнем критичності і запобігання витоку інформації з верхніх рівнів посадової ієрархії на нижні, а також блокування можливого проникнення з нижніх рівнів на верхні. При цьому вона функціонує на тлі виборчої політики, додаючи її вимогам ієрархічно упорядкований характер (відповідно до рівнів безпеки).

Склад та зміст основних заходів щодо розробки політики інформаційної безпеки

Організація заходів щодо захисту інформації

Не можна приступати до впровадження захисту інформації, поки користувачі не придбають навичок, необхідних для їхнього дотримання. Безпека вимагає не тільки знань, але і дій. Усі користувачі повинні знати, що потрібно почати і чого робити не коштує, коли вони зіштовхуються з чи порушенням можливістю його виникнення; до кого потрібно звертатися при виникненні підозр. Користувачі повинні бути упевнені в тому, що заходу для забезпечення безпеки приймаються в їхніх же інтересах, а не по інших розуміннях.

Подумайте про запрошення **кваліфікованого консультанта з безпеки**, що міг би дати вашим користувачам знання з інформаційної безпеки. Якщо консультант досить кваліфікований і ваша організація може собі це дозволити, запросите його на наступні збори групи як наставника при розробці правил. Незважаючи на те, що залучення консультанта для самостійної розробки правил може знизити витрати, ви втратите інтерес і увагу рядового користувача.

Працюючи таким способом, ви створите **правила безпеки**, до яких буде мати відношення кожен співробітник. Незважаючи на те, що в результаті може з'явитися і не самий зроблений документ, ефективність правил підвищиться відчутно. Забезпечте користувачів **керівництвом**, у якому викладений матеріал прийнятного обсягу. Навіть якщо користувачі засвоїли правила, то в них може виникнути питання, як ці правила впровадити. Надавайте разом із усіма правилами **модельні процедури впровадження і приклади**. Записуйте питання співробітників (разом з вашими відповідями і поясненнями) у супровідній документації до правил. Повідомляйте користувачам про ці доповнення.

Доповнюйте правила модельними процедурами і прикладами реалізації. Переконаєтеся, що ваші правила присвячені захисту від дійсних небезпек – від тих, імовірність виникнення яких досить реальна і дійсно представляють для вас погрозу.

У загальному виді сукупність заходів, спрямованих на запобігання погроз, визначається в такий спосіб:

– уведення надвикористання технічних засобів, ПЗ і масивів даних, тобто непотрібне дублювання або використання не за призначенням;

– резервування технічних засобів;

– регулювання доступу до технічних засобів, ПЗ, масивам інформації;

– регулювання використання програмно-апаратних засобів і масивів інформації;

– криптографічний захист інформації;

– контроль елементів ІС;

– реєстрація зведень;

– своєчасне знищення непотрібної інформації;

– сигналізація;

– своєчасне реагування.

У системному плані безліч і розмаїтість можливих видів захисту інформації визначається **способами впливу** на дестабілізуючі фактори їхні причини, що породжують, на елементи ІС, що захищається інформацію і навколишнє середовище, причому в напрямку, що сприяє підвищенню значень показників захищеності інформації. Ці **способи** можуть бути **класифіковані** в такий спосіб:

– **Фізичні засоби** – механічні, електричні, електромеханічні, електронні, електронно-механічні й інші пристрої і системи, що функціонують автономно, створюючи різного роду перешкоди дестабілізуючим факторам.

– **Апаратні засоби** – різні електронні, електронно-механічні і подібні пристрої, що вбудовуються в апаратуру ІС чи, що сполучаються з нею спеціально для рішення задач захисту інформації.

– **Програмні засоби** – спеціальні пакети чи програм окремі програми, використовувані для рішення задач захисту.

– **Організаційні заходи** – організаційно-технічні заходи, передбачаються спеціально в ІС з метою рішення задач захисту.

– **Правові заходи** – законодавчо-правові акти, що існують у державі, спеціально видавані закони, зв'язані з забезпеченням захисту інформації. Вони регламентують права й обов'язки всіх облич і підрозділів, що мають відношення до функціонування ІС, і установлюють відповідальність за дії, наслідком яких може бути порушення захищеності інформації.

– **Морально-етичні норми** – це сформовані в чи суспільстві колективі моральні норми й етичні правила, дотримання яких сприяє захисту інформації, а порушення їх прирівнюється до недотримання правил поводження в суспільстві.

Для забезпечення ефективності захисту інформації усі використовувані засоби і заходи доцільно об'єднати в систему захисту інформації, що повинна бути функціонально самостійною підсистемою ІС. Головною властивістю побудови системи захисту повинна бути здатність до її пристосування при зміні структури технологічних чи схем умов функціонування ІС.

Іншими принципами можуть бути:

– мінімізація витрат, максимальне використання серійних засобів;
– забезпечення рішення необхідної сукупності задач захисту;
– комплексне використання засобів захисту, оптимізація архітектури;
– зручність для персоналу;
– простота експлуатації.

СЗІ доцільно будувати у виді взаємозалежних підсистем, а саме:

– підсистема криптографічного захисту;
– підсистема забезпечення юридичної значимості електронних документів;
– підсистема захисту від НСД;
– підсистема організаційно-правового захисту;
– підсистема керування СЗІ.

Побудова системи захисту інформації в такому виді дозволить забезпечити комплексність процесу захисту інформації в ІС, керованість процесу і можливість адаптації при зміні умов функціонування ІС:

– *Підсистема криптографічного захисту* поєднує засобу такого захисту інформації і по ряду функцій кооперується з підсистемою захисту від НСД.

– *Підсистема забезпечення юридичної значимості* електронних документів служить для додання юридичного статусу документам в електронному представленні і є визначальним моментом при переході до без паперової технології документообігу. Дану підсистему зручно і доцільно розглядати як частина підсистеми криптографічного захисту.

– *Підсистема захисту від НСД* запобігає доступу несанкціонованих користувачів до ресурсів ІС.

– *Підсистема керування СЗІ* призначена для керування ключовими структурами підсистеми криптографічного захисту, а також контролю і діагностування програмно-апаратних засобів і забезпечення взаємодії всіх підсистем СЗІ.

– *Підсистема організаційно-правового захисту* призначена для регламентації діяльності користувачів ІС і являє собою упорядковану сукупність організаційних рішень, нормативів, законів і правил, що визначають загальну організацію робіт із захисту інформації в ІС.

Система захисту інформації являє собою сукупність автоматизованих робочих місць (АРМ), що входять до складу ІС, і програмно-апаратних засобів, інтегрованих в АРМ користувачів ІС.

Політики безпеки для Internet

Організації повинні відповісти на наступні питання, щоб правильно врахувати можливі наслідки підключення до Internety в області безпеки:

– Чи можуть хакери зруйнувати внутрішні системи?

– Чи може бути скомпрометована (змінена чи прочитана) важлива інформація організації при її передачі по Internet?

– Чи можна перешкодити роботі організації?

Ціль політики безпеки для Internet – прийняти рішення про те, як організація збирається захищатися. ПІБ звичайно складається з двох частин – загальних принципів і конкретних правил роботи (які еквівалентні специфічній політиці, описаної нижче). Загальні принципи визначають підхід до безпеки в Internet. Правила ж визначають що дозволено, а що – заборонено. Правила можуть доповнюватися конкретними процедурами і різними посібниками.

Internet при проектуванні і не задумувалася як захищена мережа, тому його **проблемами в поточній версії TCP/IP** є:

– Легкість перехоплення даних і фальсифікації адрес машин у мережі – основна частина трафіку Internet – це нешифровані дані. E-mail, паролі і файли можуть бути перехоплені, використовуючи легко доступні програми.

– Уразливість засобів TCP/IP – ряд засобів TCP/IP не був спроектований бути захищеними і може бути скомпрометований кваліфікованими зловмисниками; засобу, використовувані для тестування особливо уразливі.

– Відсутність політики – багато хто сайти через незнання сконфигуровані таким чином, що надають широкий доступ до себе з боку Internet, не з огляду на можливість зловживання цим доступом; багато хто сайти дозволяють роботу більшого числа сервісів TCP/IP, чим їм потрібно для роботи і не намагаються обмежити доступ до інформації про свої комп'ютери, що може допомогти зловмисникам.

– Складність конфігурування – засоби керування доступом хоста складні; найчастіше складно правильно зконфігурувати і перевірити ефективність установок. Засоби, що помилково неправильно сконфигуровані, можуть привести до неавторизованого доступу.

Рівні політики безпеки

З практичної точки зору політику безпеки можна умовно розділити на три рівні: верхній, середній і нижній.

До **верхнього рівня** відносяться рішення, що торкаються організацію в цілому. Вони носять дуже загальний характер і, як правило, виходять від керівництва організації.

Зразковий список подібних рішень може містити в собі наступні елементи:

– чи формування перегляд комплексної програми забезпечення інформаційної безпеки, визначення відповідальних за просування програми;

– формулювання цілей, що переслідує організація в області інформаційної безпеки, визначення загальних напрямків у досягненні цих цілей;

– забезпечення бази для дотримання законів і правил;

– формулювання управлінських рішень по тим питанням реалізації програми безпеки, що повинні розглядатися на рівні організації в цілому.

Мети політики верхнього рівня організації в області інформаційної безпеки формулюються в термінах цілісності, приступності і конфіденційності.

Якщо організація відповідає за підтримку критично важливих баз даних, на першому плані може стояти зменшення випадків утрат, чи ушкоджень перекручувань даних. Для організації, що займається продажами, імовірно, важлива актуальність інформації про надані послуги і ціни, а також її приступність максимальному числу потенційних покупців.

Режимна організація в першу чергу піклується про захист від несанкціонованого доступу – конфіденційності.

На верхній рівень виноситься керування захисними ресурсами і координація використання цих ресурсів, виділення спеціального персоналу для захисту критично важливих систем, підтримка контактів з іншими організаціями, що забезпечують чи контролюють режим безпеки.

ПІБ верхнього рівня повинна чітко окреслювати сферу свого впливу. Можливо, це будуть усі комп'ютерні системи чи організації навіть більше, якщо ПІБ регламентує деякі аспекти використання співробітниками своїх домашніх комп'ютерів. Можлива, однак, і така ситуація, коли в сферу впливу включаються лише найбільш важливі системи.

У політику повинні бути визначені обов'язки посадових осіб по виробленню програми безпеки і по проведенню її в життя. У цьому змісті ПІБ є основою підзвітності персоналу.

На верхній рівень варто виносити мінімум питань, що визначають значну економію чи засобів коли інакше надійти просто неможливо.

До **середнього рівня** варто віднести питання, що стосуються окремих аспектів інформаційної безпеки, але важливі для різних систем, експлуатованих організацією. Приклади таких питань – відношення до передового, але ще недостатньо перевіреним технологіям: доступ до Internet (як сполучити волю одержання інформації з захистом від зовнішніх погроз?), використання домашніх комп'ютерів, застосування користувачами неофіційного програмного забезпечення і т.д.

Політика безпеки **нижнього рівня** відноситься до конкретних сервісам. Вона містить у собі два аспекти – мети і правила їхнього досягнення, тому її часом важко відокремити від питань реалізації. На відміну від двох верхніх рівнів, розглянута ПІБ повинна бути набагато детальніше.

Є багато речей, специфічних для окремих сервісів, які не можна єдиним образом регламентувати в рамках всієї організації. У той же час ці речі настільки важливі для забезпечення режиму безпеки, що рішення, що відносяться до них, повинні прийматися на управлінському, а не технічному рівні.

Приведемо кілька прикладів питань, на які варто дати відповідь при проходженні політиці безпеки нижнього рівня:

- хто має право доступу до об'єктів, підтримуваним сервісом?
- при яких умовах можна читати і модифікувати дані?
- як організований віддалений доступ до сервісу?

При формулюванні цілей ПІБ нижнього рівня може виходити з заходів цілісності, приступності і конфіденційності, але вона не повинна на них зупинятися. Її мети повинні бути конкретніше

З цілей виводяться правила безпеки, що описують, хто, що і при яких умовах може робити. Чим детальніше правила, тим більш формально вони викладені, тим простіше підтримати їхнє виконання програмно-технічними заходами. З іншого боку, занадто тверді правила можуть заважати роботі користувачів, імовірно, їх прийдеться часто переглядати.

Керівництву треба знайти розумний компроміс, коли за прийнятну ціну буде забезпечений прийнятний рівень безпеки, а працівники не виявляться занадто скровані.

Основні принципи політики забезпечення інформаційної безпеки підприємства

Основними принципами інформаційної безпеки є:

– забезпечення цілісності і збереження даних, тобто надійне їх зберігання в неспотвореному вигляді;

– дотримання конфіденційності інформації (її недоступність для тих користувачів, які не мають відповідних прав);

– доступність інформації для всіх авторизованих користувачів за умови контролю за всіма процесами використання ними отриманої інформації;

– безперешкодний доступ до інформації в будь-який момент, коли вона може знадобитися підприємству.

Ці принципи неможливо реалізувати без особливої **інтегрованої системи інформаційної безпеки**, що виконує наступні функції:

– вироблення політики інформаційної безпеки;

– аналіз ризиків (тобто ситуацій, в яких може бути порушена нормальна робота інформаційної системи, а також втрачені або розсекречені дані);

– планування заходів щодо забезпечення інформаційної безпеки;

– планування дій в надзвичайних ситуаціях;

– вибір технічних засобів забезпечення інформаційної безпеки.

Отже, етапи проведення робіт із забезпечення інформаційної безпеки підприємства виглядають таким чином:

1. Проведення обстеження підприємства на предмет виявлення реальних загроз несанкціонованого доступу до конфіденційної інформації;

2. Розробка політики безпеки, організаційно-розпорядчих документів і заходів щодо забезпечення інформаційної безпеки системи відповідно до вимог по захищеності технічних і програмних засобів від витоку конфіденційної інформації;

3. Проектування системи інформаційної безпеки;

4. Створення прототипу системи інформаційної безпеки;

5. Розробка зразка системи інформаційної безпеки;

6. Впровадження системи інформаційної безпеки в діючу структуру підприємства;

7. Навчання персоналу;

8. Атестація системи інформаційної безпеки підприємства.

Метою комплексної інформаційної безпеки є збереження інформаційної системи підприємства, захист і гарантування повноти і точності виданої нею інформації, мінімізація руйнувань і модифікація інформації, якщо такі трапляються.

Види моделей розробки політики інформаційної безпеки

Серед моделей ПБ найвідомішими є дискреційна, мандатна та рольова. Перші дві досить давно відомі й детально досліджені, а рольова політика є недавнім досягненням теорії та практики захисту інформації.

Дискреційна політика безпеки

Основою **дискреційної політики безпеки (ДПБ)** є дискреційне управління доступом (Discretionary Access Control – DAC), яке визначається двома властивостями:

– усі суб’єкти й об’єкти мають бути однозначно ідентифіковані;

– права доступу суб’єкта до об’єкта системи визначаються на основі певних зовнішніх відносно системи правил.

Назва пункту є дослівним перекладом з англійської терміна Discretionary policy, ще один варіант перекладу – розмежувальна політика. Ця політика одна з найпоширеніших в світі, в системах по замовчуванню мається на увазі саме ця політика. ДПБ реалізується за допомогою матриці доступу, яка фіксує множину об’єктів та суб’єктів, доступних кожному суб’єкту.

Наведемо приклади варіантів задання матриці доступу:

1. Листи можливостей: для кожного суб'єкта створюється лист (файл) усіх об'єктів, до яких має доступ даний суб'єкт;

2. Листи контролю доступу: для кожного об'єкта створюється список усіх суб'єктів, що мають доступи до цього об'єкта;

До **переваг ДПБ** можна віднести відносно просту реалізацію відповідних механізмів захисту. Саме цим зумовлено той факт, що більшість поширених нині захищених автоматизованих систем забезпечують виконання положень саме ДПБ. Однак багатьох проблем захисту ця політика розв'язати не може.

Наведемо найбільш суттєві **вади ДПБ**:

1. Один з найбільших недоліків цього классу політик – вони не витримують атак за допомогою «Троянського коня». Це, зокрема, означає, що система захисту, яка реалізує ДПБ, погано захищає від проникнення вірусів у систему та інших способів прихованої руйнівної дії.

2. Автоматичне визначення прав. Оскільки об'єктів багато і їх кількість безперервно змінюється, то задати заздалегідь вручну перелік прав кожного суб'єкта на доступ до об'єктів неможливо. Тому матриця доступу різними способами агрегується, наприклад, суб'єктами залишаються тільки користувачі, а у відповідну клітину матриці вставляються формули функцій, обчислення яких визначає права доступу суб'єкта, породженого користувачем, до об'єкта. Звичайно, ці функції можуть змінюватися з часом. Зокрема, можливе вилучення прав після виконання певної події, також можливі модифікації, що залежать від інших параметрів.

3. Контроль поширення прав доступу. Найчастіше буває так, що власник файла передає вміст файла іншому користувачеві і той відповідно набуває права власника на цю інформацію. Отже, права можуть поширюватись, і навіть якщо перший власник не хотів передати доступ іншому суб'єкту до своєї інформації, то після кількох кроків передача прав може відбутися незалежно від його волі. Виникає задача про умови, за якими в такій системі певний суб'єкт рано чи пізно отримає необхідний йому доступ.

4. При використанні ДПБ виникає питання визначення правил поширення прав доступу й аналізу їх впливу на безпеку АС. У загальному випадку при використанні ДПБ органом, який її реалізує і який при санкціонуванні доступу суб'єкта до об'єкта керується певним набором правил, стоїть задача, яку алгоритмічно неможливо розв'язати: перевірити, призведуть його дії до порушень безпеки чи ні. Отже, матриця доступів не є тим механізмом, який дозволив би реалізувати ясну і чітку СЗІ в АС. Більш досконалою ПБ виявилася мандатна ПБ.

Мандатна політика

Основу мандатної (повноважної) політики безпеки (МПБ) становить мандатне управління доступом (Mandatory Access Control – MAC), яке передбачає, що:

– всі суб'єкти й об'єкти повинні бути однозначно ідентифіковані;

– у системі визначено лінійно упорядкований набір міток секретності;

– кожному об’єкту системи надано мітку секретності, яка визначає цінність інформації, що міститься в ньому, – його рівень секретності в АС;

– кожному суб’єкту системи надано мітку секретності, яка визначає рівень довіри до нього в АС, – максимальне значення мітки секретності об’єктів, до яких суб’єкт має доступ; мітка секретності суб’єкта називається його рівнем доступу.

Основна мета МПБ – запобігання витоку інформації від об’єктів з високим рівнем доступу до об’єктів з низьким рівнем доступу, тобто протидія виникненню в КС інформаційних каналів згори вниз. Вона оперує, таким чином, поняттями інформаційного потоку і цінності інформаційних об’єктів. Цінність інформаційних об’єктів (або їх мітки рівня секретності) часто дуже важко визначити. Однак досвід показує, що в будь-якій КС майже завжди для будь-якої пари об’єктів X та *Y* можна сказати, який з них більш цінний.

Тобто, можна вважати, що таким чином фактично визначається деяка однозначна функція *c(X),* яка дозволяє для будь-яких об’єктів *X* і *Y* сказати, що:

– коли *Y* більш цінний об’єкт, ніж *X,* то *c(Y) > c(X).*

– і навпаки, якщо *c(Y) > c(X),* то *Y* – більш цінний об’єкт, ніж *X.*

– тоді потік інформації від *X* до *Y* дозволяється, якщо *c(X) < c(Y),* і не дозволяється, якщо *c(X) > c(Y).*

Отже, МПБ має справу з множиною інформаційних потоків, яка ділиться на дозволені і недозволені за дуже простою умовою – значенням наведеної функції. МПБ у сучасних системах захисту на практиці реалізується мандатним контролем на найнижчому апаратно-програмному рівні, що дає змогу досить ефективно будувати захищене середовище для механізму мандатного контролю.

Пристрій мандатного контролю називають монітором звернень. Мандатний контроль, який ще називають обов’язковим, оскільки його має проходити кожне звернення суб’єкта до об’єкта, організується так:

– монітор звернень порівнює мітки рівня секретності кожного об’єкта з мітками рівня доступу суб’єкта;

– за результатом порівняння міток приймається рішення про допуск.

Найчастіше МПБ описують у термінах, поняттях і визначеннях властивостей **моделі Белла-Лападула**. У рамках цієї моделі доводиться важливе твердження, яке вказує на принципову відмінність систем, що реалізують мандатний захист, від систем з дискреційним захистом: «якщо початковий стан системи безпечний і всі переходи системи зі стану до стану не порушують обмежень, сформульованих ПБ, то будь-який стан системи безпечний».

Наведемо ряд **переваг** МПБ порівняно з ДПБ:

1. Для систем, де реалізовано МПБ, є характерним вищий ступінь надійності. Це пов’язано з тим, що за правилами МПБ відстежуються не тільки правила доступу суб’єктів системи до об’єктів, а й стан самої КС. Таким чином, канали витоку в системах такого типу не закладені первісно (що є в положеннях ДПБ), а можуть виникнути тільки при практичній реалізації систем внаслідок помилок розробника.

2. Правила МПБ ясніші і простіші для розуміння розробниками і користувачами АС, що також є фактором, який позитивно впливає на рівень безпеки системи.

3. МПБ стійка до атак типу «Троянський кінь».

4. МПБ допускає можливість точного математичного доведення, що система в заданих умовах підтримує ПБ.

Однак МПБ має дуже серйозні вади – вона дуже складна для практичної реалізації і вимагає значних ресурсів КС. Це пов'язано з тим, що інформаційних потоків у системі величезна кількість і їх не завжди можна ідентифікувати. Сааме ці вади часто заважають її практичному використанню.

МПБ прийнята всіма розвинутими державами світу. Вона розроблялася, головним чином, для збереження секретності (тобто конфіденційності) інформації у військових організаціях. Питання ж цілісності за її допомогою не розв'язуються або розв'язуються частково, як побічний результат захисту секретності.

Рольова політика безпеки

Рольову політику безпеки (РПБ) (Role Base Access Control – RBAC) не можна віднести ані до дискреційної, ані до мандатної, тому що керування доступом у ній здійснюється як на основі матриці прав доступу для ролей, так і за допомогою правил, які регламентують призначення ролей користувачам та їх активацію під час сеансів. Отже, рольова модель є цілком новим типом політики, яка базується на компромісі між гнучкістю керування доступом, характерною для ДПБ, і жорсткістю правил контролю доступу, що притаманна МПБ.

У РПБ класичне поняття «суб'єкт» заміщується поняттями «користувач» і «роль».

Користувач – це людина, яка працює з системою і виконує певні службові обов'язки.

Роль – це активно діюча в системі абстрактна сутність, з якою пов'язаний обмежений, логічно зв'язаний набір повноважень, необхідних для здійснення певної діяльності.

РПБ застосовується досить широко, тому що вона, на відміну від інших більш строгих і формальних політик, є дуже близькою до реального життя.

Справді, за суттю, користувачі, що працюють у системі, діють не від свого власного імені – вони завжди виконують певні службові обов'язки, тобто виконують деякі ролі, які аж ніяк не пов'язані з їх особистістю. Тому цілком логічно здійснювати керування доступом і призначати повноваження не реальним користувачам, а абстрактним (не персоніфікованим) ролям, які представляють учасників певного процесу обробки інформації. Такий підхід до ПБ дозволяє врахувати розподіл обов'язків і повноважень між учасниками прикладного інформаційного процесу, оскільки з точки зору РПБ має значення не особистість користувача, користувача, що здійснює доступ до інформації, а те, які повноваження йому необхідні для виконання його службових обов'язків.

Наприклад, у реальній системі обробки інформації можуть працювати системний адміністратор, менеджер баз даних і прості користувачі. У такій ситуації РПБ дає змогу розподілити повноваження між цими ролями відповідно

до їх службових обов'язків: ролі адміністратора призначаються спеціальні повноваження, які дозволять йому контролювати роботу системи і керувати її конфігурацією, роль менеджера баз даних дозволяє здійснювати керування сервером БД, а права простих користувачів обмежуються мінімумом, необхідним для запуску прикладних програм. Крім того, кількість ролей у системі може не відповідати кількості реальних користувачів – один користувач, якщо він має різні повноваження, може виконувати (водночас або послідовно) кілька ролей, а кілька користувачів можуть користуватися однією й тією ж роллю, якщо вони виконують однакову роботу. При використанні РПБ керування доступом здійснюється в дві стадії: по-перше, для кожної ролі вказується набір повноважень, що представляють набір прав доступу до об'єктів, і, по-друге, кожному користувачеві призначається список доступних йому ролей. Повноваження призначаються ролям відповідно до принципу найменших привілеїв, з якого випливає, що кожний користувач повинен мати тільки мінімально необхідні для виконання своєї роботи повноваження. У моделі РПБ визначаються множини: множина користувачів, множина ролей, множина повноважень на доступ до об'єктів, наприклад, у вигляді матриці прав доступу, множина сеансів роботи користувачів з системою. Для перелічених множин визначаються відношення, які встановлюють для кожної ролі набір наданих їй повноважень, а також для кожного користувача – набір доступних йому ролей.

Правила керування доступом РПБ визначаються певними функціями, які для кожного сеансу визначають користувачів, набір ролей, що можуть бути одночасно доступні користувачеві в цьому сеансі, а також набір доступних у ньому повноважень, що визначається як сукупність повноважень усіх ролей, що беруть участь у цьому сеансі. Як критерій безпеки рольової моделі використовується правило: «система вважається безпечною, якщо будь-який користувач системи, що працює в певному сеансі, може здійснити дії, які вимагають певних повноважень тільки в тому випадку, коли ці повноваження належать сукупності повноважень усіх ролей, що беруть участь у цьому сеансі».

З формулювання критерію безпеки рольової моделі випливає, що управління доступом здійснюється, головним чином, не за допомогою призначення повноважень ролям, а шляхом встановлення відношення, яке призначає ролі користувачам, і функції, що визначає доступний у сеансі набір ролей. Тому численні інтерпретації рольової моделі відрізняються видом функцій, що визначають правила керування доступом, а також обмеженнями, що накладаються на відношення між множинами. Завдяки гнучкості та широким можливостям РПБ суттєво перевершує інші політики, хоча іноді її певні властивості можуть виявитися негативними. Так, вона практично не гарантує безпеку за допомогою формального доведення, а тільки визначає характер обмежень, виконання яких і є критерієм безпеки системи. Хоча такий підхід дозволяє отримати прості й зрозумілі правила контролю доступу (перевага), які легко застосовувати на практиці, проте позбавляє систему теоретичної доказової бази (вада). У деяких ситуаціях ця обставина утруднює використання РПБ, однак у кожному разі оперувати ролями набагато зручніше, ніж суб'єктами (знову перевага), оскільки це більше відповідає поширеним технологіям обробки

інформації, які передбачають розподіл обов'язків і сфер відповідальності між користувачами. Крім того, РПБ може використовуватися одночасно з іншими ПБ, коли повноваження ролей, що призначаються користувачам, контролюється контролюється ДПБ або МПБ, що дозволяє будувати багаторівневі схеми контролю доступу.

Наведений огляд сучасних ПБ визначає основні принципи їх функціонування, а також підкреслює їх роль і виключну важливість при побудові та експлуатації захищених АС. Додамо, що в багатьох сучасних програмних засобах захисту інформації розглянуті ПБ уже реалізовані. Однак слід зазначити, що це зовсім не означає їх механічного застосування. Зрозуміло, що спочатку в конкретній організації має бути проведений ретельний аналіз процесів обробки інформації, на основі якого потім створюється і застосовується конкретна ПБ. Необхідно також зазначити, що, крім загального опису поняття ПБ, в Українському стандарті з технічного захисту інформації більш конкретних нормативних та методичних матеріалів з розробки ПБ для АС поки що немає. Зауважимо, що, в більшості організацій (як державних, так і недержавних) про поняття ПБ навіть не мають уявлення. Але парадокс якраз полягає в тому, що фактично в будь-якій організації завжди існують конкретні правила, що регламентують процес її функціонування, зокрема і процес захисту інформації, а саме ці правила і є політикою. Отже, фактично в будь-яких АС окремі елементи ПБ завжди наявні.

16.7. Дотримання політик інформаційної безпеки під час забезпечення бізнес-процесів

Кожна компанія, в процесі здійснення своєї діяльності, повинна приділяти значну увагу інформаційній безпеці, що полягає зокрема в розробці різноманітних стратегій управління процесами, створенні інструментів та політик, необхідних для запобігання, виявлення, документування та протидії загрозам цифровій та нецифровій інформації.

Інформаційна безпека в контексті цінності компанії

Інформаційна безпека, в широкому розумінні цього слова є сукупністю технічних та організаційних заходів, а також розроблених документів, основною метою яких є захист та збереження інформації, якою володіє компанія. Разом з тим, інформаційна безпека все ж залишається складовою частиною кібербезпеки, що є значно ширшою категорією та включає в себе не лише захист інформації та даних, а й захист систем, мереж та інше.

До основних цілей інформаційної безпеки також відноситься створення набору бізнес-процесів, які захищатимуть інформаційні активи незалежно від того, як форматується інформація, чи вона перебуває в транзиті, обробляється чи знаходиться в стані спокою, тобто зберігається у відповідних базах даних.

Цінність компанії, на думку деяких експертів, визначається перш за все в тому, яка інформація перебуває у володінні компанії, а також як ця інформація

зберігається. Безпека інформації є вирішальним фактором для забезпечення здійснення ефективних ділових операцій, а також для збереження та завоювання довіри клієнтів, як майбутніх, так і існуючих.

Організація інформаційної безпеки в рамках компанії

Для можливості максимально ефективно забезпечити інформаційну безпеку в рамках компанії, насамперед необхідно визначитися з основною стратегією, якої повинна дотримуватися компанія. Така стратегія повинна визначатися керівництвом компанії, з одночасним залученням спеціалістів з інформаційної безпеки, якими можуть виступати як працівники компанії, так і залучені зовнішні підрядники. Результатом розроблюваної стратегії зазвичай є затверджений проект з інформаційної безпеки, а також шляхи та методи його реалізації.

Після визначення глобальної стратегії, компанія, як правило, створює **спеціалізовану команду спеціалістів з питань інформаційної безпеки (Information security team / IS team)** для впровадження та підтримки проекту з інформаційної безпеки. Зазвичай, цією групою керує **головний співробітник інформаційної безпеки (Chief information security officer/CISO**). Інші ж члени команди повинні обиратися, виходячи з рівня їхньої компетенції та вмінь в питаннях безпеки інформації.

Information security team відповідає за управління ризиками, реалізацію процесів, з допомогою яких постійно оцінюються вразливості та загрози по відношенню до інформації, якою володіє компанія, а також за приймання і застосування відповідних захисних засобів контролю. Разом з тим, команда з інформаційної безпеки повинна реагувати на всі порушення безпеки інформації та оперативно приймати рішення про усунення таких порушення, а також про мінімізацію ризиків для інтересів компанії чи фундаментальних прав, свобод та інтересів фізичних осіб, якщо порушення будь-яким чином стосується персональних даних таких осіб.

Проект з реалізації інформаційної безпеки повинен будуватися навколо основних трьох аспектів безпеки, які полягають в підтримці конфіденційності, цілісності та доступності до інформації, в тому числі в межах IT систем та баз даних компанії. Впровадження таких принципів допоможе забезпечити розкриття конфіденційної інформації лише уповноваженим сторонам (конфіденційність), запобігти несанкціонованому зміненню даних (цілісності) та гарантувати, що до інформації можуть отримати доступ тільки уповноважені сторони (за наявності).

Перший аспект безпеки це **конфіденційність**. Такий аспект зазвичай вимагає використання ключів шифрування та шифрування. Тобто, якщо компанія забезпечує недоступність до інформації шляхом її шифрування, обов'язково повинні бути ключі, зокрема у вигляді паролів, які дають можливість дешифрувати інформацію в її первинний вигляд, для можливості використання інформації для цілей компанії.

Другий аспект безпеки – **цілісність**. Він передбачає, наприклад, що коли інформація завантажується (записується) або надсилається в будь-яке місце, а

потім зчитується чи отримується назад, вона повинна бути точно такою, якою вона була в момент надсилання чи завантаження. Інколи, для більшої гарантії безпеки інформації, компанії може знадобитися надсилання однієї і тієї ж інформації у два різних місця, тобто, створення резервної копії інформації.

Третій аспект безпеки полягає в **доступності** інформації, що означає під собою забезпечення своєчасного використання нової інформації, а також оперативне відновлення інформації протягом прийнятного, в рамках загальноприйнятої практики, строку відновлення, який би не порушував інтереси будь-яких осіб, незалежно від того, юридичні це особи чи фізичні. Мається на увазі, що доступ до інформації повинен бути вільний та безперебійний, але тільки звісно ж тільки для тих осіб, хто має на те право.

Не секрет, що заходи інформаційної безпеки повинні бути також зосереджені на мережевих системах та комп'ютерній інфраструктурі компанії, яка найчастіше всього може стати об'єктом кібератак та інших зловмисних дій, направлених на знищення, крадіжку або пошкодження інформації, що належить або якою користується компанія.

Політики та процедури, які регламентують інформаційну безпеку

В процесі впровадження проекту з інформаційної безпеки, компанія повинна забезпечити наявність відповідних документів, якими повинні керуватися працівники компанії, залучені компанією особи, а також Information security team, забезпечуючи реалізацію тих чи інших заходів. Іншими словами, компанія повинна розробити та провадити ISMS (information security management system), що являє собою набір керівних принципів, політик та процесів, що створений для допомоги компанії в процесі управління безпекою інформації та у випадках, пов'язаних з порушенням даних. Маючи розроблений набір керівних принципів, компанія має можливість мінімізувати ризики в контексті безпеки інформації, а також може забезпечити безперервність роботи у разі зміни персоналу.

Компанія може використовувати шаблонні рішення, які користуються популярністю на ринку. Наприклад, стандарти ISO 27001 є надзвичайно популярною та відомою основою для розроблюваної компанією ISMS. Разом, з тим, компанією повинні враховуватися всі аспекти своєї діяльності, а також інші особливості інформації, якою володіє компанія.

Керівні принципи, процеси та політики інформаційної безпеки зазвичай передбачають розробку та імплементацію фізичних та технічних заходів безпеки для захисту інформації від несанкціонованого доступу, використання, розповсюдження або знищення. Ці заходи можуть включати в себе пастки, систему управління ключами шифрування, мережеві системи виявлення вторгнень, політику паролів, політику управління системою електронних адрес та політику антивірусних заходів.

Немаловажним заходом, який повинен включатися в ISMS, є проведення аудиту існуючих документів та систем компанії на відповідність вимогам, які гарантують максимальний захист інформації. Аудит безпеки повинен проводитися компанією з метою оцінки здатності компанії підтримувати захищеність системи на основі та в рамках встановлених критеріїв.

Основна порада, в процесі забезпечення інформаційної безпеки, полягає в залученні кваліфікованих спеціалістів в сфері інформаційної безпеки в процесі імплементації та реалізації проекту з інформаційної безпеки в рамках компанії.

Також, однією з основних порад буде використання світових визнаних стандартів, які забезпечують основний каркас інформаційної безпеки. Компанії, в свою чергу, залишається тільки пристосувати запропоновані алгоритми до своїх внутрішніх процесів, з допомогою яких забезпечується безпека інформації. Це наприклад стандарти ISO або PCI DSS.

Загалом же, підходьте до питання організації інформаційної безпеки досить виважено та скрупульозно, обов'язково застосовуючи сучасні досягнення в області техніки, комп'ютерних технологій, а також, враховуючи вимоги законодавства, зокрема у сфері захисту персональних даних.

Розділ 17. Симетричні криптосистеми

17.1. Модель симетричної криптосистеми.

17.2. Класичні методи шифрування: Шифр Цезаря, Вернама. Квадрат Полібія. Шифр гамування.

17.3. Блокові шифри: DES. ДСТУ ГОСТ 28147:2009. AES. ДСТУ 7624:2014 (режими роботи, довжина ключів, довжина блоку вхідного тексту, кількість раундів, крипостійкість згідно з ДСТУ ISO/IEC 10116:2019).

17.4. Потокові шифри: RC4, STRUMOK. (ДСТУ 8845:2019) (довжина ключів, криптостійкість).

17.1. Модель симетричної криптосистеми

Розглянемо загальну схему ***симетричної, або традиційної, криптографії***.



Рисунок 17.1 – Загальна схема симетричного шифрування

У процесі шифрування використовується певний алгоритм шифрування, на вхід якому подаються вихідне незашифроване повідомлення, називане також ***plaintext***, і ключ. Виходом алгоритму є зашифроване повідомлення, називане також ***ciphertext***. Ключ є значенням, що не залежить від шифруємого повідомлення. Зміна ключа повинна приводити до зміни зашифрованого повідомлення.

Зашифроване повідомлення передається одержувачеві. Одержувач перетворить зашифроване повідомлення у вихідне незашифроване повідомлення за допомогою алгоритму дешифрування й того ж самого ключа, що використовувався при шифруванні, або ключа, легко одержуваного із *ключа шифрування*.

Незашифроване повідомлення будемо позначати P або M, від слів *plaintext* і message. Зашифроване повідомлення будемо позначати C, від слова ciphertext.

Безпека, забезпечувана традиційною *криптографією*, залежить від декількох факторів:

– Криптографічний алгоритм повинен бути досить сильним, щоб передане зашифроване повідомлення неможливо було розшифрувати без ключа, використовуючи тільки різні статистичні закономірності зашифрованого повідомлення або які-небудь інші способи його аналізу.

– Безпека переданого повідомлення повинна залежати від таємності ключа, але не від таємності алгоритму. Алгоритм повинен бути проаналізований фахівцями, щоб виключити наявність слабких місць, при яких погано схований взаємозв'язок між незашифрованим і зашифрованим повідомленнями. До того ж при виконанні цієї умови виробники можуть створювати дешеві апаратні чипи й вільно розповсюджувані програми, що реалізують даний алгоритм шифрування.

– Алгоритм повинен бути таким, щоб не можна було довідатися ключ, навіть знаючи досить багато пар (зашифроване повідомлення, незашифроване повідомлення), отриманих при шифруванні з використанням даного ключа.

Клод Шеннон увів поняття *дифузії* й *конфузії* для опису *стійкості алгоритму* шифрування.

Дифузія – це розсіювання статистичних особливостей незашифрованого тексту в широкому діапазоні статистичних особливостей зашифрованого тексту. Це досягається тим, що значення кожного елемента незашифрованого тексту впливає на значення багатьох елементів зашифрованого тексту або, що той же саме, будь-який елемент зашифрованого тексту залежить від багатьох елементів незашифрованого тексту.

Конфузія – це знищення статистичного взаємозв'язку між зашифрованим текстом і ключем.

Якщо X – це вихідне повідомлення й K – криптографічний ключ, то зашифрований переданий текст можна записати у вигляді

$$Y = E_K[X].$$

Одержувач, використовуючи той же ключ, розшифровує повідомлення

$$X = D_K[Y]$$

Супротивник, не маючи доступу до K і X, повинен спробувати довідатися X, K або й те, і інше.

Алгоритми симетричного шифрування розрізняються способом, яким обробляється вихідний текст. **Можливе шифрування блоками або шифрування потоком.**

17.2. Класичні методи шифрування: Шифр Цезаря, Вернама. Квадрат Полібія. Шифр гамування

Шифр Цезаря

Теоретичні відомості. Розглянемо задачу, що полягає в захисті інформації від несанкціонованого доступу. Розглянемо алфавіт укр. мови та занумеруємо літери так, щоб А мала номер 0, Б – номер 1 і т.д. та "розташуємо" їх в рядок згідно номерів. Внизу випишемо ще такий самий рядок, зсунувши його вправо на одну літеру та переставимо літеру Я на початок другого рядка:

А Б В Г Д Е Є Ж З І Ї Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ь Ю Я
Я А Б В Г Д Е Є Ж З І Ї Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ь Ю

Цим самим виконаємо зсув на одну літеру. Аналогічним чином визначаємо зсув на N, або що те саме-циклічну перестановку літер алфавіту. Використаємо цей другий рядок для кодування тексту з метою конфіденційності (захисту від несанкціонованого використання).

Розглянемо обернену задачу – декодування тексту, закодованого при певному зсуві алфавіту. Для того щоб взламати текст закодований методом цезаря застосовується наступний підхід:

Використаємо статистичні методи для визначення величини зсуву наступним чином:

1. Побудуємо таблицю 1 ймовірності всіх літер алфавіту на базі величезного текстового файлу.

2. Побудуємо таблицю 2 частот появи літер в закодованому текстовому файлі.

3. Визначаємо величину зсуву алфавіту:

а) Підрахувати суму різниць частоти літери із кожного рядка та ймовірності появи відповідної літери. Наприклад для уявного зсуву на 1 маємо таку суму:

$$S_1=|V_2\,(А)-V_1\,(Я)+V_2\,(Б)-V_1\,(А)+V_2\,(В)-V_1\,(Б)+\ldots+V_2\,(Я)-V_1\,(Ю)|$$

де $V_2\,(А)$ – частота появи літер А в декодованому тексті, $V_1\,(Я)$ – ймовірність появи літери Я в укр. тексті.

б) Якщо позначити через Si-суму, побудовану в а) для уявного зсуву на *i* всіх літер алфавіту, то можливо побудувати множину $\{S_i\}$, $i = 0,\ldots,33$ в якій найменший елемент буде відповідати величині зсуву літер алфавіту.

4.Таким чином статистичним методом знайдемо можливість для декодування тексту, про який відомий спосіб кодування.

Шифр Вернама

Шифр Вернама (інша назва: англ. *one-time pad* – схема одноразових блокнотів) – у криптографії, система симетричного шифрування, винайдена в 1917 році співробітниками AT&T Мейджором Джозефом Моборном і Гільбертом Вернамом. Шифр Вернама є єдиною системою шифрування, для якої доведена абсолютна криптографічна стійкість.

Для утворення шифротексту повідомлення об'єднується операцією XOR з ключем (названим одноразовим блокнотом або шифроблокнотом). При цьому ключ повинен мати три критично важливі властивості:

1. Бути справді випадковим.
2. Збігатися за розміром з заданим відкритим текстом.
3. Застосовуватися тільки один раз.
4. Повинен зберігатися в повній таємниці сторонами, що спілкуються.

Шифр названий на честь телеграфіста AT&T Гільберта Вернама, який у 1917 році побудував телеграфний апарат, що виконував цю операцію автоматично – треба було тільки подати на нього стрічку з ключем. Не будучи шифрувальником, Вернам, тим не менш, помітив важливу властивість свого шифру – кожна стрічка повинна використовуватися тільки один раз і після цього знищуватися. Це було важко застосувати на практиці – тому апарат був перероблений на кілька зациклених стрічок із взаємно простими періодами.

Квадрат Полібія

У криптографії квадрат Полібія (англ. *Polybius square*), також відомий як шахова дошка Полібія – оригінальний код простої заміни, одна з найдавніших систем кодування, запропонована Полібієм (грецький історик, полководець, державний діяч, III століття до н.е.). Цей спосіб кодування спочатку застосовувався для грецької абетки, але потім поширився на інші мови.

Спосіб шифрування

Квадрат спочатку створювався для кодування, з його допомогою можна успішно шифрувати. Для того, щоб зашифрувати текст квадратом Полібія, потрібно зробити кілька кроків:

Крок 1: Формування таблиці шифрування

До кожної мови окремо складається таблиця шифрування з однаковою (не обов'язково) кількістю пронумерованих рядків та стовпців, параметри якої залежать від її потужності (кількості букв в абетці). Беруться два цілих числа, добуток яких найближче до кількості букв у мові – отримуємо потрібну кількість рядків і стовпців. Потім вписуємо в таблицю всі букви алфавіту поспіль – по одній на кожну клітину. При нестачі клітин можна вписати в одну дві букви (рідко вживані або схожі за вживанням).

Латинський алфавіт

У сучасній латинській абетці 26 букв, отже таблиця повинна складатися з 5 рядків і 5 стовпців, оскільки 25=5*5 найбільш близьке до 26 число. При цьому літери I, J не розрізняються (J ототожнюється з буквою I), оскільки не вистачає однієї комірки:

	1	**2**	**3**	**4**	**5**
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Українська абетка

Ідею формування таблиці шифрування проілюструємо для української мови. Число букв в українській абетці відрізняється від числа букв у грецькій абетці, тому розмір таблиці вибрано інший (квадрат 6*6=36, оскільки 36 найбільш близьке число до 33):

	1	2	3	4	5	6
1	А	Б	В	Г	Ґ	Д
2	Е	Є	Ж	З	И	І
3	Ї	Й	К	Л	М	Н
4	О	П	Р	С	Т	У
5	Ф	Х	Ц	Ч	Ш	Щ
6	Ю	Я	Ь	—	—	—

Можливий також інший варіант складання, що передбачає об'єднання букв Г і Ґ, И і Й, видання І і Ї. В даному випадку отримуємо такий результат:

	1	2	3	4	5	6
1	А	Б	В	Г/Ґ	Д	Е
2	Є	Ж	З	И/Й	І/Ї	К
3	Л	М	Н	О	П	Р
4	С	Т	У	Ф	Х	Ц
5	Ч	Ш	Щ	Ю	Я	Ь

Використовуючи подібний алгоритм, таблицю шифрування можна задати для будь-якої мови. Щоб розшифрувати закритий текст, необхідно знати, таблицею шифрування якого алфавіту він зашифрований.

Крок 2: Принцип шифрування

Існує кілька методів шифрування з допомогою квадрата Полібія. Нижче наведено три з них.

Метод 1

Зашифруємо слово «SOMETEXT»:

Для шифрування на квадраті знаходили букву тексту і вставляли в шифровку нижню від неї в тому ж стовпці. Якщо буква була в нижньому рядку, то брали верхню з стовпця.

Таблиця координат								
Буква тексту:	**S**	**O**	**M**	**E**	**T**	**E**	**X**	**T**
Буква шифротексту:	**X**	**T**	**R**	**K**	**Y**	**K**	**C**	**Y**

Таким чином після шифрування отримуємо:

Результат	
До шифрування:	**SOMETEXT**
Після шифрування:	**XTRKYKCY**

Метод 2

Повідомлення перетвориться в координати по квадрату Полібія, координати записуються вертикально:

Таблиця координат								
Буква:	**S**	**O**	**M**	**E**	**T**	**E**	**X**	**T**
Координата горизонтальна:	**3**	**4**	**2**	**5**	**4**	**5**	**3**	**4**
Координата вертикальна:	**4**	**3**	**3**	**1**	**4**	**1**	**5**	**4**

Потім координати зчитують по рядках: 34 25 45 34 43 31 41 54 (*)

Далі координати перетворюються в літери з цього ж квадрату:

Таблиця координат								
Координата горизонтальна:	**3**	**2**	**4**	**3**	**4**	**3**	**4**	**5**
Координата вертикальна:	**4**	**5**	**5**	**4**	**3**	**1**	**1**	**4**
Буква:	**S**	**W**	**Y**	**S**	**O**	**C**	**D**	**U**

Таким чином після шифрування отримуємо:

Результат	
До шифрування:	**SOMETEXT**
Після шифрування:	**SWYSOCDU**

Метод 3

Ускладнений варіант, який полягає в наступному: отриманий первинний шифротекст (*) шифрується вдруге. При цьому він виписується без розбиття на пари: 3425453443314154 Отримана послідовність цифр зсувається циклічно вліво на один крок (непарна кількість кроків): 4254534433141543 Ця послідовність знову розбивається в групи по два: 42 54 53 44 33 14 15 43 і за таблицею замінюється на остаточний шифротекст:

Таблиця координат								
Координата горизонтальна:	**4**	**5**	**5**	**4**	**3**	**1**	**1**	**4**
Координата вертикальна:	**2**	**4**	**3**	**4**	**3**	**4**	**5**	**3**
Буква:	**I**	**U**	**P**	**T**	**N**	**Q**	**V**	**O**

Таким чином після шифрування отримуємо:

Результат	
До шифрування:	**SOMETEXT**
Після шифрування:	**IUPTNQVO**

Додавання ключа

На перший погляд шифр здається дуже нестійким, але для його реальної оцінки слід враховувати два фактори:

1. Можливість заповнити квадрат Полібія буквами довільно, а не тільки строго за алфавітом.

2. Можливість періодично замінювати квадрати.

Тоді розбір попередніх повідомлень нічого не дає, оскільки до моменту розкриття шифру він може бути замінений.

Букви можуть вписуватися в таблицю в довільному порядку – заповнення таблиці в цьому випадку і є ключем. Для латинської абетки в першу клітку можна вписати одну з 25 букв, у другу – одну з 24, в третю – одну з 23 і т. д. Отримуємо максимальну кількість ключів для шифру на таблиці латинської абетки:

$$N=25*24*23*...*2*1=25!$$

Відповідно для дешифрування повідомлення буде потрібно не тільки знання абетки, але і ключа, за допомогою якого складалася таблиця шифрування. Але довільний порядок букв важко запам'ятати, тому користувачеві шифру необхідно постійно мати при собі ключ – квадрат. з'являється небезпека таємного ознайомлення з ключем сторонніх осіб. Як компромісне рішення був запропонований ключ – пароль. Пароль виписується без повторів букв в квадрат; в клітини, що залишилися, в абетковому порядку виписуються букви абетки, відсутні в паролі.

Приклад

Зашифруємо слово «SOMETEXT», використовуючи ключ «DRAFT». Складемо попередньо таблицю шифрування з даним ключем, записуючи символи ключа по порядку в таблицю, після них абетки:

	1	**2**	**3**	**4**	**5**
1	D	R	A	F	T
2	B	C	E	G	H
3	I	K	L	M	N
4	O	P	Q	S	U
5	V	W	X	Y	Z

Перетворимо повідомлення в координати по квадрату Полібія:

Таблиця координат								
Буква:	**S**	**O**	**M**	**E**	**T**	**E**	**X**	**T**
Координата горизонтальна:	**4**	**1**	**4**	**3**	**5**	**3**	**3**	**5**
Координата вертикальна:	**4**	**4**	**3**	**2**	**1**	**2**	**5**	**1**

Рахуємо координати по рядках: 41 43 53 35 44 32 12 51

Перетворимо координати в літери з цього ж квадрату:

Таблиця координат								
Координата горизонтальна:	**4**	**4**	**5**	**3**	**4**	**3**	**1**	**5**
Координата вертикальна:	**1**	**3**	**3**	**5**	**4**	**2**	**2**	**1**
Буква:	**F**	**M**	**N**	**X**	**S**	**E**	**B**	**T**

Таким чином після шифрування отримуємо:

Результат	
До шифрування:	**SOMETEXT**
Після шифрування:	**FMNXSEBT**

Шифр гамування

Принцип шифрування гаммуванням полягає в генерації гамми шифру за допомогою датчика псевдовипадкових чисел і накладення отриманої гамми шифру на відкриті дані зверненим способом (наприклад, за допомогою операції складання за модулем 2). Процес дешифрування здійснюється для повторної генерації гамми шифру при відомому ключі та накладенні такої ж гами на зашифровані дані.

Отриманий зашифрований текст є достатньо трудомістким для розкриття в тому випадку, якщо гамма-шифр не містить повторюваних бітових послідовностей і змінюється випадковим чином для кожного зашифрованого слова. Якщо період гамми перевищує довжину всього зашифрованого тексту і невідома жодна частина вихідного тексту, то шифр можна розкрити тільки прямим перебором (підбором ключа). В цьому випадку криптостійкість визначається розміром ключа.

Метод гамування стає бессильним, якщо відомий фрагмент вихідного тексту і відповідна йому шифрограма. В цьому випадку простим відніманням за модулем 2 отримується відрізок псевдовипадковой послідовності й за ним відновлюється вся ця послідовність.

17.3. Блокові шифри: DES. ДСТУ ГОСТ 28147:2009. AES. ДСТУ 7624:2014 (режими роботи, довжина ключів, довжина блоку вхідного тексту, кількість раундів, крипостійкість згідно з ДСТУ ISO/IEC 10116:2019)

Блокові шифри

Блок тексту розглядається як ненегативне ціле число, або як кілька незалежних ненегативних цілих чисел. Довжина блоку завжди вибирається рівною ступеню двійки. У більшості блокових алгоритмів симетричного шифрування використовуються наступні типи операцій:

– Таблична підстановка, при якій група біт відображається в іншу групу біт. Це так звані S-***box***.

– Переміщення, за допомогою якого біти повідомлення переупорядковуються.

– Операція додавання за модулем 2, позначувана XOR або ⊕.

– Операція додавання за модулем 2^{32} або за модулем 2^{16}.

– Циклічне зрушення на деяке число біт.

Ці операції циклічно повторюються в алгоритмі, створюючи так звані ***раунди***. Входом кожного *раунду* є вихід попереднього *раунду* й ключ, що отриманий по певному алгоритму із ключа шифрування K. Ключ *раунду* називається ***підключем***. Кожний алгоритм шифрування може бути представлений у такий спосіб:

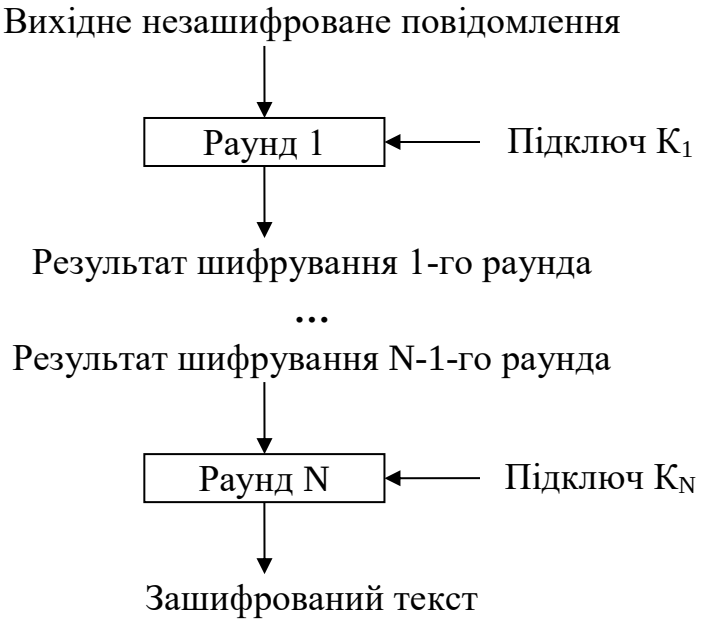


Рисунок 17.2 – Структура алгоритму симетричного шифрування

Області застосування

Стандартний алгоритм шифрування повинен бути застосуємо в багатьох додатках:

– Шифрування даних. Алгоритм повинен бути ефективний при шифруванні файлів даних або великого потоку даних.

– Створення випадкових чисел. Алгоритм повинен бути ефективний при створенні певної кількості випадкових біт.

– Ґешування. Алгоритм повинен ефективно перетворюватися в однобічну ґеш-функцію.

Платформи

Стандартний алгоритм шифрування повинен бути реалізований на різних платформах, які, відповідно, висувають різні вимоги.

– Алгоритм повинен ефективно реалізовуватися на спеціалізованій апаратурі, призначеної для виконання шифрування/дешифрування.

– Великі процесори. Хоча для найбільш швидких додатків завжди використовується спеціальна апаратура, програмні реалізації застосовуються частіше. Алгоритм повинен допускати ефективну програмну реалізацію на 32-бітних процесорах.

– Процесори середнього розміру. Алгоритм повинен працювати на мікроконтролерах і інших процесорах середнього розміру.

– Малі процесори. Повинна існувати можливість реалізації алгоритму на смарт-картах, нехай навіть із урахуванням твердих обмежень на використовувану пам'ять.

Додаткові вимоги

Алгоритм шифрування повинен, по можливості, задовольняти деяким додатковим вимогам.

– Алгоритм повинен бути простим для написання коду, щоб мінімізувати ймовірність програмних помилок.

– Алгоритм повинен мати плоский простір ключів і допускати будь-який випадковий рядок біт потрібної довжини як можливий ключ. Наявність слабких ключів небажано.

– Алгоритм повинен легко модифікуватися для різних рівнів безпеки й задовольняти як мінімальним, так і максимальним вимогам.

– Всі операції з даними повинні здійснюватися над блоками, кратними байту або 32-бітному слову.

Мережа Фейштеля

Блоковий алгоритм перетворює n-бітний блок незашифрованого тексту в n-бітний блок зашифрованого тексту. Число блоків довжини n дорівнює 2^n. Для того щоб перетворення було оборотним, кожний з таких блоків повинен перетворюватися у свій унікальний блок зашифрованого тексту. При маленькій довжині блоку така підстановка погано приховує статистичні особливості незашифрованого тексту. Якщо блок має довжину 64 біта, то він уже добре приховує статистичні особливості вихідного тексту. Але в цьому випадку перетворення тексту не може бути довільним у силу того, що ключем буде саме перетворення, що виключає ефективну як програмну, так і апаратну реалізації.

Найбільш широке поширення одержали ***мережі Фейштеля***, тому що, з одного боку, вони задовольняють всім вимогам до алгоритмів симетричного шифрування, а з іншого боку, досить прості й компактні.

Мережа Фейштеля має наступну структуру. Вхідний блок ділиться на трохи рівної довжини підблоків, називаних гілками. У випадку, якщо блок має довжину 64 біта, використовуються дві гілки по 32 біта кожна. Кожна гілка обробляється незалежно від інший, послу чого здійснюється циклічне зрушення всіх гілок уліво. Таке перетворення виконується кілька циклів або *раундів*. У випадку двох гілок кожний *раунд* має структуру, показану на рисунку:

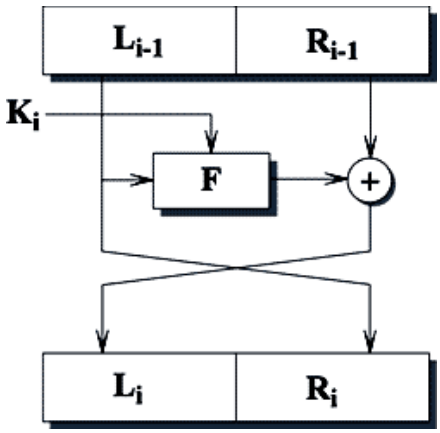


Рисунок 17.3 – і-ий раунд мережі Фейштеля

Функція F називається утворюючою. Кожний *раунд* складається з обчислення функції F для однієї гілки й побітового виконання операції XOR результату F з іншою гілкою. Після цього гілки міняються місцями. Вважається, що оптимальне число *раундів* – від 8 до 32. Важливо те, що збільшення кількості *раундів* значно збільшує криптостійкість алгоритму. Можливо, ця особливість і вплинула на настільки активне поширення *мережі Фейштеля*, тому що для більшої криптостійкости досить просто збільшити кількість *раундів*, не змінюючи сам алгоритм. Останнім часом кількість *раундів* не фіксується, а лише вказуються припустимі межі.

Мережа Фейштеля є оборотною навіть у тому випадку, якщо функція F не є такою, тому що для дешифрування не потрібно обчислювати F^{-1}. Для дешифрування використовується той же алгоритм, але на вхід подається зашифрований текст, і ключі використовуються у зворотному порядку.

Останнім часом все частіше використовуються різні різновиди *мережі Фейштеля* для 128-бітного блоку із чотирма гілками. Збільшення кількості галузей, а не розмірності кожної гілки пов'язане з тим, що найбільш популярними дотепер залишаються процесори з 32-розрядними словами, отже, оперувати 32-розрядними словами ефективніше, ніж з 64-розрядними.

Основною характеристикою алгоритму, побудованого на основі *мережі Фейштеля*, є функція F. Різні варіанти стосуються також початкового й кінцевого перетворень. Подібні перетворення, називані забілюванням (whitening), здійснюються для того, щоб виконати початкову рандомизацію вхідного тексту.

Алгоритм DES

Принципи розробки

Найпоширенішим і найбільш відомим алгоритмом симетричного шифрування є ***DES*** (Data Encryption Standard). Алгоритм був розроблений в 1977 році, в 1980 році був прийнятий NIST (National Institute of Standards and Technolody США) як стандарт (FIPS PUB 46).

DES є класичною *мережею Фейштеля* із двома гілками. Дані шифруються 64-бітними блоками, використовуючи 56-бітний ключ. Алгоритм перетворить за кілька *раундів 64*-бітний вхід в 64-бітний вихід. Довжина ключа дорівнює 56 бітам. Процес шифрування складається із чотирьох етапів. На першому з них виконується початкова перестановка (IP) 64-бітного вихідного тексту (забілювання), під час якої біти з у відповідності зі стандартною таблицею. Наступний етап складається з 16 *раундів* однієї й тої ж функції, що використовує операції зрушення й підстановки. На третьому етапі ліва й права половини виходу останньої (16-й) ітерації міняються місцями. Нарешті, на четвертому етапі виконується перестановка IP^{-1} результату, отриманого на третьому етапі. Перестановка IP^{-1} інверсна початковій перестановці.



Рисунок 17.4 – Загальна схема DES

Праворуч на рисунку показаний спосіб, яким використовується 56-бітний ключ. Спочатку ключ подається на вхід функції перестановки. Потім для кожного з 16 *раундів підключ* K_i є комбінацією лівого циклічного зрушення й перестановки. Функція перестановки та сама для кожного *раунду*, але *підключи* K_i для кожного *раунду* виходять різні внаслідок повторюваного зрушення біт ключа.

Потрійний DES

У цей час основним недоліком *DES* вважається маленька довжина ключа, тому вже давно почали розроблятися різні альтернативи цьому алгоритму шифрування. Один з підходів полягає в тому, щоб розробити новий алгоритм, і успішний тому приклад – **IDEA**. Інший підхід припускає повторне застосування шифрування за допомогою *DES* з використанням декількох ключів.

Недоліки подвійного DES

Найпростіший спосіб збільшити довжину ключа складається в повторному застосуванні *DES* із двома різними ключами. Використовуючи незашифроване повідомлення P і два ключі K_1 і K_2, зашифроване повідомлення C можна одержати в такий спосіб:

$$C = E_{k2} [E_{k1} [P]]$$

Для дешифрування потрібно, щоб два ключі застосовувалися у зворотному порядку:

$$P = D_{k1} [D_{k2} [C]]$$

У цьому випадку довжина ключа дорівнює 56 * 2 = 112 біт.

Потрійний DES із двома ключами

Очевидна протидія атаці "зустріч посередині", що буде розглядатися пізніше, складається у використанні третьої стадії шифрування із трьома різними ключами. Це піднімає вартість лобової атаки до 2^{168}, що на сьогоднішній день вважається вище практичних можливостей. Але при цьому довжина ключа дорівнює 56 * 3 = 168 біт, що іноді буває громіздко.

Як альтернатива пропонується метод потрійного шифрування, що використовує тільки два ключі. У цьому випадку виконується послідовність **зашифрування-розшифрування-зашифрування (EDE).**

$$C = E_{K1} [D_{K2} [E_{K1} [P]]]$$

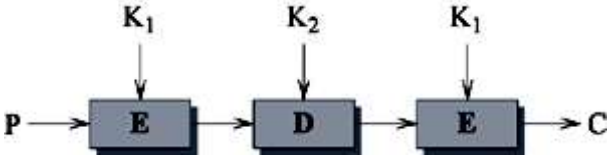


Рисунок 17.5 – Шифрування потрійним DES

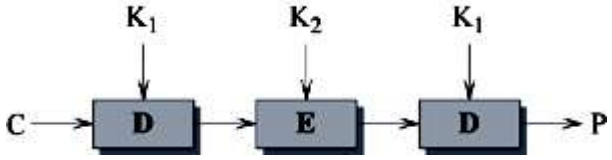


Рисунок 17.6 – Дешифрування потрійним DES

Не має великого значення, що використовується на другій стадії: шифрування або дешифрування. У випадку використання дешифрування існує тільки та перевага, що можна *потрійний DES* звести до звичайного одиночного *DES*, використовуючи $K_1 = K_2$:

$$C = E_{K1} [D_{K1} [E_{K1} [P]]] = E_{K1} [P]$$

Потрійний DES є досить популярною альтернативою *DES* і використовується при керуванні ключами в стандартах ANSI X9.17 і ISO 8732 і в PEM (Privacy Enhanced Mail).

Відомих криптографічних атак на *потрійний DES* не існує. Ціна підбора ключа в *потрійному DES* дорівнює 2^{112}.

Алгоритм Blowfish

Blowfish є мережею Фейштеля, у якої кількість ітерацій дорівнює 16. Довжина блоку дорівнює 64 бітам, ключ може мати будь-яку довжину в межах 448 біт. Хоча перед початком будь-якого шифрування виконується складна фаза ініціалізації, саме шифрування даних виконується досить швидко.

Алгоритм призначений в основному для додатків, у яких ключ міняється нечасто, до того ж існує фаза початкового рукостискання, під час якої відбувається автентифікація сторін і узгодження загальних параметрів і секретів. Класичним прикладом подібних додатків є мережна взаємодія. При реалізації на 32-бітних мікропроцесорах з великим кешем даних *Blowfish* значно швидше DES.

Алгоритм складається із двох частин: розширення ключа й шифрування даних. Розширення ключа перетворить ключ довжиною, принаймні, 448 біт у кілька масивів *підключей* загальною довжиною 4168 байт.

В основі алгоритму лежить мережа Фейштеля з 16 ітераціями. Кожна ітерація складається з перестановки, що залежить від ключа, і підстановки, що залежить від ключа й даних. Операціями є XOR і додавання 32-бітних слів.

Blowfish використовує велику кількість *підключей*. Ці ключі повинні бути обчислені заздалегідь, до початку будь-якого шифрування або дешифрування даних.

Алгоритм IDEA

IDEA (International Data Encryption Algorithm) є блоковим симетричним алгоритмом шифрування, розробленим Сюдзя Гавкіт (Xuejia Lai) і Джеймсом Массей (James Massey) зі швейцарського федерального інституту технологій. Первісна версія була опублікована в 1990 році. Переглянута версія алгоритму, посилена засобами захисту від диференціальних криптографічних атак, була представлена в 1991 році й докладно описана в 1992 році.

IDEA є одним з декількох симетричних криптографічних алгоритмів, якими спочатку передбачалося замінити DES.

Принципи розробки

IDEA є блоковим алгоритмом, що використовує 128-бітовий *ключ для шифрування* даних блоками по 64 біта.

Метою розробки *IDEA* було створення щодо стійкого криптографічного алгоритму з досить простою реалізацією.

Криптографічна стійкість

Наступні характеристики *IDEA* характеризують його криптографічну стійкість:

1. **Довжина блоку**: довжина блоку повинна бути достатньою, щоб сховати всі статистичні характеристики вихідного повідомлення. З іншого боку, складність реалізації криптографічної функції зростає експоненціально відповідно до розміру блоку. Використання блоку розміром в 64 біта в 90-і роки означало достатню силу. Більше того, використання режиму шифрування CBC говорить про подальше посилення цього аспекту алгоритму.

2. **Довжина ключа**: довжина ключа повинна бути досить великою для того, щоб запобігти можливості простого перебору ключа. При довжині ключа 128 біт *IDEA* вважається досить безпечним.

3. **Конфузія**: зашифрований текст повинен залежати від ключа складним і заплутаним способом.

4. **Дифузія**: кожний біт незашифрованого тексту повинен впливати на кожний біт зашифрованого тексту. Поширення одного незашифрованого біта на велику кількість зашифрованих біт приховує статистичну структуру незашифрованого тексту. Визначити, як статистичні характеристики зашифрованого тексту залежать від статистичних характеристик незашифрованого тексту, повинне бути непросто. *IDEA* із цього погляду є дуже ефективним алгоритмом.

В *IDEA* два останніх пункти виконуються за допомогою трьох операцій. Це відрізняє його від DES, де все побудовано на використанні операції XOR і маленьких нелінійних S-*boxes*.

Алгоритм ДСТУ ГОСТ 28147:2009

Алгоритм ДСТУ ГОСТ 28147:2009 є вітчизняним стандартом для алгоритмів симетричного шифрування. ***ДСТУ ГОСТ 28147:2009*** розроблений в 1989 році, є блоковим алгоритмом шифрування, довжина блоку дорівнює 64 бітам, довжина ключа дорівнює 256 бітам, кількість *раундів* дорівнює 32. Алгоритм являє собою класичну мережу Фейштеля.

$$L_i = R_{i-1}$$

$$R_i = L_i \oplus f(R_{i-1}, K_i)$$

Функція F проста. Спочатку права половина й і-ий *підключ* складаються за модулем 2^{32}. Потім результат розбивається на вісім 4-бітових значень, кожне з яких подається на вхід S-*box*. *ДСТУ ГОСТ 28147:2009* використовує вісім різних S-*boxes*, кожний з яких має 4-бітовий вхід і 4-бітовий вихід. Виходи всіх S-*boxes* поєднуються в 32-бітне слово, що потім циклічно зрушується на 11 біт уліво. Нарешті, за допомогою XOR результат поєднується з лівою половиною, у результаті чого виходить нова права половина.

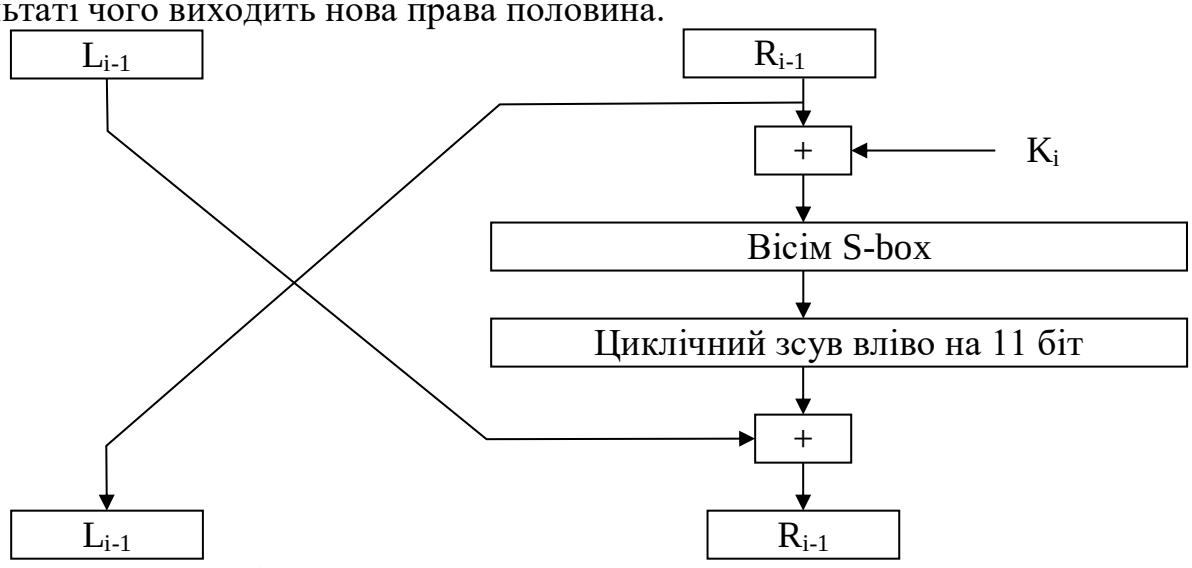


Рисунок 17.7 – і-ий раунд ДСТУ ГОСТ 28147:2009

Режими виконання алгоритмів симетричного шифрування

Для будь-якого симетричного блокового алгоритму шифрування визначено чотири режими виконання.

ECB – Electronic Codebook – кожний блок з 64 біт незашифрованого тексту шифрується незалежно від інших блоків, із застосуванням того самого *ключа шифрування*. Типові додатки – безпечна передача одиночних значень (наприклад, криптографічного ключа).

CBC – Cipher Block Chaining – вхід криптографічного алгоритму є результатом застосування операції XOR до наступного блоку незашифрованого тексту й попередньому блоку зашифрованого тексту. Типові додатки – загальна блокоорієнтована передача, автентифікація.

CFB – Cipher Feedback – при кожному виклику алгоритму обробляється J біт вхідного значення. Попередній зашифрований блок використовується як вхід в алгоритм; до J биток виходу алгоритму й наступному незашифрованому блоку з J біт застосовується операція XOR, результатом якої є наступний зашифрований блок з J біт. Типові додатки – потокоорієнтована передача, автентифікація.

OFB – Output Feedback – аналогічний *CFB*, за винятком того, що на вхід алгоритму при шифруванні наступного блоку подається результат шифрування попереднього блоку; тільки після цього виконується операція XOR із черговими J бітами незашифрованого тексту. Типові додатки – потокоорієнтована передача по зашумленому каналу (наприклад, супутниковий зв'язок).

Advanced Encryption Standard (AES)

Опис симетричного алгоритму шифрування AES

Поліпшений стандарт шифрування (AES) – це нова симетрична схема шифрування прийнята американським Національним інститутом Стандартів і Технології (NIST). Стандарт описаний в NIST-197 і визначає симетричний блоковий шифр, що називається Rijndael, сконструйований Дж. Даеменом і В. Риджменом. Цей шифр був відібраний в 2001 році після процесу публічної оцінки протягом більш ніж 2 роки й призначений для заміни існуючого Цифрового Стандарту Шифрування (DES). Алгоритм AES не був формально представлений на NESSIE, але був включений в оцінювання як широко використовуваний і затверджений FIPSом алгоритм для симетричного шифрування.

Опис примітива. Блоковий шифр Rijndael ліг у основу AES. Він був спочатку створений для обробки широкого спектра розмірів блоків і довжин ключів. Однак тільки три певні комбінації розмірів блоків і довжин ключів підтримуються стандартом FIPS. Ці три варіанти **AES, AES-128, AES-192 і AES-256**, мають фіксований розмір блоку в 128 біти і приймають ключі довжиною **128, 192 і 256** бітів відповідно.

Блоковий шифр AES – це підстановочно-перестановочна система (Substitution Permutation Network – SPN), що включає **10, 12 або 14** циклів (раундів) залежно від довжини ключа. Шифр бере 128-бітний блок відкритого тексту P і шифрує його в 128-бітний блок шифрованого тексту C

відповідно до секретного ключа K. Всі операції під час цього ітеративного процесу виконуються над масивом байт **4×4**, які розглядаються як елементи кінцевого поля GF (2^8).

Один цикл (раунд) включає:

– нелінійну підстановку байтів (SubBytes);

– перетворення зсуву у рядках (ShiftRows);

– перетворення змішування колонок (MixColumns) (у 10-му раунді пропускається);

– додаток ключа циклу (AddRoundKey). Ключі циклу, кожний зі 128 біт, походять від оригінального 128-бітового, 192-бітового або 256-бітового секретного ключа за допомогою процедури розширення окремого ключа.

Зворотний процес, що дозволяє відкрити зашифрований відкритий текст для даного секретного ключа, дуже схожий з алгоритмом шифрування, але різні перетворення злегка модифіковані.

При цьому, вихідний алгоритм Rijndael допускає довжину ключа й розмір блоку від 128 до 256 біт із кроком в 32 біта. Для позначення обраних довжин input, State і Cipher Key у байтах використовується нотація ***Nb* = 4** для input і State, ***Nk* = 4, 6, 8** для Cipher Key відповідно для різних довжин ключів.

Визначення й допоміжні процедури

Визначення:

– Block – послідовність біт, з яких складається input, output, State і Round Key. Також під Block можна розуміти послідовність байт.

– Cipher Key – секретний, криптографічний ключ, що використовується Key Expansion процедурою, щоб зробити набір ключів для раундів (Round Keys); може бути представлений як прямокутний масив байтів, що має чотири рядки й *Nk* колонок.

– Ciphertext – вихідні дані алгоритму шифрування, з метою збереження конфіденційності.

– Key Expansion – процедура використовувана для генерації Round Keys з Cipher Key.

– Round Key – Round Keys виходять із Cipher Key використовуючи процедуру Key Expansion. Вони застосовуються до State при шифруванні й розшифруванні.

– State – проміжний результат шифрування, з метою збереження конфіденційності, що може бути представлений як прямокутний масив байтів що має 4 рядки й *Nb* колонок.

– S-box – нелінійна таблиця замін, що використовується в декількох трансформаціях заміни байт і в процедурі Key Expansion для взаємнооднозначної заміни значення байта.

– *Nb* – число стовпців (32-ух бітних слів), що становлять *State*. Для, AES *Nb* = 4.

– *Nk* – число 32-ух бітних слів, що становлять шифроключ. Для AES, *Nk* = 4,6, або 8.

– *Nr* – число раундів, що є функцією *Nk* і *Nb*. Для AES, *Nr* = 10, 12, 14.

– Rcon[] – масив, що складається з біт 32-х розрядного слова і є постійним для даного раунду.

Допоміжні процедури:

– AddRoundKey () – трансформація при шифруванні й зворотному шифруванні, при якуму Round Key XOR *c* State. Довжина RoundKey дорівнює розміру State (ті, якщо *Nb* = 4, то довжина RoundKey дорівнює 128 біт або 16 байт).

– InvMixColumns () – трансформація при розшифруванні яка є зворотною стосовно MixColumns ().

– InvShiftRows () – трансформація при розшифруванні яка є зворотною стосовно ShiftRows ().

– InvSubBytes () – трансформація при розшифруванні яка є зворотною стосовно SubBytes ().

– MixColumns () – трансформація при шифруванні яка бере всі стовпці State і змішує їх дані (незалежно друг від друга), щоб одержати нові стовпці.

– RotWord () – функція, що використовується в процедурі Key Expansion, що бере 4-х байтне слово й робить над ним циклічну перестановку.

– ShiftRows () – трансформації при шифруванні, які обробляють State, циклічно зміщаючи останні три рядки State на різні величини.

– SubBytes () – трансформації при шифруванні які обробляють State використовуючи нелінійну таблицю заміщення байтів (S-box), застосовуючи її незалежно до кожного байта State.

– SubWord () – функція, використовувана в процедурі Key Expansion, що бере на вході чотирьохбайтне слово й застосовуючи S-box до кожного із чотирьох байтів видає вихідне слово.

На початку шифрування, з метою збереження конфіденційності, input копіюється в масив State за правилом:

$$s[r,c] = in[r + 4c],$$

для $0 \le r < 4$ й $0 \le c < Nb$.

Після цього до State застосовується процедура AddRoundKey () і потім State проходить через процедуру трансформації (раунд) **10, 12,** або **14** разів (залежно від довжини ключа), при цьому треба врахувати, що останній раунд трохи відрізняється від попередніх. У підсумку, після завершення останнього раунду трансформації, State копіюється в output за правилом:

$out[r + 4c] = s[r,c]$,

для $0 \le r < 4$ й $0 \le c < Nb$.

Операція шифрування, з метою збереження конфіденційності, описана в псевдокоді. Окремі трансформації SubBytes (), ShiftRows (), MixColumns (), і AddRoundKey () – обробляють State. Масив *w*[] – містить key schedule.

Функція шифрування в псевдокоді

```
Cipher (byte in[4*Nb], byte out[4*Nb], word w[Nb* (Nr+1)])
begin
  byte state[4,Nb]
  state = in
  AddRoundKey (state, w[0, Nb-1])
  for round = 1 step 1 to Nr-1
    SubBytes (state)
    ShiftRows (state)
    MixColumns (state)
    AddRoundKey (state, w[round*Nb, (round+1)* Nb-1])
  end for
  SubBytes (state)
  ShiftRows (state)
  AddRoundKey (state, w[Nr*Nb, (Nr+1)* Nb-1])
  out = state
end
```

SubBytes ()

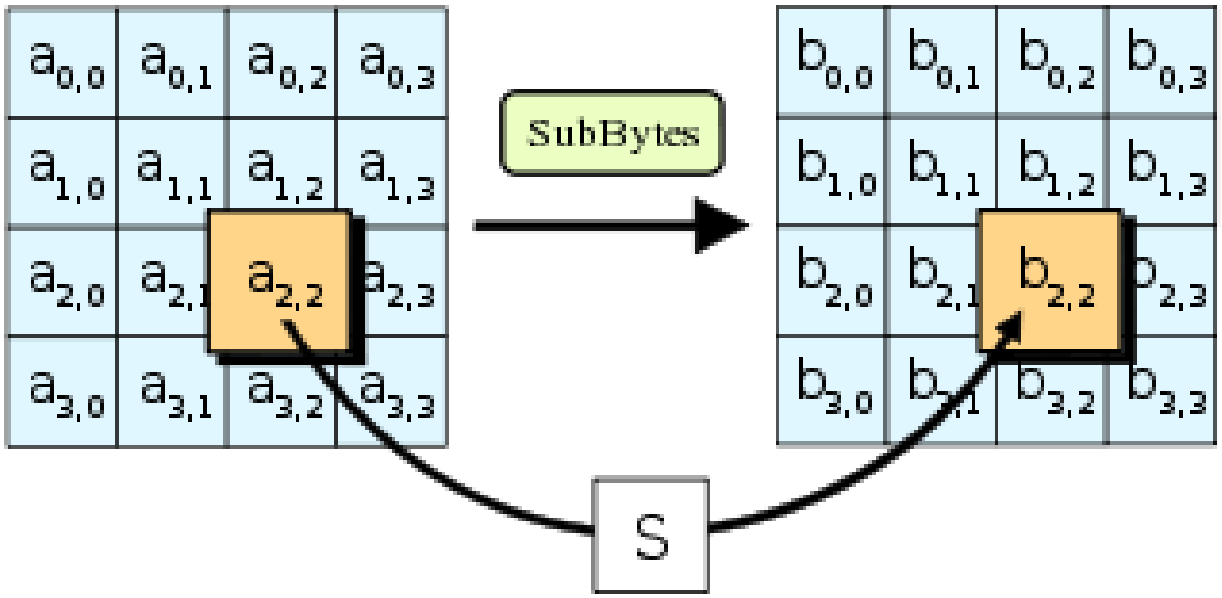


Рисунок 17.8 – Опис процедури SubBytes ()

У процедурі SubBytes, кожний байт в state заміняється відповідним елементом у фіксованої 8-бітній таблиці пошуку, *S*; $b_{ij} = S(a_{ij})$.

Процедура SubBytes () обробляє кожний байт стану, незалежно роблячи нелінійну заміну байтів використовуючи таблицю замін (S-box). Така операція забезпечує нелінійність алгоритму шифрування, з метою збереження конфіденційності. Побудова S-box складається із двох кроків. По-перше, виробляється узяття оберненого числа в GF$\{2^8\}$. По-друге, до кожного байта *b* з яких складається S-box застосовується наступна операція:

$$b_i' = b_i \oplus b_{(i+4)mod8} \oplus b_{(i+5)mod8} \oplus b_{(i+6)mod8} \oplus b_{(i+7)mod8} \oplus c_i,$$

де:

– $0 \leq i < 8$;

– b_i є *i-ий* біт *b*,

– c_i – *i-ий* біт *c* = {63} або {01100011}.

Таким чином, забезпечується захист від атак, заснованих на простих алгебраїчних властивостях.

$$\begin{Vmatrix} b_0' \\ b_1' \\ b_2' \\ b_3' \\ b_4' \\ b_5' \\ b_6' \\ b_7' \end{Vmatrix} = \begin{Vmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{Vmatrix} * \begin{Vmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{Vmatrix} + \begin{Vmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{Vmatrix}$$

S-box можна відобразити таблицею простої підстановки:

S-box																
\	0	1	2	3	4	5	6	7	8	**9**	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	**d4**	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Наприклад, на вході **19** на виході отримаємо **d4**.

Фактично це звичайний шифр простої підстановки.

ShiftRows ()

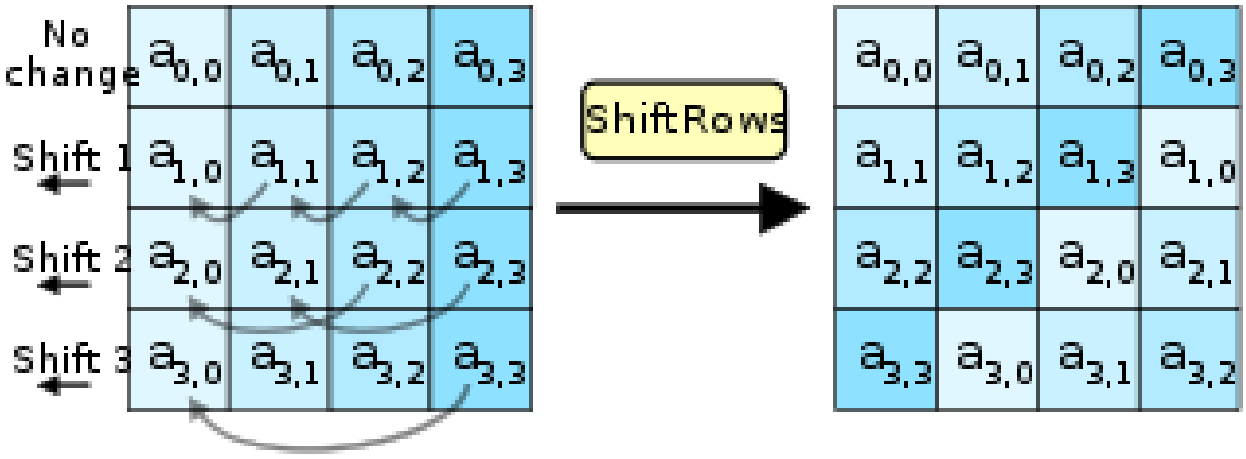


Рисунок 17.9 – Опис процедури ShiftRows ()

У процедурі ShiftRows, байти в кожному рядку state циклічно зрушуються вліво. Розмір зсуву байтів кожного рядка залежить від її номера.

ShiftRows працює з рядками State. При цій трансформації рядка стани циклічно зрушуються на *r* байт по горизонталі, залежно від номера рядка. Для нульового рядка $r = 0$, для першого рядка $r = 1$ і т.д.. У такий спосіб кожна колонка вихідного стану після застосування процедури ShiftRows складається з байтів з кожної колонки початкового стану. Для алгоритму Rijndael паттерн зсуву рядків для 128 і 192-х бітних рядків однаковий. Однак для блоку розміром 256 біт відрізняється від попередніх тим, що 2, 3, і 4-і рядки зміщаються на 1, 3, і 4 байти відповідно.

MixColumns ()

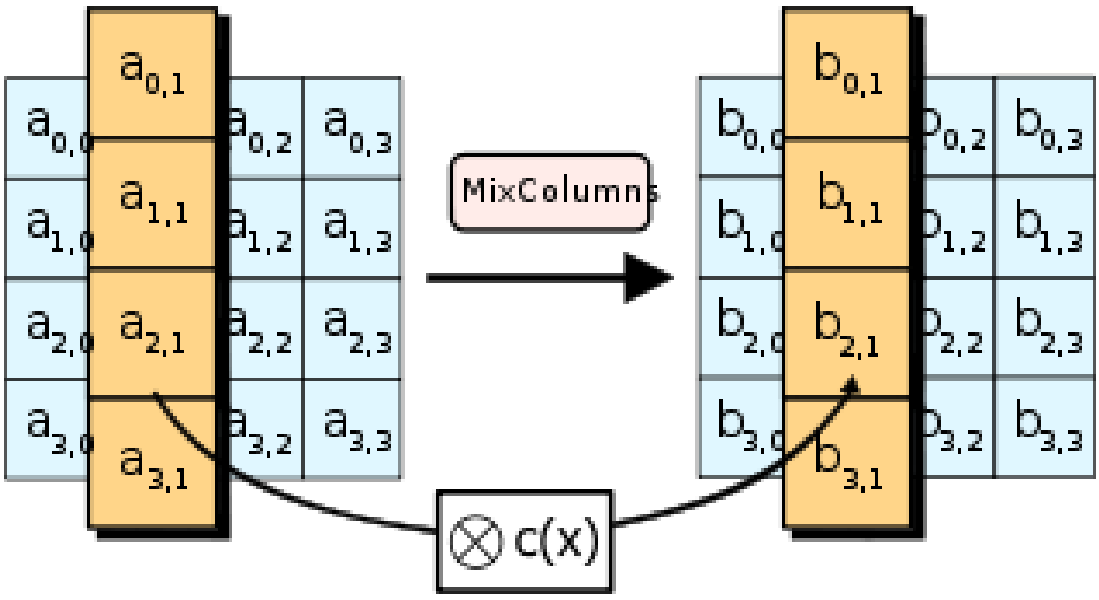


Рисунок 17.10 – Опис процедури MixColumns ()

У процедурі MixColumns, кожна колонка стану перемножується з фіксованим багаточленом *c (x)*.

У процедурі MixColumns, чотири байти кожної колонки State змішуються використовуючи для цього оборотну лінійну трансформацію. MixColumns обробляє стану по колонках, трактуючи кожну з них як поліном четвертого ступеня. Над цими поліномами виробляється множення в $GF(2^8)$ за модулем $x^4 + 1$ на фіксований багаточлен $c(x) = 3x^3 + x^2 + x + 2$. Разом з ShiftRows, MixColumns вносить дифузію в шифр.

AddRoundKey ()

У процедурі AddRoundKey, кожний байт стану поєднується з RoundKey використовуючи XOR operation (⊕).

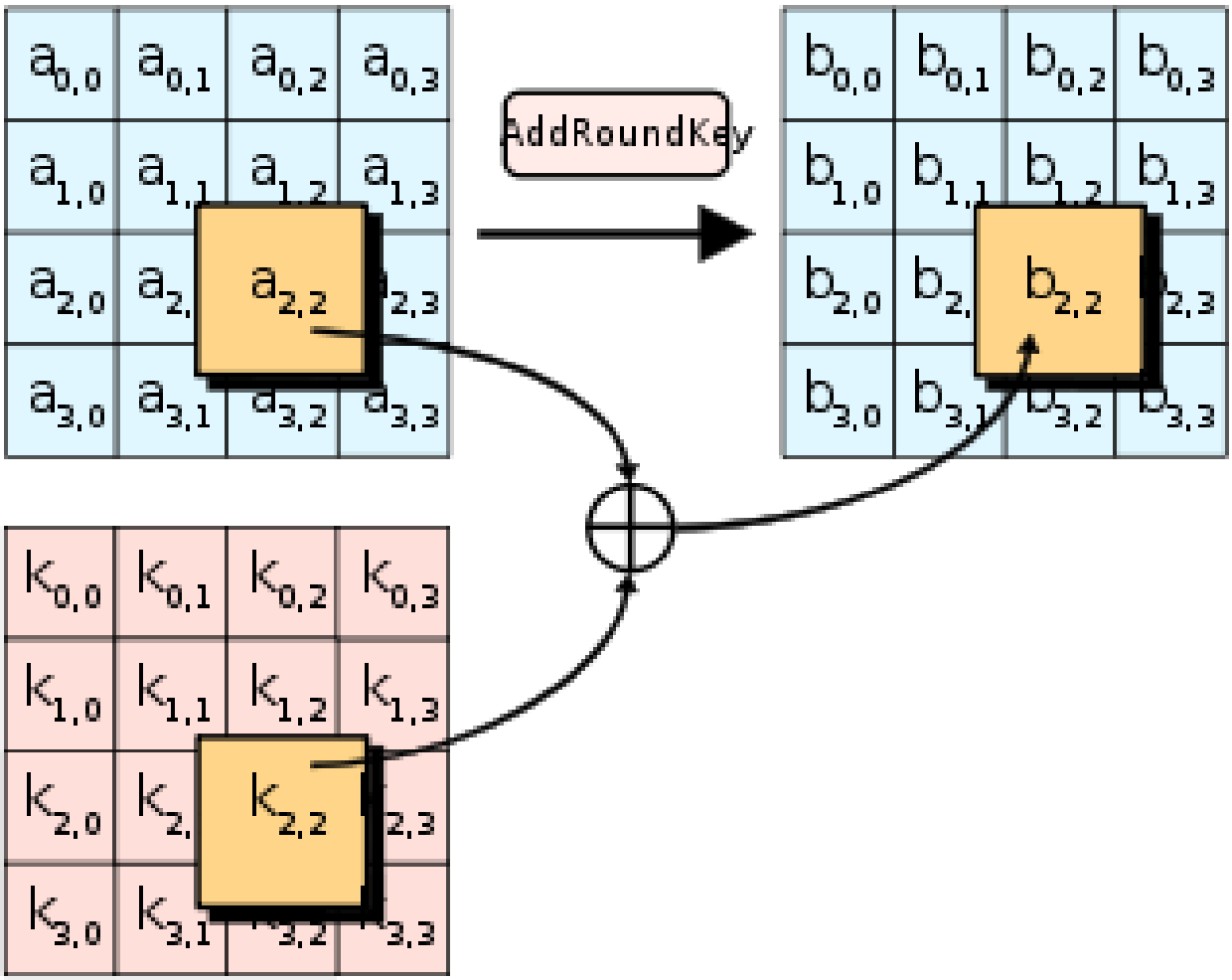


Рисунок 17.11 – Опис процедури AddRoundKey ()

У процедурі AddRoundKey, RoundKey кожного раунду поєднується з State. Для кожного раунду Roundkey виходить із CipherKey використовуючи процедуру KeyExpansion; кожний RoundKey такого ж розміру, що й State. Процедура робить побітовий XOR кожного байта State з кожним байтом RoundKey.

Опис симетричного алгоритму шифрування ДСТУ 7624:2014 (Калина) згідно з ДСТУ ISO/IEC 10116:2019

«Калина» (англ. Kalyna) – блочний симетричний шифр описаний у національному стандарті України ДСТУ 7624:2014 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення». Стандарт набрав чинності з 1 липня 2015 року наказом Мінекономрозвитку від 2 грудня 2014 року №1484. Текст стандарту у вільному доступі.

Стандарт ДСТУ 7624:2014 розроблено у співпраці Держспецзв'язку та провідних українських науковців і враховує досвід та результати проведення міжнародних і відкритого національного конкурсу криптографічних алгоритмів. Він призначений для поступової заміни міждержавного стандарту ДСТУ ГОСТ 28147:2009.

Згідно чинного наказу Мінцифри від 30 вересня 2020 року №140/614 після 1 січня 2022 року разом з функцією ґешування Купина є обов'язковим для використання при накладанні та перевірці електронного цифрового підпису за ДСТУ 4145-2002 замість криптографічного перетворення за ДСТУ ГОСТ 28147:2009.

Розмір блоку може складати 128, 256, 512 біт. (відповідно 10, 14, 30 раундів шифрування).

Використовує 8 S-боксів 8*8 біт. (8*256 = 2048 байт).

Основні відмінності “Калини” від Rijndael (AES):

– збільшена кількість циклів шифрування (запас стійкості);

– використання додавання за модулем 2^{32} і за модулем 2 для введення ключової інформації (захист від алгебраїчних атак, лінійного та диференціального криптоаналізів, інтерполяційної атаки тощо);

– використання 8 блоків нелінійного перетворення (S-блоків) замість одного (додатковий захист від алгебраїчних атак, поліпшення властивостей розсіювання шифру – поліпшені статистичні властивості, відповідно більш високий рівень стійкості до диференціального та лінійного криптоаналізів тощо);

– використання випадково сформованих S-блоків, відібраних за критеріями стійкості до диференціального, лінійного криптоаналізів та степені нелінійності булевих функцій (на відміну від S-блоку Rijndael/Camellia та інших шифрів, що використовують звернення в полі та, відповідно, квадратичні залежності між входом і виходом – захист від алгебраїчних атак);

– принципово нова схема створення підключів (захист від всіх відомих атак на схеми створення підключів;

– досить висока продуктивність;

– високе відновлення майстер-ключа за окремим підключем – додатковий захист від атак, що виконують відновлення підключів).

Всі поліпшення спрямовані на збільшення стійкості та перекриття потенційних вразливостей відносно Rijndael, що виявлені в останні роки.

Режими роботи та їх позначення

У стандарті описані наступні режими роботи криптографічного алгоритму, їх позначення та послуги безпеки, які забезпечує відповідний режим

Таблиця 17.1 – Режими роботи алгоритму

#	**Назва режиму**	**Позначення**	**Послуга безпеки**
1	Проста заміна (базове перетворення)	ECB	Конфіденційність
2	Гамування	CTR	Конфіденційність
3	Гамування зі зворотним зв'язком за шифротекстом	CFB	Конфіденційність
4	Вироблення імітовставки	CMAC	Цілісність
5	Зчеплення шифроблоків	CBC	Конфіденційність
6	Гамування зі зворотним зв'язком за шифрогамою	OFB	Конфіденційність
7	Вибіркове гамування із прискореним виробленням імітовставки	GCM, GMAC	Конфіденційність і цілісність (GCM), тільки цілісність (GMAC)
8	Вироблення імітовставки і гамування	CCM	Цілісність і конфіденційність
9	Індексована заміна	XTS	Конфіденційність
10	Захист ключових даних	KW	Конфіденційність і цілісність

Режим роботи криптографічного алгоритму, позначають так: **«Калина-I/k-позначення режиму-параметри режиму»** (для деяких режимів параметрів немає), де I – розмір блока базового перетворення, k – довжина ключа. Наприклад, **«Калина-256/512-CCM-32,128»** визначає використання базового перетворення з розміром блока 256 бітів, довжиною ключа 512 бітів, застосування у режимі вироблення імітовставки і гамування, довжина конфіденційної (та відкритої) частини повідомлення завжди менше ніж 232 байтів, довжина імітовставки дорівнює 128 бітів. Режим простої заміни збігається з базовим перетворенням, тому крім позначення **«Калина-I/k-ECB»** можна використовувати позначення **«Калина-I/k»**.

Загальна структура алгоритму

Загальна структура – SPN, square-type, байт-орієнтований шифр. Структура алгоритму аналогічна структурі Rijndael, забезпечує гарне розсіювання та перемішування (відмінні криптографічні та статистичні властивості, висока продуктивність).

Використовуються цикли перетворення 2-х типів: із введенням ключа за модулем 2 і за модулем 2^{32}, що збільшує нелінійність шифру, вводить додаткові залежності між результуючими значеннями.

Значно збільшує стійкість до алгебраїчних атак, диференціального та лінійного криптоаналізів тощо.

Таблиці підстановки (вузли нелінійного перетворення)

Застосування випадково сформованих таблиць підстановок, відібраних за критеріями стійкості до диференціального, лінійного криптоаналізів та ступеня нелінійності булевих функцій.

S-блоки Rijndael/Camellia та інших шифрів використовують перетворення в полі. Такий S-блок забезпечує найкращі показники з погляду диференційного та лінійного криптоаналізів (ДК/ЛК), але підстановка (S-блок) має яскраво виражену математичну структуру та просте алгебраїчне подання. Відповідно, досить серйозну загрозу наявності вразливостей шифру до алгебраїчних атак.

Маючи багаторазовий запас стійкості до ДК/ЛК (як в Rijndael, так і в "Калини"), можливе використання S-блоків з небагато гіршими показниками S-блоку, ніж в Rijndael, але в той же час позбутися від явної математичної структури, що дозволяє побудувати квадратичні залежності між входом і виходом.

Використання випадкових S-блоків дозволяє позбутися від таких залежностей (детермінованих), і перейти до ймовірнісних рівнянь опису підстановки в алгебраїчних атаках.

Застосування 8 підстановок додатково знижує можливість побудови та ймовірність знаходження правильного рішення для такої системи рівнянь.

Крім того, використання 8 S-блоків замість одного – поліпшення статистичних властивостей, відповідно більш високий рівень стійкості до диференціального та лінійного криптоаналізів тощо.

У цілому до формування S-блоків шифру "Калина" були задані такі вимоги:

– випадкова генерація, що забезпечує мінімізацію ймовірності одержання строгих математичних залежностей між вхідними та вихідними бітами;

– обмеження максимального значення ймовірність проходження різниці через підстановку (для "Калини" – 2^{-5}, для Rijndael – теоретично досяжний мінімум – 2^{-6});

– обмеження максимального значення ймовірності лінійної апроксимації підстановки (для "Калини" – 2^{-5}, для Rijndael – теоретично досяжний мінімум – 2^{-3});

– нелінійний порядок підстановки (для "Калини" теоретично досяжний максимум).

Можливе використання довільних S-блоків (відмінних від наведених у специфікації), що задовольняють даним вимогам, при цьому всі криптографічні властивості та стійкість шифру зберігаються.

Крім того, допускається використання S-блоків як додатково встановлюваного секретного параметра.

Блок лінійного перетворення

Як блок лінійного перетворення використовується добре перевірене МДР-перетворення (MixColumns), що дає найкращі властивості розсіювання (поширення різниці).

Завдяки використанню 64-бітного МДР-коду, забезпечується повна

залежність кожного біта від входу вже на 2-х циклах шифрування, незалежно від розміру блоку. МДР-код – це лінійний код, для якого виконується рівність: k = n – d + 1. Відомим представником таких кодів, є коди Ріда –Соломона.

Характеристики кращі, ніж в Rijndael 256/256, де потрібна більша кількість циклів для поширення різниці на весь блок.

Недолік – менш ефективна реалізація на 32-бітових процесорах, що поки використовуються.

Проте на 64-бітових процесорах, що одержують все більше поширення, показники продуктивності близькі до Rijndael.

Розширення ключа

Недоліки схеми створення підключів Rijndael:

– можливість відновлення майстер-ключа за одним підключем (!);

– досить прості залежності між підключами (уразливість до атак на зв'язаних ключах);

– перший з підключів – майстер-ключ (!);

– слабкий вплив змін бітів майстер-ключа на біти перших підключів (задовільні результати – тільки 5-7 підключів)

– використання в схемі розгортання іншої конструкції, відмінної від циклової функції;

– різна складність генерації послідовності підключів для шифрування та дешифрування.

У зв'язку з наявністю істотних недоліків було прийнято використовувати **принципово нову схему розгортання ключів**. Вона розроблена на основі таких вимог:

– нелінійна залежність кожного біта кожного підключа від кожного біта майстер-ключа, відповідно забезпечення всіх необхідних лавинних властивостей і відсутність "проміжних точок";

– забезпечення стійкості до всіх відомих атак на схеми створення підключів;

– відсутність слабких ключів, на яких може відбутися погіршення криптографічних властивостей шифру;

– неможливість (висока обчислювальна складність) відновлення майстер-ключа за одним або декількома підключами;

– простота реалізації, використання циклового перетворення шифру;

– обчислювальна складність генерації всіх підключів не перевищує складності однієї операції шифрування;

– можливість генерації підключів у будь-якому порядку (як для шифрування, так і для дешифрування).

Вимоги до констант C^j_{len}:

– різні константи для різних ключових станів (видалення симетрії між циклами);

– відмінності 64-бітних блоків, що попадають на MixColumn, у межах

однієї константи (видалення симетрії перетворення, що шифрує, у межах циклу).

Можливе використання довільних значень, що задовольняють цим вимогам, при цьому всі криптографічні властивості та стійкість шифру зберігаються. У специфікації наведені найбільш очевидні значення.

Режими роботи симетричного блокового шифру

На основі аналізу встановлено, що доцільно використовувати стандартні режими роботи, які визначені в NIST SP 800-38A (режими ГОСТ 28147-89, крім створення імітовставки, є підмножиною цих режимів).

Ці режими використовуються більше 20 років (специфікація DES modes of operation), існують рекомендації з їх вибору для конкретних умов застосування, і використання цих режимів забезпечує високий рівень захисту переданих повідомлень, властивості режимів добре досліджені.

Через недостатнє дослідження на даний момент вважаємо недоцільним використання режиму, що одночасно забезпечує конфіденційність і цілісність повідомлень.

Режим забезпечення цілісності

Недолік стандартного CBC: неможливість обробки повідомлення, якщо його довжина не кратна розміру блоку шифру (потрібне доповнення повідомлення, причому імітовставка доповненого повідомлення та співпадаючого з ним недоповненого, такої ж довжини, залишається деякий ризик нав'язування).

Вимоги до режиму забезпечення цілісності:

– відповідність всім вимогам стійкості, пропонованих до ґеш-функцій;

– можливість обробки повідомлень довільної довжини;

– використання одного ключа шифрування;

– забезпечення стійкості.

Більшість відомих альтернативних схем використовують 2 або 3 ключі шифрування, що є істотним недоліком.

З відомих режимів один ключ використовується в OMAC, при цьому забезпечується захист механізму доповнення повідомлення, чия довжина не кратна розміру блоку.

Краща атака на OMAC є атакою з обраними відкритими текстами, коли криптоаналітик виконує статистичний пошук колізії ($2^{n/2}$ шифрувань, де n – розмір блоку), тобто фактично теоретичний максимум стійкості.

Схема є стійкою, має низьку обчислювальну складність, проста в реалізації та зручна у використанні.

Детальний опис алгоритму «Калина»

Допустимі комбінації розміру блока та довжини ключа шифрування наведено у таблиці 17.2.

Таблиця 17.2 – Параметри алгоритму “Калина”

№ з/п	Розмір блоку (l)	Довжина ключа (k)	Кількість ітерацій перетворення (t)	Кількість стовпців в матриці (c)
1	128	128	10	2
2		256	14	
3	256	256	14	4
4		512	18	
5	512	512	18	8

Алгоритм шифрування є процедурою, що складається з попереднього і прикінцевого забілювання та ітеративного циклового перетворення. На вхід кожного циклового перетворення подається поточний стан, а також необхідна кількість ключової інформації (цикловий ключ). Відкритий текст копіюється в поточний стан перед початком зашифрування, а після його завершення в поточному стані знаходиться шифртекст. Кількість циклів шифрування (N r) залежить від довжини ключа; її наведено у таблиці 17.2. На початку та у кінці процедури зашифрування/розшифрування виконуються додаткові операції забілювання.

У стандарті визначені обсяги повідомлень, після обробки яких потрібна обов’язкова зміна ключа. Крім того, наводяться рекомендації розробникам, що звертають увагу на необхідність запобігання атак з використанням особливостей реалізації засобів шифрування. Зокрема, враховані особливості, які дозволяли організацію атак BEAST і CRIME/BREACH в протоколах SSL/TLS, повторний прийом повідомлень, відновлення конфіденційних параметрів на основі залежності часу шифрування від даних (через промахи кешу при табличній реалізації) та інших.

До вхідних та вихідних даних алгоритму “Калина” належать відкритий текст та шифртекст відповідно. Ці параметри представляються у вигляді рядків заданої довжини $8 \times Nb$ байт ($64 \times Nb$ біт). Додатковим вхідним параметром є ключ, розмір якого дорівняє $8 \times Nk$ байт ($64\times Nk$ біт). Байтовий рядок довжиною $n = 8 \times Nb$ байт представляється у наступній формі: $B_0\ B_1\ B_2\ \ldots\ B_{n-1}$.

До початку зашифрування відкритий текст копіюється в поточний стан шифру. Після завершення процедури зашифрування шифртекст копіюється з поточного стану.

Відкритий текст представлено байтовим рядком $in_0, in_1, \ldots in_{31}$. Отриманий шифртекст представлено як послідовність байт $out_0, out_1, \ldots out_{31}$.

Заповнення початкового стану шифру перед початком зашифрування та після його закінчення для блоку 128 біт представлено на на рис.17.12.

Вхідна послідовність		→	Поточний стан		→	Вихідна послідовність	
in_0	in_8		$s_{0,0}$	$s_{0,1}$		out_0	out_8
in_1	in_9		$s_{1,0}$	$s_{1,1}$		out_1	out_9
in_2	in_{10}		$s_{2,0}$	$s_{2,1}$		out_2	out_{10}
in_3	in_{11}		$s_{3,0}$	$s_{3,1}$		out_3	out_{11}
in_4	in_{12}		$s_{4,0}$	$s_{4,1}$		out_4	out_{12}
in_5	in_{13}		$s_{5,0}$	$s_{5,1}$		out_5	out_{13}
in_6	in_{14}		$s_{6,0}$	$s_{6,1}$		out_6	out_{14}
in_7	in_{15}		$s_{7,0}$	$s_{7,1}$		out_7	out_{15}

Рисунок 17.12 – Заповнення початкового стану для довжини блоку 128 біт

Аналогічно, при розшифруванні шифртекст позначається байтовою послідовністю in_0, in_1,… $in_{31;}$ отриманий відкритий текст представлено послідовністю байт $out_{0,}$ out_1, …out_{31}; заповнення відповідає рис.17.12.

Операція лінійного розсіювання (перемішування в стовбці) алгоритму “Калина” використовує поліноміальне представлення байт в полі GF (2^8), сформованому незвідним поліномом. Для алгоритму шифрування “Калина” у якості незвідного полінома використовується $f(x) = x^8 + x^4 + x^3 + x^2 + 1$.

Зашифрування у режимі простої заміни передбачає те, що на вхід процедури подається відкритий текст та циклові ключі. На початку зашифрування відкритий текст представляється у вигляді блоку даних, що описує поточний стан шифру. Після закінчення зашифрування отриманий шифртекст формується у вигляді байтової послідовності.

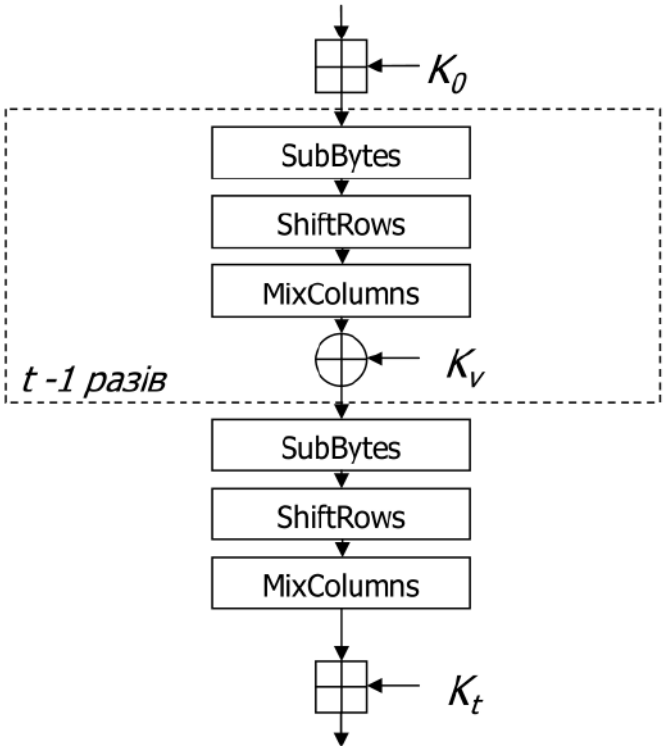


Рисунок 17.13 – Алгоритм шифрування «Калина»

При здійсненні перетворення XORRoundKey (функція $K_l^{(Kv)}$ в ДСТУ 7624:2014) виконується побітове складання за модулем 2 (XOR) поточного стану та циклового ключа. Після виконання операції результат записується на місце першого аргументу.

Представлення циклового ключа як матриці віповідного розміру є аналогічним представленню відкритого тексту у вигляді поточного стану шифра.

Для поточного стану $A = (a_{i,j})$ та циклового ключа $k = (k_{i,j})$ результат перетворення $B = (b_{i,j}) = A \oplus k$ обчислюється за формулою $b_{i,j} = a_{i,j} \oplus k_{i,j}$, $0 \le i < 8$, $0 \le j < N_b$. Приклад здійснення перетворення для розміру блока 128 біт представлено на рис. 17.14.

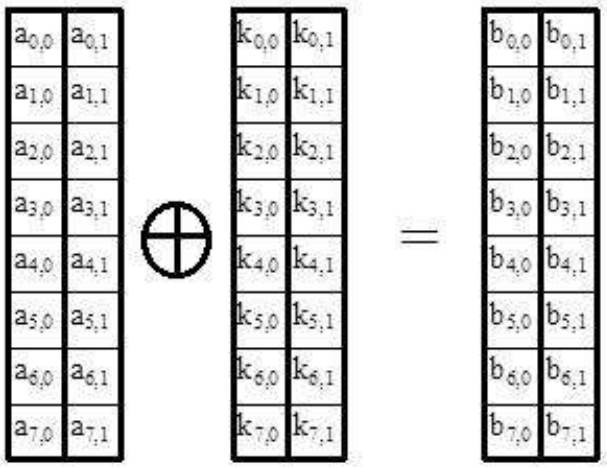


Рисунок 17.14 – Перетворення XORRoundKey для розміру блока 128 біт

При здійсненні Add64RoundKey виконується складання за модулем 2^{64} 64-бітних слів поточного стану та циклового ключа. Після виконання операції результат записується на місце першого аргументу (рис 17.15).

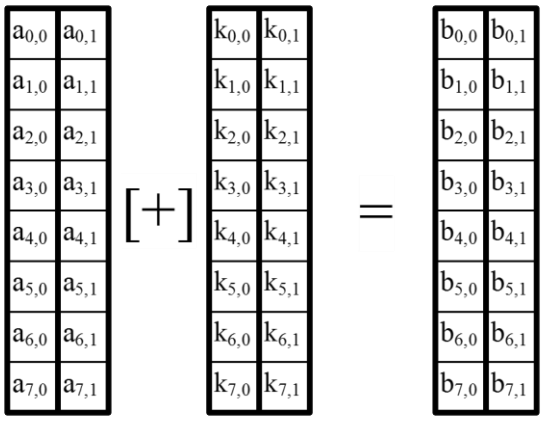


Рисунок 17.15 – Перетворення Add64RoundKey для розміру блока 128 біт

Представлення циклового ключа як матриці віповідного розміру є аналогічним представленню відкритого тексту у вигляді поточного стану шифру. При розбитті поточного стану та циклового ключа на 64-бітні блоки молодшим бітом 64-бітного блоку буде молодший біт байту рядка з найменшим номером, старшим бітом 64-бітного блоку – старший біт байта рядка з найбільшим номером (формат little endian).

Перетворення Kalyna_S_boxes виконує заміну кожного байта поточного стану у відповідності з заданою таблицею підстановки. Використовуються 4 різні підстановки “байт-в-байт”, причому для байтів одного рядка поточного стану шифру використовується одна і та ж підстановка:

для байт 0-го рядка (елементи s 0,i) – підстановка S0;
для байт 1-го рядка (елементи s 1,i) – підстановка S1;
для байт 2-го рядка (елементи s 2,i) – підстановка S2;
для байт 3-го рядка (елементи s 3,i) – підстановка S3;
для байт 4-го рядка (елементи s 4,i) – підстановка S0;
для байт 5-го рядка (елементи s 5,i) – підстановка S1;
для байт 6-го рядка (елементи s 6,i) – підстановка S2;
для байт 7-го рядка (елементи s 7,i) – підстановка S12.

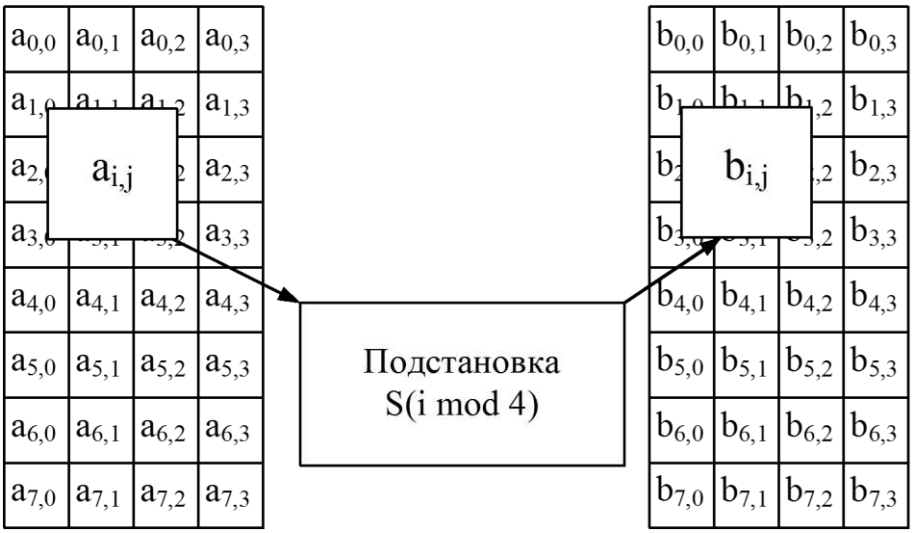


Рисунок 17.16 – Приклад підстановки байта для розміра блоку 256 біт

Заміна одного байту полягає у виборі з таблиці підстановки нового значення за адресою із зсувом, що задає поточне значення байту. Нове вибране значення і є результатом здійснення підстановки для одного байту.

Приклад підстановки для таблиці S0 байта з шістнадцятковим значенням 5A наведено у табл. 17.17.

Таблиця 17.3 – Приклад підстановки для таблиці S0

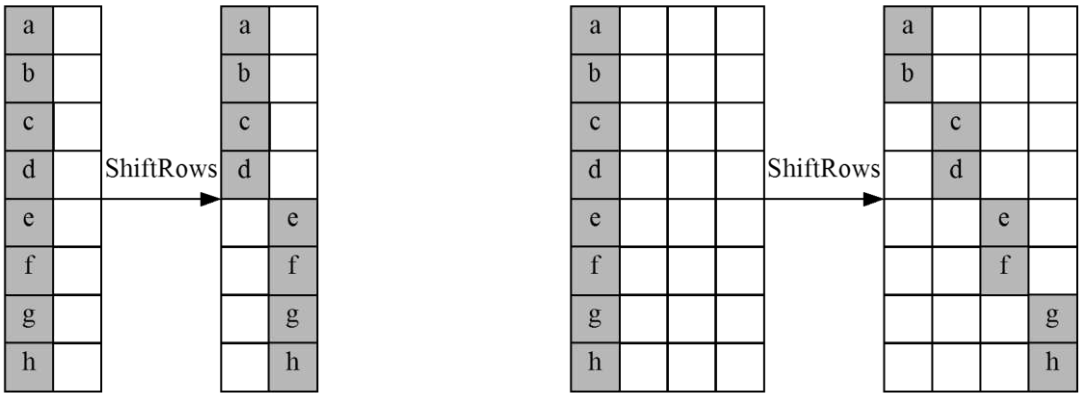
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	A8	43	5F	06	6B	75	6C	59	71	DF	87	95	17	F0	D8	09
1	6D	F3	1D	CB	C9	4D	2C	AF	79	E0	97	FD	6F	4B	45	39
2	3E	DD	A3	4F	B4	B6	9A	0E	1F	BF	15	E1	49	D2	93	C6
3	92	72	9E	61	D1	63	FA	EE	F4	19	D5	AD	58	A4	BB	A1
4	DC	F2	83	37	42	E4	7A	32	9C	CC	AB	4A	8F	6E	04	27
5	2E	E7	E2	5A	96	16	23	2B	C2	65	66	0F	BC	A9	47	41
6	34	48	FC	B7	6A	88	A5	53	86	F9	5B	DB	38	7B	C3	1E
7	22	33	24	28	36	C7	B2	3B	8E	77	BA	F5	14	9F	08	55
8	9B	4C	FE	60	5C	DA	18	46	CD	7D	21	B0	3F	1B	89	FF
9	EB	84	69	3A	9D	D7	D3	70	67	40	B5	DE	5D	30	91	B1
A	78	11	01	E5	00	68	98	A0	C5	02	A6	74	2D	0B	A2	76
B	B3	BE	CE	BD	AE	E9	8A	31	1C	EC	F1	99	94	AA	F6	26
C	2F	EF	E8	8C	35	03	D4	7F	FB	05	C1	5E	90	20	3D	82
D	F7	EA	0A	0D	7E	F8	50	1^a	C4	07	57	B8	3C	62	E3	C8
E	AC	52	64	10	D0	D9	13	0C	12	29	51	B9	CF	D6	73	8D
F	81	54	C0	ED	4E	44	A7	2^a	85	25	E6	CA	7C	8B	56	80

Старші 4 біти визначають рядок, молодші 4 біти – стовбець. Результат підстановки для значення 5A – це число в шістнадцятковому представленні 66, що знаходиться в таблиці на перетині 6-го рядка (з індексом 5) та 11-го стовбця.

Під час виконання перетворення ShiftRows (перестановка елементів τ_i в ДСТУ 7624:2014) здійснюється рівномірне розподілення байт кожного 64-бітного стовбця серед інших стовбців. Це досягається шляхом циклічного зсуву рядків стану вправо на різну кількість байт. Значення зсувів залежать від розміру блока шифрування і представлені у табл. 17.4. Рис. 17.17 пояснює порядок виконання перетворення ShiftRows для різних розмірів блоку.

Таблиця 17.4 – Значення циклічних зсувів рядків для різних розмірів блоку

Номер рядка	Значення зсуву, байти		
	Довжина блоку 128 біт	Довжина блоку 256 біт	Довжина блоку 512 біт
0	0	0	0
1	0	0	1
2	0	1	2
3	0	1	3
4	1	2	4
5	1	2	5
6	1	3	6
7	1	3	7



а) 128-бітний блок б) 256-бітний блок

Рисунок 17.17 – Порядок розподілення байт першого стовбця при здійсненні перетворення ShiftRows

Під час здійснення перетворення MixColumns (лінійне перетворення ψ_l в ДСТУ 7624:2014) виконується послідовна обробка всіх стовбців поточного стану. Кожний 8-байтний стовбець розглядається як поліном над полем GF (2^8), що складається з суми 8 одночленів (кожний байт представляється у вигляді елемента поля GF (2^8) і є коефіцієнтом перед змінною степеня, що дорівнює індексу байту у стовбці). При перетворенні виконується множення цього полінома за модулем x^8+1 на фіксований поліном C (*x*), де

$$C(x) = \{01\}x^7 + \{05\}x^6 + \{01\}x5 + \{08\}x^4 + \{06\}x^3 + \{07\}x^2 + \{04\}x + \{01\}.$$

Ця операція еквівалентна матричному множенню над GF (2^8) початкового 8-байтового вектору на фіксовану матрицю, результат зберігається у 8 байтний вектор b (див. рис. 17.18).

Порядок обчислення елементів результуючого вектору *b* пояснюється на рис. 17.19 при цьому всі операції множення на байт виконуються у полі GF (2^8). шифру.

На рис. 17.20 пояснюється порядок виконання перетворення MixColumns для поточного стану шифру.

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 01 & 01 & 05 & 01 & 08 & 06 & 07 & 04 \\ 04 & 01 & 01 & 05 & 01 & 08 & 06 & 07 \\ 07 & 04 & 01 & 01 & 05 & 01 & 08 & 06 \\ 06 & 07 & 04 & 01 & 01 & 05 & 01 & 08 \\ 08 & 06 & 07 & 04 & 01 & 01 & 05 & 01 \\ 01 & 08 & 06 & 07 & 04 & 01 & 01 & 05 \\ 05 & 01 & 08 & 06 & 07 & 04 & 01 & 01 \\ 01 & 05 & 01 & 08 & 06 & 07 & 04 & 01 \end{bmatrix} \times \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{bmatrix}$$

Рисунок 17.18 – Матричне представлення перемішування у стовбці

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 01\cdot a_0 \oplus 01\cdot a_1 \oplus 05\cdot a_2 \oplus 01\cdot a_3 \oplus 08\cdot a_4 \oplus 06\cdot a_5 \oplus 07\cdot a_6 \oplus 04\cdot a_7 \\ 04\cdot a_0 \oplus 01\cdot a_1 \oplus 01\cdot a_2 \oplus 05\cdot a_3 \oplus 01\cdot a_4 \oplus 08\cdot a_5 \oplus 06\cdot a_6 \oplus 07\cdot a_7 \\ 07\cdot a_0 \oplus 04\cdot a_1 \oplus 01\cdot a_2 \oplus 01\cdot a_3 \oplus 05\cdot a_4 \oplus 01\cdot a_5 \oplus 08\cdot a_6 \oplus 06\cdot a_7 \\ 06\cdot a_0 \oplus 07\cdot a_1 \oplus 04\cdot a_2 \oplus 01\cdot a_3 \oplus 01\cdot a_4 \oplus 05\cdot a_5 \oplus 01\cdot a_6 \oplus 08\cdot a_7 \\ 08\cdot a_0 \oplus 06\cdot a_1 \oplus 07\cdot a_2 \oplus 04\cdot a_3 \oplus 01\cdot a_4 \oplus 01\cdot a_5 \oplus 05\cdot a_6 \oplus 01\cdot a_7 \\ 01\cdot a_0 \oplus 08\cdot a_1 \oplus 06\cdot a_2 \oplus 07\cdot a_3 \oplus 04\cdot a_4 \oplus 01\cdot a_5 \oplus 01\cdot a_6 \oplus 05\cdot a_7 \\ 05\cdot a_0 \oplus 01\cdot a_1 \oplus 08\cdot a_2 \oplus 06\cdot a_3 \oplus 07\cdot a_4 \oplus 04\cdot a_5 \oplus 01\cdot a_6 \oplus 01\cdot a_7 \\ 01\cdot a_0 \oplus 05\cdot a_1 \oplus 01\cdot a_2 \oplus 08\cdot a_3 \oplus 06\cdot a_4 \oplus 07\cdot a_5 \oplus 04\cdot a_6 \oplus 01\cdot a_7 \end{bmatrix}$$

Рисунок 17.19 – Порядок обчислення байт при виконанні перемішування

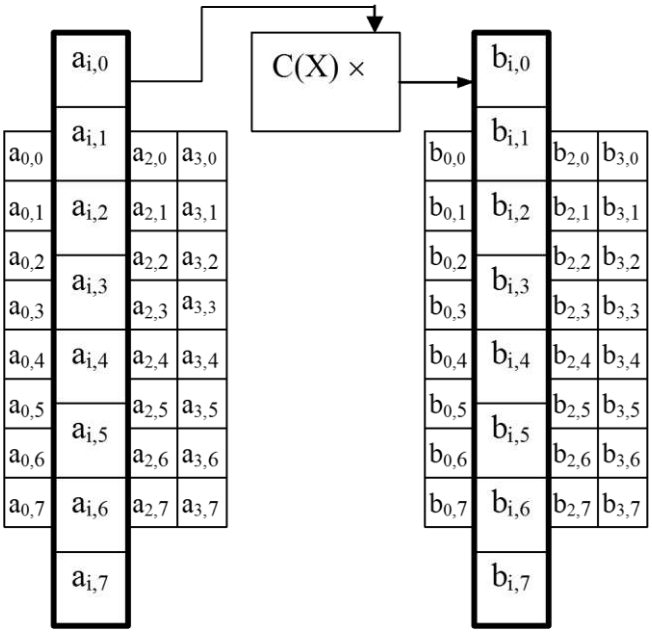


Рисунок 17.20 – Порядок виконання перетворення Mix Columns для поточного стану шифру з розміром блоку 256 біт

Процедура розшифрування є зворотною зашифруванню. На вхід подається шифртекст та циклові ключі. Після закінчення розшифрування отриманий відкритий текст формується у вигляді байтового рядка.

Операція XORRoundKey є зворотною до себе (подвійне застосування дає початкове значення), відповідно, якщо до стану $B=A \oplus k$ додати цикловий ключ k, то буде отримано початковий стан A.

При зашифруванні та розшифруванні використовується одна й та сама операція XORRoundKey.

Зворотне для Add64RoundKey перетворення Sub64RoundKey полягає в аналогічному розбитті стану та циклового ключа на 64-бітні блоки та відніманні за модулем 2^{64} від блоків стану $B = (b_i)$ відповідних блоків циклового ключа $K = (k_i)$ для отримання стану (результату).

Після виконання операції результат записується на місце першого параметра. Правила переходу від байт поточного стану до 64-бітних блоків та навпаки повністю ідентичні з перетвореннями, що виконуються під час Add64RoundKey.

ISO/IEC 10116:2017. Інформаційні технології. Методи захисту. Режими роботи n-розрядного блокового шифру

Цей документ визначає режими роботи для *n* - розрядного блочного шифру. Ці режими забезпечують методи шифрування та дешифрування даних за допомогою блокового шифру.

Це четверте видання ISO/IEC 10116 визначає п’ять режимів роботи:

– Електронна кодова книга (ECB).
– Ланцюг блоків шифру (CBC).
– Зворотній зв'язок по шифру (CFB).
– Вихідний зворотний зв'язок (OFB).
– Лічильник (CTR).

Цей документ встановлює п'ять режимів роботи для застосувань *n* - розрядного блокового шифру (наприклад, захист даних під час передачі або зберігання). Визначені режими забезпечують лише захист конфіденційності даних. Захист цілісності даних не входить до сфери застосування цього документа. Крім того, більшість режимів не захищають конфіденційність інформації про довжину повідомлення.

17.4. Потокові шифри: RC4, STRUMOK (ДСТУ 8845:2019) (довжина ключів, крипостійкість).)

RC4

RC4 (від англ. *Rivest cipher 4* або *Ron's code*), також відомий як **ARC4** або **ARCFOUR** (*alleged RC4*) – потоковий шифр, що широко застосовується в різних системах захисту інформації в комп'ютерних мережах (наприклад, в протоколах SSL і TLS, алгоритмах забезпечення безпеки бездротових мереж WEP та WPA).

Шифр розроблений компанією RSA Security і для його використання потрібна ліцензія.

Алгоритм RC4, як і будь-який потоковий шифр, будується на основі генератора псевдовипадкових бітів. На вхід генератора записується ключ, а на виході читаються псевдовипадкові біти. Довжина ключа може становити від 40 до 2048 біт. Генеровані біти мають рівномірний розподіл.

Основні **переваги шифру**:

– висока швидкість роботи;
– змінний розмір ключа.

RC4 досить вразливий, якщо:

– використовуються не випадкові чи пов'язані ключі;
– один ключовий потік використовується двічі.

Ці фактори, а також спосіб використання можуть зробити криптосистему небезпечною (наприклад, WEP).

Алгоритм шифрування RC4 застосовується в деяких широко поширених стандартах і протоколах шифрування (наприклад, WEP, WPA, SSL та TLS).

RC4 став популярним завдяки:

- простоті його апаратної та програмної реалізації;
- високої швидкості роботи алгоритму обох випадках.

У довжина ключа, рекомендована до використання у країні, дорівнює 128 бітам. Угода, укладена між «SPA» (англ. *software publishers association)* і урядом США, дозволила експортувати шифри RC4 з довжиною ключа до 40 біт. 56 бітні ключі дозволено використовувати закордонним відділенням американських компаній.

Опис алгоритму

Ядро алгоритму потокових шифрів складається з функції – генератора псевдовипадкових бітів (гами), який видає потік бітів ключа (ключовий потік, гаму, послідовність псевдовипадкових бітів).

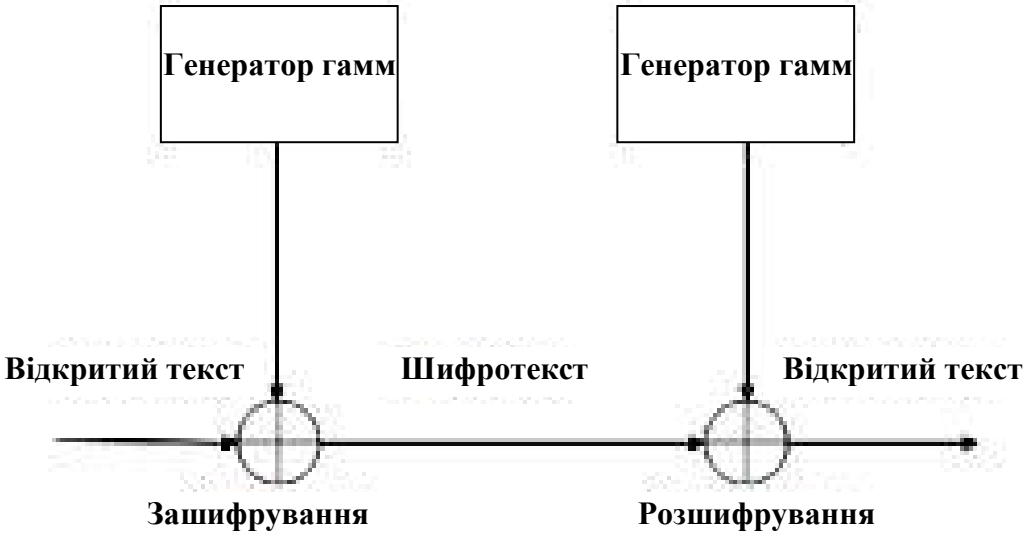


Рисунок 17.21 – Режим гамування для потокових шифрів

Алгоритм шифрування.

1. Функція генерує послідовність бітів (k_i).

2. Потім послідовність бітів за допомогою операції «додавання за модулем два» (xor) поєднується з відкритим текстом (m_i). В результаті виходить шифрограма (c_i):

$$c_i = m_i \oplus k_i$$

Алгоритм розшифрування.

1. Повторно створюється (регенерується) потік бітів ключа (ключовий потік) (k_i).

2. Потік бітів ключа складається із шифрограмою (c_i) Операцією «xor». В силу властивостей операції xor на виході виходить вихідний (незашифрований) текст (m_i):

$$m_i = c_i \oplus k_i = (m_i \oplus k_i) \oplus k_i$$

RC4 – фактично клас алгоритмів, що визначаються розміром блоку (надалі S-блоку). Параметр n є розміром слова алгоритму і визначає довжину *S-блока*. Зазвичай $n = 8$, але з метою аналізу можна зменшити його. Проте підвищення безпеки необхідно збільшити цю величину. У алгоритмі немає протиріч збільшення розміру *S-блока*. При збільшенні n, припустимо, до 16 біт, елементів у *S-блоці* стає 65536 і відповідно час початкової ітерації буде збільшено. Однак швидкість шифрування зросте.

Внутрішній стан RC4 представляється як масиву розміром 2^n і двох лічильників. Масив відомий як *S-блок* і далі буде позначатися як S. Він завжди містить перестановку 2^n можливих значень слова. Два лічильники позначені через *i* та *j*.

Ініціалізація RC4 складається із двох частин:

1. Ініціалізація *S-блоку*.
2. Генерація псевдовипадкового слова K.

Ініціалізація *S-блоку*

Алгоритм також відомий як «key-scheduling algorithm» або «KSA». Цей алгоритм використовує ключ, який подається на вхід користувачем, збережений в Key, і має довжину L байт. Ініціалізація починається із заповнення масиву S, далі цей масив перемішується шляхом перестановок, що визначаються ключем. Так як тільки одна дія виконується над S, то повинно виконуватися твердження, що S завжди містить один набір значень, який був наданий при початковій ініціалізації (*S[i]:=i*).

```
for i from 0 to 255
  S[i]:= i
endfor
j:= 0
for i from 0 to 255
  j: = (j + S [i] + Key [i mod L]) mod 256 // n = 8; 2 8 = 256
  поміняти місцями S[i] та S[j]
endfor
```

Генерація псевдовипадкового слова *K*

Ця частина алгоритму називається генератором псевдовипадкової послідовності (англ. ***p**sudo-**r**andom **g**eneration **a**lgorithm, PRGA*). Генератор ключового потоку RC4 переставляє значення, що зберігаються у S. В одному циклі RC4 визначається одне n-бітне слово K із ключового потоку. Надалі ключове слово буде складено за модулем два з вихідним текстом, який користувач хоче зашифрувати, та отримано зашифрований текст.

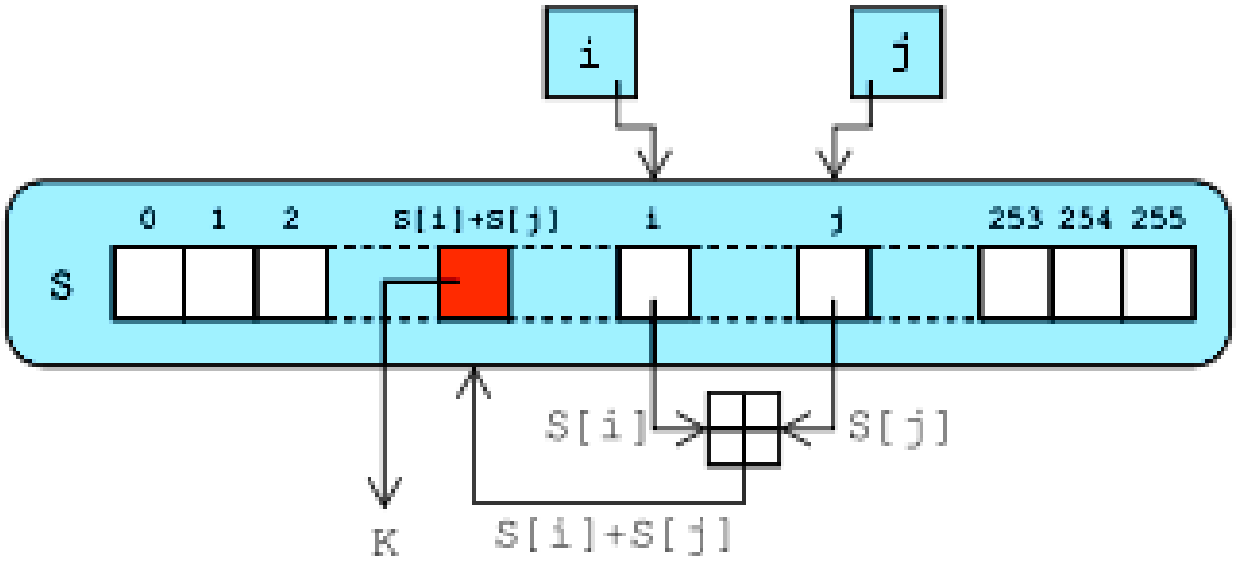


Рисунок 17.22 – Генератор ключового потоку RC4

i:= 0
j:= 0
while Цикл генерації:
  i:= (i + 1) mod 256
  j:= (j + S [i]) mod 256
  поміняти місцями S[i] та S[j]
  t:= (S[i] + S[j]) mod 256
  K:= S[t]
  згенеровано псевдовипадкове слово K (для *n* = 8 буде згенеровано один байт)
endwhile

Безпека

На відміну від сучасних шифрів (таких, як eSTREAM), RC4 не використовує nonce (від англ. *nonce* – Number that can only be used once – число, яке може бути використано один раз) поряд з ключем. Це означає, що якщо один ключ повинен використовуватися протягом тривалого часу для шифрування кількох потоків, сама криптосистема, що використовує RC4, повинна комбінувати наказ і довгостроковий ключ для отримання потокового ключа для RC4. Один з можливих виходів – генерувати **новий** ключ для RC4 за допомогою ґеш-функції від довгострокового ключа та nonce. Однак багато програм, що використовують RC4, просто конкатенують ключ і nonce. Через цей і слабкий розклад ключів, що використовується в RC4, додаток може стати вразливим. Тому він був визнаний застарілим багатьма софтверними компаніями, такими як Microsoft. Наприклад, у.NET Framework від Microsoft відсутня реалізація RC4.

Далі будуть розглянуті деякі атаки на шифр та методи захисту від них.

Дослідження Руза та відновлення ключа з перестановки

У 1995 році Андрю Руз (англ. *Andrew Roos*) експериментально поспостерігав, що перший байт ключового потоку корельований з першими трьома байтами ключа, а перші кілька байт перестановки після алгоритму розкладу ключів (англ. *KSA*) корельовані з деякою лінійною комбінацією байт. Ці усунення не були доведені до 2007 року, коли Пол, Рафі та Мейтре довели корелювання ключа та ключового потоку. Також Пол і Мейтре довели корелювання перестановки та ключа. Остання робота також використовує корелювання ключа та перестановки для того, щоб створити перший алгоритм повного відновлення ключа з останньої перестановки після KSA, не роблячи припущень про ключ і вектор ініціалізації (англ. *IV, **i**nitial **v**ector*). Цей алгоритм має постійну ймовірність успіху залежно від часу, що відповідає квадратному кореню зі складності повного перебору. Пізніше було зроблено багато робіт про відновлення ключа із внутрішнього стану RC4.

Атака Флурера, Мантіна та Шаміра (ФМШ)

У 2001 році Флурер, Мантін та Шамір опублікували роботу про вразливість ключового розкладу RC4. Вони показали, що перші байти ключового потоку серед усіх можливих ключів є невипадковими. З цих байтів можна з високою ймовірністю отримати інформацію про використовуваний шифр ключа. І якщо довготривалий ключ і nonce просто склеюються для створення ключа шифру RC4, цей довготривалий ключ може бути отриманий за допомогою аналізу досить великої кількості повідомлень, зашифрованих з використанням даного ключа. Ця вразливість та деякі пов'язані з нею ефекти були використані при зламі шифрування WEP у бездротових мережах стандарту IEEE 802.11. Це показало необхідність якнайшвидшої заміни WEP, що спричинило розробку нового стандарту безпеки бездротових мереж WPA.

Криптосистему можна зробити несприйнятливою до цієї атаки, якщо відкидати початок ключового потоку. Таким чином, модифікований алгоритм називається «RC4-drop[n]», де n кількість байтів з початку ключового потоку, які слід відкинути. Рекомендовано використовувати n = 768 консервативна оцінка становить n = 3072.

Атака базується на слабкості вектора ініціалізації. Знаючи перше псевдовипадкове слово K та m байтів вхідного ключа Key, використовуючи слабкість в алгоритмі генерації псевдовипадкового слова K, можна отримати m + 1 байт вхідного ключа. Повторюючи кроки, видобувається повний ключ. При атаці на WEP, n = 8 IV має вигляд (B; 255; N), де B – від 3 до 8, а N будь-яке число. Для визначення близько 60 варіантів *N* потрібно перехопити приблизно 4 мільйони пакетів.

Атака Кляйна

У 2005 році Андреас Кляйн представив аналіз шифру RC4, в якому він вказав на сильну корелювання ключа та ключового потоку RC4. Кляйн проаналізував атаки на першому раунді (подібні до атаки ФМШ), на другому раунді та можливі їх поліпшення. Він також запропонував деякі зміни алгоритму посилення стійкості шифру. Зокрема, він стверджує, що якщо змінити напрямок

циклу на зворотний в алгоритмі ключового розкладу, то можна зробити шифр більш стійким до атак типу ФМШ

Комбінаторна проблема

У 2001 році Аді Шамір та Іцхак Мантін першими поставили комбінаторну проблему, пов'язану з кількістю всіляких вхідних та вихідних даних шифру RC4. Якщо з різних 256 елементів внутрішнього стану шифру відомо хелементів зі стану ($x \leq 256$), то, якщо припустити, що інші елементи нульові, максимальна кількість елементів, які можуть бути отримані детермінованим алгоритмом за наступні 256 раундів, також дорівнює x. У 2004 році це припущення було доведено Сорадюті Полом (англ. *Souradyuti Paul*) і Бартом Пренелем (англ. *Bart Preneel*).

Атака Ванхофа та Пісенса (2015)

Влітку 2015 року Меті Ванхоф (Mathy Vanhoef) і Франк Пісенс (Frank Piessens) з університету Левена в Бельгії продемонстрували реальну атаку на протокол TLS, який використовує RC4 для шифрування даних. Ідея злому базується на принципі MITM. Вбудовавшись у канал передачі, атакуюча сторона генерує серверу велику кількість запитів, змушуючи їх у відповідь повертати куки, зашифровані одним і тим самим ключем. Маючи у розпорядженні близько $9x2^{27}$~2^{30} пар {відкритий текст, шифротекст}, атакуюча сторона отримала можливість на основі статистичних методів Флюрер-Макгрю та ABSAB з ймовірністю 94% відновити ключ і, отже, зашифровані куки. Практичні часові витрати становили близько 52 годин, верхня ж оцінка потрібного часу на момент демонстрації склала близько 72 годин.

STRUMOK (ДСТУ 8845:2019)

ДСТУ 8845:2019 Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного потокового перетворення

Зміст алгоритму

1 Сфера застосування
2 Нормативні посилання
3 Терміни та визначення понять
4 Познаки та скорочення
5 Загальні положення
5.1 Призначеність
5.2 Режими роботи
6 Моделі потокового шифру
7 Генератор ключових потоків СТРУМОК
7.1 Загальні параметри
7.2 Функція ініціалізації внутрішнього стану Init
7.3 Функція наступного стану Next
7.4 Функція ключового потоку Strm
7.5 Функція скінченного автомата CA
7.6 Функція нелінійної підстановки T
7.7 Множення на α в арифметиці поля GF (2^{64})

7.8 Множення на α^{-1} в арифметиці поля GF (2^{64})
7.9 Значення таблиць-констант Mul_{α} та $Mul_{\alpha^{-1}}$
Додаток А (довідковий) Додаткова інформація
Додаток Б (обов'язковий) Нелінійні таблиці підстановок π_0, π_1, π_2 та π_3
Додаток В (обов'язковий) Таблиці-константи $T_i[a]$, i = 0, 1, …, 7
Додаток Г (обов'язковий) Таблиці-константи $Mul_{\alpha}[a]$ та $Mul_{\alpha^{-1}}[a]$
Додаток Д (довідковий) Приклади для перевірення
Додаток Е (довідковий) Правила побудови таблиць Mul_{α} та $Mul_{\alpha^{-1}}$
Додаток Є (довідковий) Бібліографія

Сфера застосування

Цей стандарт установлює криптографічний алгоритм симетричного потокового перетворення для забезпечення конфіденційності та цілісності (як додаткової послуги) інформації під час її оброблення.

У стандарті описано алгоритм симетричного потокового криптографічного перетворення, який використовує ключовий потік для шифрування відкритого тексту побітово чи поблоково. Ключовий потік генерують лише із секретного ключа та вектора ініціалізації (синхропосилки), отже, стандарт визначає синхронний потоковий шифр (за класифікацією згідно з ДСТУ ISO/IEC 18033-4).

Стандарт використовують під час розроблення засобів криптографічного захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, а також у разі модернізації наявних систем для заміни потокових режимів згідно з ДСТУ ГОСТ 28147.

Для забезпечення конфіденційності та цілісності послідовностей двійкових символів можна застосовувати цей стандарт сумісно з ДСТУ ISO/IEC 18033-4 та ДСТУ 7564.

Нормативні посилання

У цьому стандарті є посилання на такі стандарти:

– ДСТУ 7564:2014 Інформаційні технології. Криптографічний захист інформації. Функція ґешування

– ДСТУ 7624:2014 Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення

– ДСТУ ГОСТ 28147:2009 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования (ГОСТ 28147–89, IDT)

– ДСТУ ISO/IEC 18033-4:2015 (ISO/IEC 18033-4:2011, IDT) Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 4. Потокові шифри.

Опис алгоритму

В основі алгоритму *Струмок* лежить класична схема підсумовуючого генератора, подібна генератору *SNOW-2.0*, який визначено в ISO/IEC 18033-4:2011. Алгоритм *Струмок* використовує 256-бітний вектор

ініціалізації *IV* та 256-бітний або 512-бітний секретний ключ *K* і забезпечує високий та надвисокий рівень стійкості із врахуванням можливого застосування квантового криптографічного аналізу. Криптоалгоритм орієнтований на 64-розрядні обчислювальні системи, отже розмір слова визначено рівним 64 бітам.

Основними структурними компонентами генератору є регістр зсуву з лінійним зворотнім зв'язком (linear feedback shift register, *LFSR*) та скінченний автомат (finite-state machine, *FSM*), в якому виконується нелінійне перетворення. Вхідні дані використовуються для ініціалізації змінної стану $Si\ (i \geq 0)$, яка складається з вісімнадцяти 64-бітових блоків, до складу яких входить дві компоненти:

– 16 змінних $s^{(i)}$ – комірок регістра зсуву з лінійним зворотнім зв'язком:

$$s^{(i)} = (s_{15}{}^{(i)}, s_{14}{}^{(i)}, ..., s_0{}^{(i)});$$

– два регістри скінченного автомату

$$r\ (^{i}): r^{(i)} = (r_2{}^{(i)}, r_1\ (^{i}).$$

На виході отримуємо ключовий потік (гаму шифру), який формується з 64-бітових слів Z_i. Схематичне зображення функціонування генератора ключових потоків *Струмок* в довільний момент часу *i* наведено на рис. 17.23. Змінну часової залежності *i* не наведено.

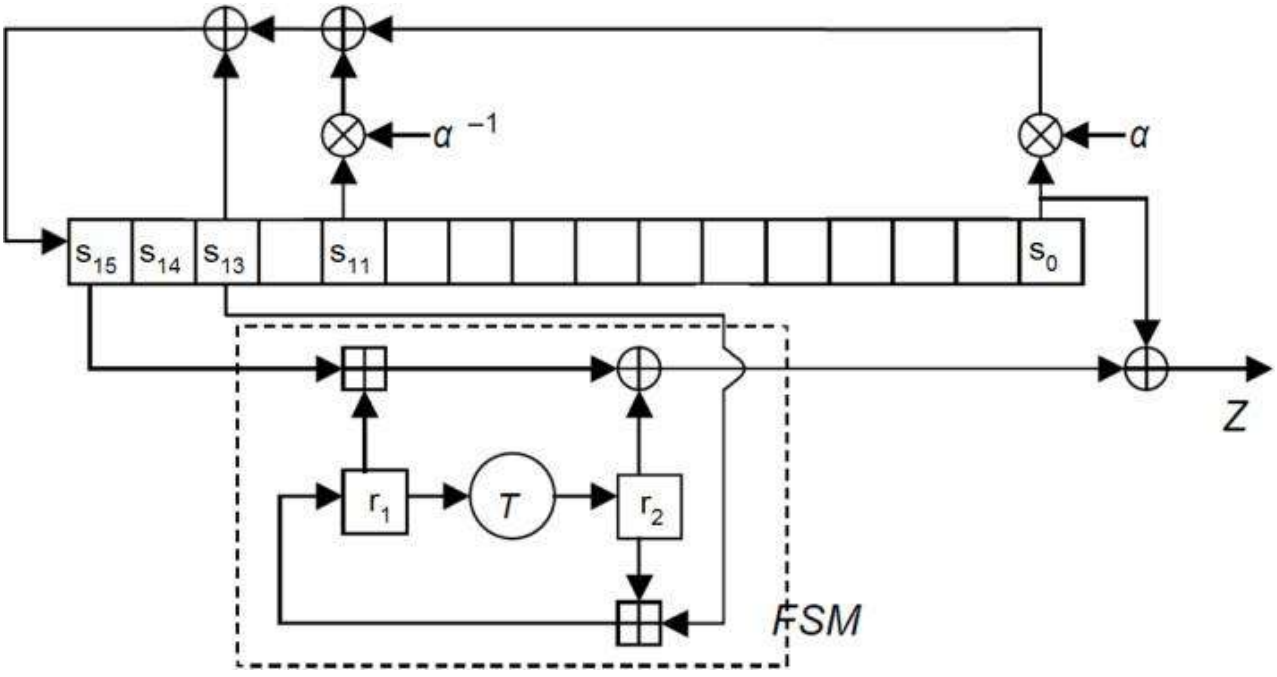


Рис. 17.23. Схематичне зображення генератору ключових потоків

Струмок у режимі генерації гами шифру (ключового потоку)

Відводи зворотного зв’язку у LFSR будується за примітивним над полем $GF\ (2^{64})$ поліномом:

$$f\ (x) = x^{16} + x^{13} + \alpha^{-1}x^{11} + \alpha,$$

де α є коренем примітивного над полем $GF\ (2^8)$ поліному:

$$g(z) = z^8 + \beta^{170}z^7 + \beta^{166}z^6 + \beta^2z^5 + \beta^{224}z^4 + \beta^{70}z^3 + \beta^2.$$

В свою чергу поле $GF(2^8)$ будується за примітивним над полем $GF(2)$ поліномом:

$$p(y) = y^8 + y^4 + y^3 + y^2 + 1,$$

а коефіцієнти поліному $g(z)$ подаються через ступінь примітивного елементу β поля $GF(2^8)$, тобто β – корінь поліному $p(y)$.

Таким чином, маємо вежу полів:

$$GF(2) \subset GF(2^8) \subset GF(2^{64}) \subset GF(2^{1024}),$$

де:

– поле $GF(2^{1024})$ задається відводами зворотного зв'язку LFSR як фактор кільце $GF(2^{64})[x] / (f(x))$,

– поле $GF(2^{64})$ задається як факторкільце $GF(2^8)[z] / (g(z))$,

– поле $GF(2^8)$ задається як факторкільце $GF(2)[y]/ (p(y))$.

Отже період вихідної послідовності *LFSR* є максимальним і дорівнює 2^{1024}-1.

Структурно в алгоритмі *Струмок* можна виділити три основні функції:

– функція ініціалізації *Init*, яка приймає в якості вхідних даних ключ *K* (256 біт або 512 біта) і вектор ініціалізації *IV* (256 біт), і виробляє початкове значення змінної стану:

$$S_0 = (s^{(0)}, r^{(0)});$$

– функція наступного стану *Next*, яка приймає на вхід змінну стану:

$$S_i = (s^{(i)}, r^{(i)})$$

і виробляє наступне значення змінної стану

$$S_{i+1} = (s^{(i+1)}, r^{(i+1)}).$$

Функція *Next* може виконуватися в двох режимах, в залежності від способу виконання ітерації – як частини реалізації або як частини нормального режиму генерації вихідних даних;

– функція ключового потоку *Strm*, що приймає на вході i змінну стану $S_i = (s^{(i)}, r^{(i)})$ і виробляє на виході 64-бітний ключовий потік Z_i.

Функція ініціалізації внутрішнього стану *Init*

Функція ініціалізації внутрішнього стану *Init* описується наступним чином.

Вхід: 256 або 512-бітний ключ *K*, 256-бітний вектор ініціалізації *IV*. *Вихід*: початкове значення змінної стану $S_0 = (s^{(0)}, r^{(0)})$.

Ключ для версії потокового шифру *Струмок-256* можна представити у вигляді чотирьох 64-бітних слів:

$$K = (K_3, K_2, K_1, K_0),$$

а для 512-бітного ключа – у вигляді восьми 64-бітних слів

$$K = (K_7, K_6, K_5, K_4, K_3, K_2, K_1, K_0),$$

де K_3 та K_7, відповідно для 256 и 512 біт, найбільш значущі слова, а K_0 – найменш значущі.

Вектор ініціалізації можна представити у вигляді чотирьох 64-бітних слів

$$IV = (IV_3, IV_2, IV_1, IV_0),$$

де IV_3 – найбільш значуще слово, а IV_0 – найменш значуще.

1. В 16 комірок LFSR заноситься значення ключа.

Для версії з 256-бітним ключем виконуються операції:

$$s_{15}^{(-33)} = \neg K_0,\ s_{14}^{(-33)} = K_1,\ s_{13}^{(-33)} = \neg K_2,\ s_{12}^{(-33)} = K_3,\ s_{11}^{(-33)} = K_0,\ s_{10}^{(-33)} = \neg K_1,\ s_9^{(-33)} = K_2,\ s_8^{(-33)} = K_3,$$
$$s_7^{(-33)} = \neg K_0,\ s_6^{(-33)} = \neg K_1,\ s_5^{(-33)} = K_2 \oplus IV_3,\ s_4^{(-33)} = K_3,\ s_3^{(-33)} = K_0 \oplus IV_2,\ s_2^{(-33)} = K_1 \oplus IV_1,$$
$$s_1^{(-33)} = K_2,\ s_0^{(-33)} = K_3 \oplus IV_0.$$

Для версії з 512-бітним ключем K виконуються операції:

$$s_{15}^{(-33)} = K_0,\ s_{14}^{(-33)} = \neg K_1,\ s_{13}^{(-33)} = K_2,\ s_{12}^{(-33)} = K_3,\ s_{11}^{(-33)} = \neg K_7,\ s_{10}^{(-33)} = K_5,\ s_9^{(-33)} = \neg K_6,$$
$$s_8^{(-33)} = K_4 \oplus IV_3,\ s_7^{(-33)} = \neg K_0,\ s_6^{(-33)} = K_1,\ s_5^{(-33)} = K_2 \oplus IV_2,\ s_4^{(-33)} = K_3,\ s_3^{(-33)} = K_4 \oplus IV_1,$$
$$s_2^{(-33)} = K_5,\ s_1^{(-33)} = K_6,\ s_0^{(-33)} = K_7 \oplus IV_0.$$

2. Виконуються 32 ініціюючих такти без генерації ключового потоку, тобто чотири пов них циклів. Формально це подається наступним чином:

$$S_{-1} = Next^{32}(S_{-33}, INIT),$$

що означає 32 ітерації з виконання функції *Next* у режимі ініціалізації *INIT*, $S_{-33} = (s^{(-33)}, r^{(-33)})$ – обраховані на попередньому кроці значення змінної стану.

3. Розраховується початкове значення змінної стану $S_0 = (s^{(0)}, r^{(0)})$ за правилом: $S_0 = Next\,(S_{-1})$, тобто шляхом виконання функції *Next* у звичайному режимі.

4. Виводиться вихідне значення $S_0 = (s^{(0)}, r^{(0)})$.

Функція наступного стану *Next*

Функція стану *Next* описується наступним чином.

Вхід: Змінна стану $S_i = (s^{(i)}, r^{(i)})$, обраний режим (звичайний, або режим ініціалізації).

Вихід: Наступне значення змінної стану $S_{i+1} = (s^{(i+1)}, r^{(i+1)})$.

1. Виконується нелінійна підстановка для оновлення значення регістру $r_2^{(i+1)}$ скінченного автомату. Для цього розраховується значення функції T: $r_2^{(i+1)} = T\,(r_1^{(i)})$.

2. Оновлюється значення регістру значення $r_1^{(i+1)}$ скінченного автомату. Для цього розраховується значення:

$$r_1^{(i+1)} = r_2^{(i+1)} +_{64} s_{13}^{(i)},$$

де $+_{64}$ позначає операцію додавання цілих чисел за модулем 2^{64} (у схемі шифру на рис. 17.23 цю операцію позначено як ⊞).

3. Оновлюється значення 15 комірок *LFSR*

$$s_j^{(i+1)} = s_{j+1}^{(i)}$$

для всіх $j = 0, 1, \ldots, 14$.

4. Оновлюється значення 16-ї комірки *LFSR*. Якщо встановлено звичайний режим функції *Next*, значення цієї комірки обчислюється за правилом:

$$s_{15}^{(i+1)} = (s_0^{(i)} \otimes \alpha) \oplus (s_{11}^{(i)} \otimes \alpha^{-1}) \oplus s_{13}^{(i)}.$$

Якщо встановлено режим ініціалізації *INIT* функції *Next*, значення обчислюється за правилом:

$$s_{15}^{(i+1)} = FSM(s_{15}^{(i)}, r_1^{(i)}, r_2^{(i)}) \oplus (s_0^{(i)} \otimes \alpha) \oplus (s_{11}^{(i)} \otimes \alpha^{-1}) \oplus s_{13}^{(i)}.$$

Операції множення $\otimes$ на α та на α^{-1} та сутність функції *FSM* пояснюються далі.

5. Обчислюється та виводиться значення змінної стану $S = (s^{(i)}, r^{(i)})$.

Схематичне зображення генератору ключових потоків *Струмок* при виконанні функції *Next* у режимі ініціалізації представлено на рис. 17.24.

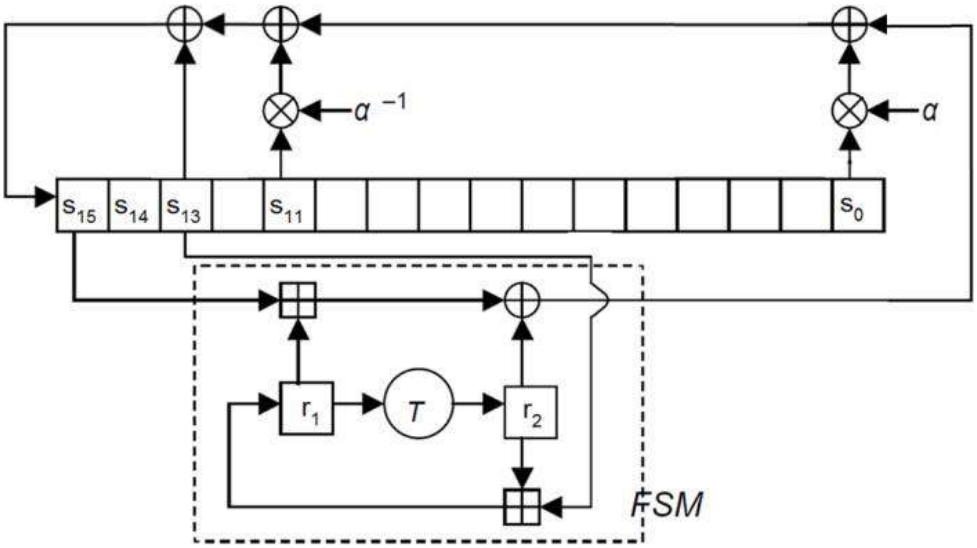


Рис. 17.24. Схематичне зображення генератору ключових потоків Струмок у режимі ініціалізації функції *Next*

Функція ключового потоку *Strm*

Функція ключового потоку *Strm* описується наступним чином.

Вхід: Змінна стану $S_i = (s^{(i)}, r^{(i)})$.

Вихід: 64-бітовий ключовий потік

1. Обчислюється значення

$$Z_i = FSM(s_{15}^{(i)}, r_1^{(i)}, r_2^{(i)}) \oplus s_0^{(i)}.$$

2. Виводиться вихідне значення *Zi*.

Функція скінченного автомату *FSM*

Функція скінченного автомату позначається як *FSM* (*x*, *y*, *z*) та описується наступним чином.

Вхід: три 64-бітових рядка *x*, *y* і *z*. *Вихід*: 64-бітовий рядок *q*.

1. Обчислюється значення $q = (x +_{64} y) \oplus z$.

2. Виводиться вихідне значення *q*.

Функція нелінійної підстановки *T*

Функція нелінійної підстановки *T* реалізує перестановку елементів скінченного поля *GF* (2^{64}) за допомогою компонентів національного стандарту блокового симетричного криптоперетворення ДСТУ 7624:2014.

Вхід: 64-бітовий рядок *w*.

Вихід: 64-бітовий рядок $T = T(w)$.

1. Вхідний 64-бітовий рядок *w* розбивається на підблоки w_j по 8 біт:

$$w = (w_7, w_6, w_5, w_4, w_3, w_2, w_1, w_0),$$

2. Для кожного підблоку w_j виконується підстановка з алгоритму ДСТУ 7624:2014 за допомогою чотирьох табличних перетворень π_0, π_1, π_2, π_3 (див. додаток Б). Виконання функції T за допомогою цих перетворень схематично (на прикладі підблоків w_j, що подано у шіснадцятковому вигляді)

зображено на рис. 17.25.

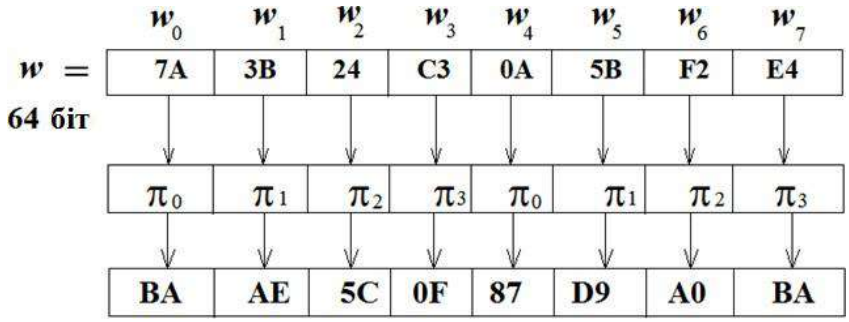


Рис. 17.25. Схематичне зображення виконання процедури підстановки $T = T(w)$

У результаті формується вихідний вектор $r = (r_7, r_6, r_5, r_4, r_3, r_2, r_1, r_0)$:

$$r_j = \pi_{j \bmod 4}\left[w_j\right],$$

де $j = 0, 1, \ldots, 7$.

3. Обчислюється вектор

$$q = (q_7, q_6, q_5, q_4, q_3, q_2, q_1, q_0)$$

за правилом:

$$\begin{pmatrix} q_0 \\ q_1 \\ q_2 \\ q_3 \\ q_4 \\ q_5 \\ q_6 \\ q_7 \end{pmatrix} = \begin{pmatrix} 01 & 01 & 05 & 01 & 08 & 06 & 07 & 04 \\ 04 & 01 & 01 & 05 & 01 & 08 & 06 & 07 \\ 07 & 04 & 01 & 01 & 05 & 01 & 08 & 06 \\ 06 & 07 & 04 & 01 & 01 & 05 & 01 & 08 \\ 08 & 06 & 07 & 04 & 01 & 01 & 05 & 01 \\ 01 & 08 & 06 & 07 & 04 & 01 & 01 & 05 \\ 05 & 01 & 08 & 06 & 07 & 04 & 01 & 01 \\ 01 & 05 & 01 & 08 & 06 & 07 & 04 & 01 \end{pmatrix} \cdot \begin{pmatrix} r_0 \\ r_1 \\ r_2 \\ r_3 \\ r_4 \\ r_5 \\ r_6 \\ r_7 \end{pmatrix},$$

де елементи матриці (подано у шістнадцятковому вигляді) та векторів r і q інтерпретуються як елементи скінченного поля $GF(2^8)$, яке задане як факторкільце $GF(2)[y]/(p(y))$.

Цю операцію можна записати у скороченому вигляді (як у ДСТУ 7624:2014):

$$q_i = (\upsilon >>> i) r^T,$$

де $\upsilon = (01, 01, 05, 01, 08, 06, 07, 04)$, $>>> i$ – операція циклічного зсуву на i розрядів праворуч, $i = 0,1,..., 7$,

$$r^T = (r_0, r_1, r_2, r_3, r_4, r_5, r_6, r_7)^T.$$

4. Виводиться вихідне значення q, яке інтерпретується як 64-бітовий рядок. Швидке обчислення вектору $(q_0, q_1, q_2, q_3, q_4, q_5, q_6, q_7) = Q$ реалізується за правилом

$$Q^T = T_0[w_0] \oplus T_1[w_1] \oplus T_2[w_2] \oplus T_3[w_3] \oplus T_4[w_4] \oplus T_5[w_5] \oplus T_6[w_6] \oplus T_7[w_7],$$

де

$$T_0[a] = \begin{pmatrix} 01 \\ 04 \\ 07 \\ 06 \\ 08 \\ 01 \\ 05 \\ 01 \end{pmatrix} \cdot \pi_0[a],\ T_1[a] = \begin{pmatrix} 01 \\ 01 \\ 04 \\ 07 \\ 06 \\ 08 \\ 01 \\ 05 \end{pmatrix} \cdot \pi_1[a],\ T_2[a] = \begin{pmatrix} 05 \\ 01 \\ 01 \\ 04 \\ 07 \\ 06 \\ 08 \\ 01 \end{pmatrix} \cdot \pi_2[a],\ T_3[a] = \begin{pmatrix} 01 \\ 05 \\ 01 \\ 01 \\ 04 \\ 07 \\ 06 \\ 08 \end{pmatrix} \cdot \pi_3[a],$$

$$T_4[a] = \begin{pmatrix} 08 \\ 01 \\ 05 \\ 01 \\ 01 \\ 04 \\ 07 \\ 06 \end{pmatrix} \cdot \pi_0[a],\ T_5[a] = \begin{pmatrix} 06 \\ 08 \\ 01 \\ 05 \\ 01 \\ 01 \\ 04 \\ 07 \end{pmatrix} \cdot \pi_1[a],\ T_6[a] = \begin{pmatrix} 07 \\ 06 \\ 08 \\ 01 \\ 05 \\ 01 \\ 01 \\ 04 \end{pmatrix} \cdot \pi_2[a],\ T_7[a] = \begin{pmatrix} 04 \\ 07 \\ 06 \\ 08 \\ 01 \\ 05 \\ 01 \\ 01 \end{pmatrix} \cdot \pi_3[a].$$

Застосування таблиць-констант T_i $[a]$, $i = 0,1,..., 7$ дозволяє значно зменшити кількість операцій, зокрема функція нелінійної підстановки обчислюється за сім операцій XOR над 64-бітовими рядками.

Множення на α в арифметиці поля *GF* (2^{64})

Множення на α в арифметиці поля *GF* (2^{64}) реалізується за допомогою таблиці передобчислень Mul_α з 256 рядків по 64 бітів в кожному.

Вхід: 64-бітовий рядок *w*, що представляє елемент поля *GF* (2^{64}).

Вихід: 64-бітовий рядок $w' = w \otimes \alpha$, що представляє елемент поля *GF* (2^{64}).

1. Обчислюється значення

$$w' = (w << 8) \oplus Mul_\alpha[w >> 56], \qquad (17.1)$$

де *w* << 8 є результатом зсуву ліворуч (в бік старших розрядів) 64-бітового рядка *w* на вісім розрядів із заповненням молодших розрядів нульовими значеннями;

w >> 56 є результатом зсуву праворуч (в бік молодших розрядів) 64-бітового рядка *w* на 56 розрядів із заповненням старших розрядів нульовими значеннями. Вісім молодших розрядів вектору *w* >> 56 інтерпретуються як елемент поля *GF* (2^8) для індексації таблиці передобчислень Mul_α;

Mul_α – таблиця-константа з 256 рядків по 64 біта в кожному (таблиця передобчислень);

$Mul_\alpha[c]$ – 64-бітне значення таблиці передобчислень у рядку з індексом *c*, де *c* представляє елемент поля *GF* (2^8), $Mul_\alpha[c]$ представляє елемент поля *GF* (2^{64}).

2. Виводиться вихідне значення *w*'.

Множення на α^{-1} в арифметиці поля *GF* (2^{64})

Множення на α^{-1} в арифметиці поля *GF* (2^{64}) реалізується за допомогою таблиці перед обчислень $Mul_{\alpha^{-1}}$ з 256 рядків по 64 бітів в кожному.

Вхід: 64-бітовий рядок *w*, що представляє елемент поля *GF* (2^{64}).

Вихід: 64-бітовий рядок $w' = w \otimes \alpha^{-1}$, що представляє елемент поля *GF* (2^{64}).

1. Обчислюється значення

$$w' = (w >> 8) \oplus Mul_{\alpha^{-1}}[w \,\&\, \gamma], \tag{17.2}$$

де:

w >> 8 є результатом зсуву праворуч (в бік молодших розрядів) 64-бітового рядка *w* на 8 розрядів із заповненням старших розрядів нульовими значеннями;

w & γ є результатом побітової кон'юнкції 64-бітового рядка *w* та 64-бітового рядка γ, який у шістнадцятковому поданні має вигляд γ = 00000000000000FF. Вісім молодших розрядів вектору *w* & γ інтерпретуються як елемент поля *GF* (2^8) для індексації таблиці перед обчислень $Mul_{\alpha^{-1}}$;

2. Виводиться вихідне значення *w*'.

Значення таблиць-констант Mul_{α}, $Mul_{\alpha^{-1}}$

Для швидкого шифрування застосовуються таблиці передобчислень Mul_{α}, $Mul_{\alpha^{-1}}$, Це дозволяє значно зменшити кількість операцій для обробки блоку вхідних даних.

Поліном, що задає зворотний зв'язок LFSR має вигляд:

$$f(x) = x^{16} + x^{13} + \alpha^{-1}x^{11} + \alpha,$$

де α та α^{-1} належать полю *GF* (2^{64}), причому $\alpha = z$ є коренем примітивного над полем *GF* (2^8) поліному *g* (*z*). Таким чином, у кожній комірці LFSR зберігається 64-бітна послідовність *w*, яку представимо у вигляді восьми підблоків w_j по вісім біт у кожному:

$$w = (w_7, w_6, w_5, w_4, w_3, w_2, w_1, w_0),$$

які інтерпретуються як коефіцієнти поліному

$$w(z) \in GF(2^8)[z] / (g(z)).$$

Якщо $\alpha = z$ є коренем примітивного над *GF* (2^8) поліному:

$$g(z) = z^8 + g_7 z^7 + \ldots + g_1 z + g_0$$

тоді маємо:

$$w(z) \cdot \alpha = (w_7 z^8 + w_6 z^7 + \ldots + w_1 z^2 + w_0 z) \bmod g(z) \equiv$$
$$\equiv (w_6 + w_7 g_7) z^7 + (w_5 + w_7 g_6) z^6 + \ldots + (w_0 + w_7 g_1) z + (w_7 g_0) z^0 =$$
$$= w_{<<8}(z) + w_{>>56}(z) \cdot g'(z),$$

де поліноми

$$w_{<<8}(z),\ w_{>>56}(z) \text{ та } g'(z)$$

мають вигляд:

$$w_{<<8}(z) = w_6 z^7 + w_5 z^6 + \ldots + w_0 z,$$

$$w_{>>56}(z) = w_7,$$

$$g'(z) = g_7 z^7 + g_6 z^6 + \ldots + g_1 z + g_0.$$

Двійкове подання коефіцієнтів поліномів

$$w_{<<8}(z) \quad \text{і} \quad w_{>>56}(z)$$

утворює розглянуті у (17.1) двійкові послідовності $w << 8$ і $w >> 56$. Отже, обчислення $w(z)\cdot\alpha$ в арифметиці поля $GF(2^{64})$ відповідає формулі (17.1), де 256 значень таблиці $Mul_\alpha[w_7]$ розраховуються як 64-бітні послідовності при двійковому поданні коефіцієнтів (w_7g_7, w_7g_6,..., w_7g_1, w_7g_0) поліному:

$$w_{>>56}(z)\cdot g'(z) = w_7(g_7 z^7 + g_6 z^6 + \ldots + g_1 z + g_0)$$

для кожного з 256 можливих значень $w_7 \in GF(2^8)$.

Якщо $\alpha = z$ є коренем примітивного над $GF(2^8)$ поліному

$$g(z) = z^8 + g_7 z^7 + \ldots + g_1 z + g_0,$$

тоді маємо:

$$\alpha^8 = g_7\alpha^7 + \ldots + g_1\alpha + g_0\alpha^0,$$

або

$$\alpha^7 = g_7\alpha^6 + \ldots + g_1\alpha^0 + g_0\alpha^{-1},$$

отже

$$g_0^{-1}\alpha^7 + g_0^{-1}g_7\alpha^6 + \ldots + g_0^{-1}g_1\alpha^0 = \alpha^{-1} = z^{-1}.$$

Тоді

$$w(z)\alpha^{-1} = w_7 z^6 + w_6 z^5 + \ldots + w_1 z^0 + w_0 z^{-1} =$$
$$w_7 z^6 + w_6 z^5 + \ldots + w_1 z^0 + w_0(g_0^{-1}z^7 + g_0^{-1}g_7 z^6 + \ldots + g_0^{-1}g_1 z^0) =$$
$$= (w_0 g_0^{-1})z^7 + (w_7 + w_0 g_0^{-1} g_7)z^6 + \ldots + (w_1 + w_0 g_0^{-1} g_1)z^0 =$$
$$= w_{>>8}(z) + w_0(z)\cdot g''(z),$$

де поліноми $w_{>>8}(z)$, $w_0(z)$ **та** $g''(z)$ **мають вигляд:**

$$w_{>>8}(z) = w_7 z^6 + w_6 z^5 + \ldots + w_2 z + w_1,$$

$$w_0(z) = w_0,$$

$$g''(z) = g_0^{-1}z^7 + g_0^{-1}g_7 z^6 + \ldots + g_0^{-1}g_2 z + g_0^{-1}g_1.$$

Двійкове подання коефіцієнтів поліномів

$$w_{>>8}(z) \quad \text{і} \quad w_0(z)$$

утворює розглянуті у (17.2) двійкові послідовності $w >> 8$ і γ. Таким чином, обчислення $w(z)\cdot\alpha^{-1}$ в арифметиці поля $GF(2^{64})$ відповідає формулі (17.2), де 256 значень таблиці $Mul_{\alpha^{-1}}[w]$ розраховуються як 64-бітні послідовності при двійковому поданні коефіцієнтів:
$(w_0 g_0^{-1}, w_0 g_0^{-1} g_7, \ldots, w_0 g_0^{-1} g_2, w_0 g_0^{-1} g_1)$ **поліному**

$$w_0(z)\cdot g''(z) = w_0(g_0^{-1}z^7 + g_0^{-1}g_7 z^6 + \ldots + g_0^{-1}g_2 z + g_0^{-1}g_1)$$

для кожного з 256 можливих значень $w \in GF(2^8)$.

Висновки

Генератор ключових потоків *Струмок* дозволяє формувати псевдовипадкові послідовності із швидкістю понад 10 Гбіт/с. За цим показником він випереджає майже всі найбільш поширені шифри, зокрема і алгоритм *SNOW2.0*.

Генератор ключового потоку *Струмок* у своїй концептуальній схемі подібний до SNOW2.0. Але розробники SNOW2.0 зосереджувалися на використанні 32-розрядних обчислювальних систем, тоді як *Струмок* призначений для використання в більш потужних 64-розрядних обчислювальних системах. У зв'язку з цим в алгоритмі *Струмок* підвищується швидкість формування псевдовипадкової послідовності, що використовується 64-розрядними словами, для зберігання потоку ключів шифрування. Проведені порівняльні тести показали, що алгоритм *Струмок* на 32-розрядних обчислювальних системах також демонструє хороші результати роботи. Використання попереднього обчислення збільшує швидкість алгоритму, оскільки в процесі генерації ключові потоку немає необхідності в складних калькуляціях. В алгоритмі *Струмок* збільшені, в порівнянні з *SNOW2.0*, довжини секретного ключа та вектору ініціалізації. Це дозволяє надійно застосовувати потоковий шифр навіть з із врахуванням квантових методів криптографічного аналізу.

Розділ 18. Несиметрична (асиметрична, з відкритим ключем) криптографія

18.1. Модель асиметричної криптосистеми.
18.2. Шифр RSA.
18.3. Алгоритм Ель-Гамаля (EG).
18.4. Генерація спільних секретів Діффі-Хеллмана (DH).
18.5. Електронний цифровий підпис DSA.
18.6. Криптографія на еліптичних кривих.
18.7. Електронний цифровий підпис згідно ДСТУ 4145-2002.
18.8. EC-DSA згідно ISO/IEC 15946-2.

18.1. Модель асиметричної криптосистеми

Основні вимоги до алгоритмів асиметричного шифрування

Несиметрична (асиметрична, з відкритим ключем) криптографія – це така криптографія у алгоритмах якої ключ шифрування не дорівнює ключу дешифрування. Створення ***алгоритмів асиметричного шифрування*** є найбільшим і, можливо, єдиним революційним досягненням в історії криптографії. Алгоритми шифрування з ***відкритим ключем*** розроблялися для того, щоб вирішити дві найбільш важкі задачі, що виникли при використанні симетричного шифрування.

Першою задачею є розподіл ключа. При симетричному шифруванні потрібно, щоб обидві сторони вже мали загальний ключ, що якимось образом повинен бути їм заздалегідь переданий. Діффі, один з основоположників шифрування з ***відкритим ключем***, помітив, що ця вимога заперечує всю суть криптографії, а саме можливість підтримувати загальну таємність при комунікаціях.

Другою задачею є необхідність створення таких механізмів, при використанні яких неможливо було б підмінити кого-небудь із учасників, тобто потрібен ***цифровий підпис***. При використанні комунікацій для рішення широкого кола задач, наприклад у комерційній і приватній цілях, електронні повідомлення й документи повинні мати еквівалент підпису, що втримується в паперових документах. Необхідно створити метод, при використанні якого всі учасники будуть переконані, що електронне повідомлення було послано конкретним учасником. Це більше сильна вимога, ніж автентифікація.

Діффі й Хеллман досягли значних результатів, запропонувавши спосіб рішення обох задач, що радикально відрізняється від всіх попередніх підходів до шифрування.

Спочатку розглянемо **загальні риси алгоритмів шифрування з *відкритим ключем* і вимоги до цих алгоритмів**. Визначимо вимоги, яким повинен відповідати алгоритм, що використовує один ключ для шифрування, інший ключ – для дешифрування, і при цьому розрахунково неможливо визначити ключ, що дешифрує, знаючи тільки алгоритм шифрування й ключ, що

шифрує. Крім того, деякі алгоритми, наприклад RSA, мають наступну характеристику: кожний із двох ключів може використовуватися як для шифрування, так і для дешифрування.

Спочатку розглянемо алгоритми, що володіють обома характеристиками, а потім перейдемо до алгоритмів *відкритого ключа*, які не мають другу властивість.

При описі симетричного шифрування й шифрування з *відкритим ключем* будемо використовувати наступну термінологію. Ключ, використовуваний у симетричному шифруванні, будемо називати ***секретним ключем***. Два ключі, використовувані при шифруванні з *відкритим ключем*, будемо називати ***відкритим ключем*** і ***закритим ключем***. *Закритий ключ* тримається в секреті, але називати його будемо *закритим ключем*, а не секретним, щоб уникнути плутанини із ключем, використовуваним у симетричному шифруванні. *Закритий ключ* будемо позначати KR, *відкритий ключ* – KU.

Будемо припускати, що всі учасники мають доступ до *відкритих ключів* один одного, а *закриті ключі* створюються локально кожним учасником і, отже, розподілятися не повинні.

У будь-який час учасник може змінити свій *закритий ключ* і опублікувати складової пари *відкритий ключ*, замінивши їм старий *відкритий ключ*.

Діффі й Хеллман описують вимоги, яким повинен задовольняти алгоритм шифрування з *відкритим ключем*.

1. Розрахунково легко створювати пари (*відкритий ключ* KU, *закритий ключ* KR).
2. Розрахунково легко, маючи *відкритий ключ* і незашифроване повідомлення M, створити відповідне зашифроване повідомлення:

$$C = E_{KU}[M]$$

3. Розрахунково легко дешифрувати повідомлення, використовуючи *закритий ключ*:

$$M = D_{KR}[C] = D_{KR}[E_{KU}[M]]$$

4. Розрахунково неможливо, знаючи *відкритий ключ* KU, визначити *закритий ключ* KR.
5. Розрахунково неможливо, знаючи *відкритий ключ* KU і зашифроване повідомлення C, відновити вихідне повідомлення M.

Можна додати шосту вимогу, хоча воно не виконується для всіх алгоритмів з *відкритим ключем*:

6. Функції, що шифрують і дешифрують можуть застосовуватися в будь-якому порядку:

$$M = E_{KU}[D_{KR}[M]]$$

Це досить сильні вимоги, які вводять поняття *однобічної функції з люком*. ***Однобічною функцією*** називається така функція, у якої кожний аргумент має єдине зворотне значення, при цьому обчислити саму функцію легко, а обчислити зворотну функцію функцію функцію важко.

$$Y = f(X) \text{ – легко}$$

$$X = f^{-1}(Y) \text{ – важко}$$

Звичайно "легко" означає, що проблема може бути вирішена за поліноміальний час від довжини входу. Таким чином, якщо довжина входу має n біт, той час обчислення функції пропорційно n^a, де a – фіксована константа. Таким чином, говорять, що алгоритм належить класу поліноміальних алгоритмів P. Термін "важко" означає більше складне поняття. У загальному випадку будемо вважати, що проблему вирішити неможливо, якщо зусилля для її рішення більше поліноміального часу від величини входу. Наприклад, якщо довжина входу n біт, і час обчислення функції пропорційно 2^n, те це вважається розрахунково неможливою задачею. На жаль, важко визначити, чи проявляє конкретний алгоритм таку складність. Більше того, традиційні подання про обчислювальну складність фокусуються на гіршому випадку або на середньому випадку складності алгоритму. Це неприйнятно для криптографії, де потрібна неможливість інвертувати функцію для всіх або майже всіх значень входів.

Повернемося до визначення ***однобічної функції з люком***, що, подібно *однобічної функції*, легко обчислити в одному напрямку й важко обчислити у зворотному напрямку доти, поки недоступно деяку додаткову інформацію. При наявності цієї додаткової інформації інверсію можна обчислити за поліноміальний час. Таким чином, *однобічна функція* з люком належить сімейству *однобічних функцій* f_k таких, що

$Y = f_k(X)$ – легко, якщо k і X відомі

$X = f_k^{-1}(Y)$ – легко, якщо k і Y відомі

$X = f_k^{-1}(Y)$ – важко, якщо Y відомо, але k невідомо

Ми бачимо, що розробка конкретного алгоритму з *відкритим ключем* залежить від відкриття відповідної однобічної функції з люком.

Основні способи використання алгоритмів з відкритим ключем

Основними способами використання алгоритмів з *відкритим ключем* є шифрування/дешифрування, створення й перевірка підпису й обмін ключа.

Шифрування з *відкритим ключем* складається з наступних кроків:

1. Користувач B створює пари ключів KU_b і KR_b, використовуваних для шифрування й дешифрування переданих повідомлень.
2. Користувач B робить доступним деяким надійним способом свій ключ шифрування, тобто *відкритий ключ* KU_b. Складової пари *закритий ключ* KR_b тримається в секреті.
3. Якщо A хоче послати повідомлення B, він шифрує повідомлення, використовуючи *відкритий ключ* B KU_b.
4. Коли B одержує повідомлення, він дешифрує його, використовуючи свій *закритий ключ* KR_b. Ніхто іншої не зможе дешифрувати повідомлення, тому що цей *закритий ключ* знає тільки B.

Якщо користувач (кінцева система) надійно зберігає свій *закритий ключ*, ніхто не зможе підглянути передані повідомлення.

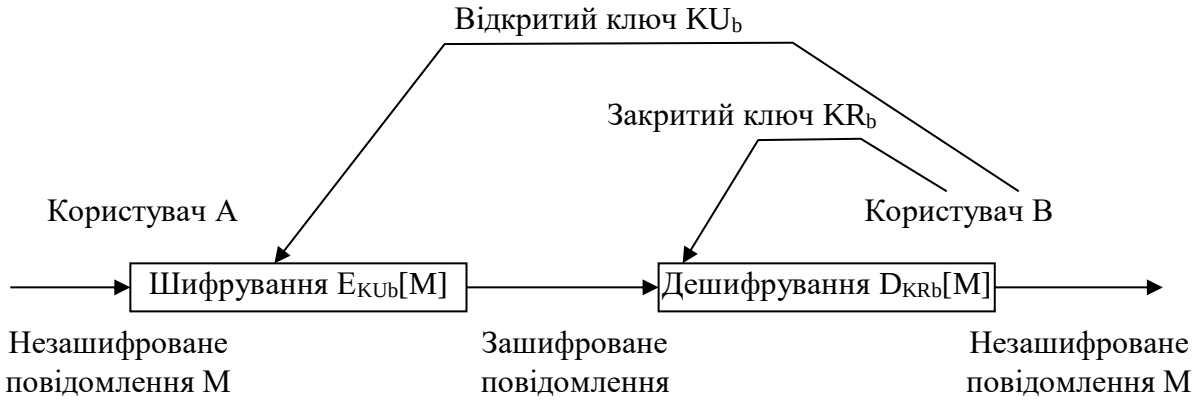


Рисунок 18.1 – Шифрування з відкритим ключем

Створення й перевірка підпису складається з наступних кроків:

1. Користувач А створює пари ключів KR_A і KU_A, використовуваних для створення й перевірки підпису переданих повідомлень.
2. Користувач А робить доступним деяким надійним способом свій ключ перевірки, тобто *відкритий ключ* KU_A. Складової пари *закритий ключ* KR_A тримається в секреті.
3. Якщо А хоче послати підписане повідомлення В, він створює підпис $E_{KRa}[M]$ для цього повідомлення, використовуючи свій *закритий ключ* KR_A.
4. Коли В одержує підписане повідомлення, він перевіряє підпис $D_{KUa}[M]$, використовуючи *відкритий ключ* А KU_A. Ніхто інший не може підписати повідомлення, тому що цей *закритий ключ* знає тільки А.

Доти, поки користувач або прикладна система надійно зберігає свій *закритий ключ*, їхні підписи достовірні.

Крім того, неможливо змінити повідомлення, не маючи доступу до *закритого ключа* А; тим самим забезпечується автентифікация й цілісність даних.

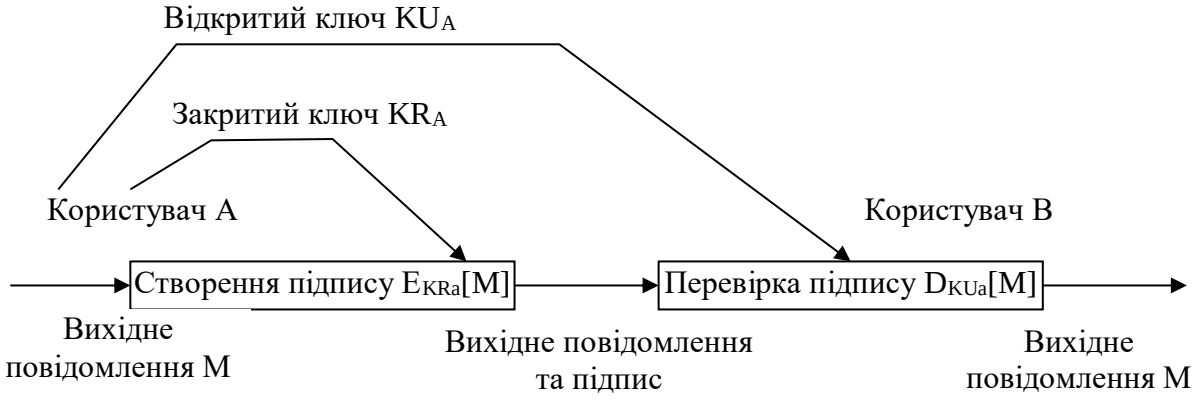


Рисунок 18.2 – Створення й перевірка підпису

У цій схемі все повідомлення підписується, причому для підтвердження цілісності повідомлення потрібно багато пам'яті. Кожне повідомлення повинне зберігатися в незашифрованому виді для використання в практичних цілях. Крім

того, копія повідомлення також повинна зберігатися в зашифрованому виді, щоб можна було перевірити якщо буде потреба підпис. Більше ефективним способом є шифрування невеликого блоку біт, що є функцією від повідомлення. Такий блок, називаний автентифікатором, повинен мати властивість неможливості зміни повідомлення без зміни автентифікатора. Якщо автентифікатор зашифрований *закритим ключем* відправника, він є ***цифровим підписом***, за допомогою якої можна перевірити вихідне повідомлення. Далі ця технологія буде розглядатися в деталях.

Важливо підкреслити, що описаний процес створення підпису не забезпечує конфіденційність. Це означає, що повідомлення, послане таким способом, неможливо змінити, але можна підглянути. Це очевидно в тому випадку, якщо підпис заснований на автентифікаторі, тому що саме повідомлення передається в явному виді. Але навіть якщо здійснюється шифрування всього повідомлення, конфіденційність не забезпечується, тому що кожний може розшифрувати повідомлення, використовуючи *відкритий ключ* відправника.

Обмін ключів: дві сторони взаємодіють для обміну ключем сесії, що надалі можна використовувати в алгоритмі симетричного шифрування.

Деякі алгоритми можна задіяти трьома способами, у той час як інші можуть використовуватися одним або двома способами.

Перелічимо найбільш популярні алгоритми з *відкритим ключем* і можливі способи їхнього застосування.

- Диффи-Хеллман DH (Diffie, Hellman);
- RSA (Rivest, Shamir, Adleman); (стандарт ISO-MKKTT X-509), RSA-PSS;
- Эль-Гамаль ElGamal (DSA (X9.30)) ;
- ACE-Sign;
- Flash, Sflash;
- Quartz;
- ESIGN;
- Цифровий підпис DSS (P1363), Шнора, EC-DSA – GF(p), EC-DSA – GF(2^m), ECSS, EC-GDSA Германії, EC-KCDSA Кореї, ДСТ Р.318.310-95 Росії, ДСТ Р.3410-2001 Росії, ДСТУ 4145-2002 України. Починаючи з алгоритму Шнора, використовуються перетворення в групі точок еліптичних кривих.

17.2. Шифр RSA

Діффі й Хеллман визначили новий підхід до шифрування, що викликало до життя розробку алгоритмів шифрування, що задовольняють вимогам систем з *відкритим ключем*. Одним з перших результатів був алгоритм, розроблений в 1977 році Роном Ривестом, Ади Шамиром і Льоном Адлеманом і опублікований в 1978 році. З того часу алгоритм Rivest-Shamir-Adleman (*RSA*) широко застосовується практично у всіх додатках, що використовують криптографію з *відкритим ключем*.

Алгоритм заснований на використанні того факту, що задача ***факторизації*** (тобто розкладення числа на множники) є важкою, тобто легко перемножити два числа, у той час як не існує поліноміального алгоритму знаходження простих співмножників великого числа.

Алгоритм RSA являє собою блоковий алгоритм шифрування, де зашифровані й незашифровані дані є цілими між 0 і n -1 для деякого n.

Опис алгоритму

Алгоритм RSA використовує вираження з експонентами. Дані шифруються блоками, кожний блок розглядається як число, менше деякого числа n. Шифрування й дешифрування мають такий вигляд для деякого незашифрованого блоку M и зашифрованого блоку C.

$$C = M^e \pmod n$$

$$M = C^d \pmod n = (M^e)^d \pmod n = M^{ed} \pmod n$$

Як відправник, так і одержувач повинні знати значення n. Відправник знає значення e, одержувач знає значення d.

Таким чином, *відкритий ключ* є KU = {e, n} і *закритий ключ* є KR = {d, n}. При цьому повинні виконуватися наступні умови:

1. Можливість знайти значення e, d і n такі, що $M^{ed} = M \bmod n$ для всіх $M < n$.
2. Відносна легкість обчислення M^e й C^d для всіх значень $M < n$.
3. Неможливість визначити d, знаючи e и n.

Тепер розглянемо сам *алгоритм RSA*.

Нехай p і q – прості.

$$n = p \cdot q.$$

Варто вибрати e і d такі, що $e \cdot d \equiv 1 \bmod \Phi(n)$, де Φ (n) – функція Ейлера, й у даному випадку:

$$\Phi(n) = (p-1)(q-1)$$

$$\text{або } e\,d \equiv 1 \bmod \Phi(n)$$

e і d є взаємнозворотними по множенню за модулем Φ(n). Помітимо, що відповідно до правил модульної арифметики, це вірно тільки в тому випадку, якщо d (і отже, e) є взаємнопростими з Φ(n). Таким чином, НЗД (Φ(n), d) = 1, де НЗД – найбільший загальний дільник.

Тепер розглянемо всі елементи *алгоритму RSA*.

p, q – два простих цілих числа	– відкрито, розраховується.
$n = p \cdot q$	– закрито, розраховується.
d, НЗД (Φ(n), d) = 1; $1 < d < \Phi(n)$	– відкрито, обирається.
$e\,d \equiv 1 \bmod \Phi(n)$	– закриті, обирані.

Закритий ключ складається з {d, n}, *відкритий ключ* складається з {e, n}. Припустимо, що користувач A опублікував свій *відкритий ключ*, і що користувач B хоче послати користувачеві A повідомлення M. Тоді B обчислює $C = M^e \pmod n$ і передає C. При одержанні цього зашифрованого тексту користувач A дешифрує обчисленням $M = C^d \pmod n$.

Підсумуємо ***алгоритм RSA***:

Створення ключів
Вибрати прості p та q
Обчислити $n = p \cdot q$
Вибрати d НЗД $(\Phi(n), d) = 1$; $1 < d < \Phi(n)$
Обчислити e $e = d^{-1} \bmod \Phi(n)$
Відкритий ключ KU = {e, n}
Закритий ключ KR = {d, n}

Шифрування
Незашифрований текст: $M < n$
Зашифрований текст: $C = M^e \pmod n$

Дешифрування
Зашифрований текст: C
Незашифрований текст: $M = C^d \pmod n$

Розглянемо конкретний **приклад**:
Вибрати два простих числа: $p = 7$, $q = 17$.
Обчислити $n = p \cdot q = 7 \cdot 17 = 119$.
Обчислити $\Phi(n) = (p - 1) \cdot (q - 1) = 96$.
Вибрати e так, щоб e було взаємопростим з $\Phi(n) = 96$ і менше, ніж $\Phi(n)$:
$e = 18$.
Визначити d так, щоб $d \cdot e \equiv 1 \bmod 96$ и $d < 96$.
$d = 77$, тому що $77 \cdot 5 = 385 = 4 \cdot 96 + 1$.
Результуючі ключі: *відкритий* KU = {5, 119} і *закритий* KR = {77, 119}.
Наприклад, потрібно зашифрувати повідомлення M = 19.
$19^5 = 66 \pmod{119}$; C = 66.
Для дешифрування обчислюється $66^{77} \pmod{119} = 19$.

Обчислювальні аспекти

Розглянемо складність обчислень в *алгоритмі RSA* при створенні ключів і при шифруванні/дешифруванні.

Створення ключів

Створення ключів включає наступні задачі:

1. Визначити два простих числа p й q.
2. Вибрати e й обчислити d.

Насамперед, розглянемо проблеми, пов'язані з вибором p й q. Тому що значення $n = p \cdot q$ буде відомо будь-якому потенційному супротивникові, для запобігання розкриття p и q ці прості числа повинні бути обрані з досить великої множини, тобто p и q повинні бути великими числами. З іншого боку, метод, використовуваний для пошуку великого простого числа, повинен бути досить ефективним. У цей час невідомі алгоритми, які створюють довільно великі прості числа. Процедура, що використовується для цього, вибирає випадкове непарне

число з необхідного діапазону й перевіряє, чи є воно простим. Якщо число не є простим, то знову вибирається випадкове число доти, поки не буде знайдено просте.

Були розроблені різні тести для визначення того, чи є число простим. Це тести імовірнісні, тобто тест показує, що дане число ймовірно є простим. Незважаючи на це вони можуть виконуватися таким чином, що зроблять імовірність близької до 1. Якщо n "провалює" тест, то воно не є простим. Якщо n "пропускає" тест, то n може як бути, так і не бути простим. Якщо n пропускає багато таких тестів, то можна з високим ступенем вірогідності сказати, що n є простим. Це досить довга процедура, але вона виконується відносно рідко: тільки при створенні нової пари (KU, KR).

На складність обчислень також впливає те, яка кількість чисел буде відкинута перед тим, як буде знайдене просте число. Результат з теорії чисел, відомий як теорема простого числа, говорить, що простих чисел, розташованих біля n у середньому одне на кожні ln (n) чисел. Таким чином, у середньому потрібно перевірити послідовність із ln (n) цілих, перш ніж буде знайдене просте число. Тому що всі парні числа можуть бути відкинуті без перевірки, то потрібно виконати приблизно ln (n)/2 перевірок. Наприклад, якщо просте число шукається в діапазоні величин 2^{200}, то необхідно виконати біля ln (2^{200}) / 2 = 70 перевірок.

Вибравши прості числа p и q, далі варто вибрати значення e так, щоб НЗД(Ф(n), e) = 1 і обчислити значення d, $d = e^{-1} \bmod Ф(n)$. Існує єдиний алгоритм, називаний розширеним алгоритмом Евклида, що за фіксований час обчислює найбільший загальний дільник двох цілих і якщо цей загальний дільник дорівнює одиниці, визначає інверсне значення одного по модулі іншого. Таким чином, процедура складається в генерації серії випадкових чисел і перевірці кожного відносно Ф(n) доти, поки не буде знайдене число, взаємопросте з Ф(n). Виникає питання, як багато випадкових чисел прийде перевірити доти, поки не найдеться потрібне число, що буде взаємопростим з Ф(n). Результати показують, що ймовірність того, що два випадкових числа є взаємопростими, дорівнює 0.6.

Шифрування/дешифрування

Як шифрування, так і дешифрування включають піднесення цілого числа в цілий ступінь за модулем n. При цьому проміжні значення будуть величезними. Для того, щоб частково цього уникнути, використовується наступна властивість модульної арифметики:

$$[(a \bmod n) \cdot (b \bmod n)] \bmod n = (a \cdot b) \bmod n$$

Інша оптимізація складається в ефективному використанні показника ступеня, тому що у випадку *RSA* показники ступеня дуже більші. Припустимо, що необхідно обчислити x^{16}. Прямий підхід вимагає 15 множень. Однак можна домогтися того ж кінцевого результату за допомогою тільки чотирьох множень, якщо використовувати квадрат кожного проміжного результату: x^2, x^4, x^8, x^{16}.

18.3. Алгоритм Ель-Гамаля (EG)

Основна ідея алгоритму Ель-Гамаля полягає в тому, що не існує ефективних методів рішення порівняння $a^x == b \pmod p$

Позначення. Через $Z(n)$ позначимо відрахування по модулі n, через $Z^*(n)$ – мультиплікативну групу оборотних елементів в $Z(n)$. Через $a^b \pmod n$ будемо позначати піднесення a у ступінь b у кільці $Z(n)$. Якщо p – простої число, то група $Z^*(p)$ ізоморфна $Z(p\text{-}1)$.

Нехай числа p і $2p+1$ – прості, $p>2$,v і w – утворюючих мультиплікативних груп $Z^*(p)$ і $Z^*(2p+1)$ відповідно.

Позначення.

p, $2p+1$ – прості числа,

v, w – утворюючих груп $Z^*(p)$ і $Z^*(2p+1)$ відповідно,

$v_0 = p + (p+1)v$ – утворююча $Z^*(2p)$,

x – секретний пароль, число з $Z(p\text{-}1)$,

z – проміжне вираження з $Z(2p)$,

y – відкриттів пароль, число з $Z^*(2p+1)$,

s – інформаційне число,

r – випадкове число з $Z(2p)$,

(a,b) – електронний підпис: a з $Z(2p)$, b з $Z^*(2p+1)$,

(c,d) – зашифроване повідомлення: c з $Z^*(2p+1)$, d з $Z^*(2p+1)$,

e – проміжне вираження з $Z^*(2p+1)$.

Знаходження відкритого ключа по секретному. $x => y$

1. $v_0 = p + (p+1)*v \pmod{2p}$
2. $z = v_0^x \pmod{2p}$
3. $y = w^z \pmod{2p+1}$

Електронний підпис $x, s, r => a, b$ (r – випадкове)

1. $v_0 = p + (p+1)*v \pmod{2p}$
2. $a = v_0^{(p-1-x)}*r*s \pmod{2p}$
3. $b = w^s \pmod{2p+1}$

Перевірка підпису $y, s, a, b => y/n$

1. $y^a == b_s \pmod{2p+1}$

Шифрування $y, s, r => c, d$

1. $e = y^r \pmod{2p+1}$
2. $c = w^r \pmod{2p+1}$
3. $d = s*e \pmod{2p+1}$

Розшифровка $x, c, d => s$

1. $v_0 = p + (p+1)*v \pmod{2p}$
2. $z = v_0^x \pmod{2p}$
3. $1/e = c^{2\,p-z} \pmod{2p+1}$
4. $s = d/e \pmod{2p+1}$

За складністю ведення криптоаналізу вище перераховані алгоритми приблизно еквівалентні, тому що в цей час завдання факторизації багаторазрядного модуля, і завдання ДЛ, уважаються розрахунково нерозв'язними для використовуваних на практиці 512-ти бітних модулів

(вимагають порядку 10^{20} групових операцій). Однак при однаковій довжині модуля алгоритм Ель-Гамаля є трохи більш стійким. Довжина ключа не менше 320 біт.

18.4. Генерація спільних секретів Діффі-Хеллмана (DH)

Алгоритм обміну ключа Діффі-Хеллмана

Ціль алгоритму полягає в тому, щоб два учасники могли безпечно обмінятися ключем, що надалі може використовуватися в якому-небудь алгоритмі симетричного шифрування. Сам ***алгоритм Діффі-Хеллмана*** може застосовуватися тільки для обміну ключами.

Алгоритм заснований на труднощі обчислень *дискретних логарифмів*. ***Дискретний логарифм*** визначається в такий спосіб. Уводиться поняття ***примітивного кореня простого числа*** Q як числа, чиї ступені створюють всі цілі від 1 до Q – 1. Це означає, що якщо A є *примітивним коренем простого числа* Q, тоді числа

$$A \bmod Q,\ A^2 \bmod Q,\ldots,\ A^{Q-1} \bmod Q$$

є різними й складаються із цілих від 1 до Q – 1 з деякими перестановками. У цьому випадку для будь-якого цілого Y < Q і *примітивного кореня* A простого числа Q можна знайти єдину експоненту X, таку, що

$$Y = A^X \bmod Q, \text{ де } 0 \leq X \leq (Q-1)$$

Експонента X називається ***дискретним логарифмом***, або індексом Y, по підставі A mod Q. Це позначається як

$$\text{ind}_{,Q}(Y).$$

Тепер опишемо **алгоритм обміну ключів Діффі-Хеллмана**.

Загальновідомі елементи

Q – просте число

A – A < Q і A є *примітивним коренем* Q

Створення пари ключів користувачем I

Вибір випадкового числа X_i (*закритий ключ*) $X_i < Q$

Обчислення числа Y_i (*відкритий ключ*) $Yi = A^{Xi} \bmod Q$

Створення *відкритого ключа* користувачем J

Вибір випадкового числа X_j (*закритий ключ*) $X_j < Q$

Обчислення випадкового числа Y_j (*відкритий ключ*) $Yj = A^{Xj} \bmod Q$

Створення загального секретного ключа користувачем I:

$$K = (Y_j)^{Xi} \bmod Q$$

Створення загального секретного ключа користувачем J:

$$K = (Y_i)^{Xj} \bmod Q$$

Передбачається, що існують два відомих усім числа: просте число Q і ціле A, що є *примітивним коренем* Q. Тепер припустимо, що користувачі I і J хочуть обмінятися ключем для алгоритму симетричного шифрування. Користувач I вибирає випадкове число $X_i < Q$ і обчислює $Y_i = A^{Xi} \bmod Q$. Аналогічно користувач J незалежно вибирає випадкове ціле число $X_j < Q$ і обчислює $Y_j = A^{Xj} \bmod Q$. Кожна сторона тримає значення X у секреті й робить значення Y

доступним для іншої сторони. Тепер користувач I обчислює ключ як $K = (Y_j)^{Xi} \bmod Q$, і користувач J обчислює ключ як $K = (Y_i)^{Xj} \bmod Q$. У результаті обоє одержать те саме значення:

$$K = (Y_j)^{Xi} \bmod Q = (A^{Xj} \bmod Q)^{Xi} \bmod Q = (A^{Xj})^{Xi} \bmod Q =$$

за правилами модульної арифметики:

$$= A^{Xj\,Xi} \bmod Q = (A^{Xj})^{Xj} \bmod Q = (A^{Xi} \bmod Q)^{Xj} \bmod Q = (Y_i)^{Xj} \bmod Q = K$$

Таким чином, дві сторони обмінялися секретним ключем. Так як X_i і X_j є закритими, супротивник може одержати тільки наступні значення: Q, A, Y_i і Y_j. Для обчислення ключа атакуючий повинен зламати *дискретний логарифм*, тобто обчислити

$$X_j = \text{ind}_{a,\,q}(Y_j)$$

Безпека обміну ключа в *алгоритмі Діффі-Хеллмана* випливає з того факту, що, хоча відносно легко обчислити експоненти по модулі простого числа, дуже важко обчислити *дискретні логарифми*. Для великих простих чисел задача вважається нерозв'язною.

Варто помітити, що даний алгоритм уразливий для атак типу " in-the-middle". Якщо супротивник може здійснити активну атаку, тобто має можливість не тільки перехоплювати повідомлення, але й заміняти їх іншими, він може перехопити *відкриті ключі* учасників Y_i і Y_j, створити свою пару *відкритого* й *закритого ключа* ($X_{оп}$, $Y_{оп}$) і послати кожному з учасників свій *відкритий ключ*. Після цього кожний учасник обчислить ключ, що буде загальним із супротивником, а не з іншим учасником. Якщо немає контролю цілісності, то учасники не зможуть виявити подібну підміну.

17.5. Електронний цифровий підпис DSA

Алгоритм цифрового підпису DSA (Digital Signature Algorithm) запропонований в 1991 р в США для використання в стандарті цифрового підпису DSS (Digital Signature Standard). Алгоритм DSA є розвитком алгоритмів цифрового підпису Ель Гамаля та К. Шнорра.

Відправник та одержувач електронного документа використовують при обчисленні великі цілі числа: g та p – прості числа, l біт кожне ($512 \le l \le 1024$); q – просте число довжиною 160 біт (дільник числа (p-1)). числа g, p, q є відкритими та можуть бути загальними для всіх користувачів мережі.

Відправник вибирає випадкове ціле число x, яке є **секретним ключем** $0 < x < q$.

Потім відправник обчислює значення:

$$y = g^x \bmod p.$$

число y **є відкритим ключем** для перевірки підпису відправника. Число y передається всім одержувачам документів.

Відкритими параметрами є числа (p, q, g, y). Закритий параметр лише один – число x. У цьому числа (p, q, g) може бути загальними групи користувачів, а числа x та y є відповідно закритим та відкритим ключами конкретного користувача. Під час підписування повідомлення використовуються секретні

числа x та k, причому число k має вибиратися випадковим чином (на практиці псевдовипадковим) при обчисленні підпису кожного наступного повідомлення.

Оскільки (p, q, g) можуть бути використані для декількох користувачів, на практиці часто поділяють користувачів за деякими критеріями групи з однаковими (p, q, g). Тому ці параметри називають доменними параметрами (Domain Parameters).

Підпис повідомлення

Цей алгоритм також передбачає використання односторонньої функції ґешування h(·). У стандарті DSS визначено алгоритм безпечного ґешування SHA (Secure Hash Algorithm).

Для того щоб підписати документ M, відправник ґешує його в ціле ґеш-значення m:

$$m = \mathrm{h}(M),\ l < q.$$

Потім генерує випадкове ціле число k, $0 < k < q$

$$r = (g^k \bmod p) \bmod q.$$

Потім відправник обчислює за допомогою секретного ключа x ціле число s:

$$s = k^{-1}(\mathrm{h}(M)) + x \cdot r) \bmod q$$

Пара чисел r та s утворює цифровий підпис (r, s) під документом M.

Таким чином, підписане повідомлення являє собою трійку чисел $[M, r, s]$.

Перевірка підпису

Одержувач обчислює значення:

$$w = s^{-1} \bmod q,$$

ґеш-значення:

$$m = h(M)$$

та числа:

$$u_1 = (m * w) \bmod q,$$
$$u_2 = (r * w) \bmod q.$$

Далі одержувач за допомогою відкритого ключа y обчислює значення:

$$v = (g^{u1} \cdot y^{u2} \bmod p) \bmod q$$

та перевіряє виконання умови

$$v = r.$$

Якщо умова $v = r$ виконується, тоді підпис (r, s) під документом m визнається одержувачем справжньої.

Можна строго математично довести, що остання рівність буде виконуватися тоді, та тільки тоді, коли підпис (r, s) під документом M отримана за допомогою саме того секретного ключа x, з якого був отриманий відкритий ключ y. Таким чином, можна надійно упевнитися, що відправник повідомлення володіє саме даними секретним ключем x (не розплющуючи при цьому значення ключа X) та що відправник підписав саме даний документ M.

У порівнянні з алгоритмом цифрового підпису Ель Гамаля алгоритм DSA має наступні основні переваги:

1. При будь-якому допустимому рівні стійкості, тобто при будь-якій парі чисел g та p (від 512 до 1024 біт), числа q, x, r, s мають довжину по 160 біт, скорочуючи довжину підписи до 320 біт.

2. Більшість операцій з числами k, r, s, x при обчисленні підписи проводиться за модулем числа q довжиною 160 біт, що скорочує час обчислення підпису.

3. При перевірці підпису більшість операцій з числами u_1, u_2, v, w також проводиться за модулем числа q довжиною 160 біт, що скорочує обсяг пам'яті та час обчислення.

Недоліком алгоритму DSA є те, що при підписуванні та при перевірці підпису доводиться виконувати складні операції ділення за модулем q:

$$s = k^{-1}(\mathrm{h}(M)) + x \cdot r) \bmod q,\ w = s^{-1} \bmod q,$$

що не дозволяє отримувати максимальну швидкодію.

Слід зазначити, що реальне виконання алгоритму DSA може бути прискорене за допомогою виконання попередніх обчислень. Зауважимо, що значення r не залежить від повідомлення M та його ґеш-значення m. Можна заздалегідь створити рядок випадкових значень k та потім для кожного з цих значень обчислити значення r. Можна також заздалегідь обчислити зворотні значення k^{-1} для кожного із значень k. Потім, під час вступу повідомлення m, можна обчислити значення s для даних значень r та k^{-1}. Ці попередні обчислення значно прискорюють роботу алгоритму DSA.

17.6. Криптографія на еліптичних кривих

У 1985 році незалежно Нілом Кобилице та Віктором Міллером було запропоновано використовувати в криптографії алгебраїчні властивості еліптичних кривих. З цього моменту почався бурхливий розвиток нового напряму несиметричної криптографії, для якого використовується термін "криптографія на еліптичних кривих". Роль основний криптографічних операції виконує операція скалярного множення точки на еліптичній кривій на дане ціле число, що визначається через операції додавання і подвоєння точок еліптичної кривої. Останні, в свою чергу, виконуються на основі операцій додавання, множення та інвертування в кінцевому полі, над якими розглядається крива. Особливий інтерес до криптографії на еліптичних кривих обумовлений тим, що для забезпечення тієї ж стійкості використовуються менші за розмірами ключі.

Ранні криптосистеми з відкритим ключем, такі як алгоритм RSA, крипостійкість завдяки тому, що складно розкласти складене число на прості множники. При використанні алгоритмів на еліптичних кривих вважається, що не існує субекспоненціальних алгоритмів для вирішення задачі дискретного логарифмування в групах точок ЕК. При цьому порядок групи точок еліптичної кривої визначає складність завдання. Для досягнення такого ж рівня криптостійкості як і в RSA, потрібні групи менших порядків, що зменшує витрати на зберігання і передачу інформації. Наприклад, на конференції RSA 2005 Агентство національної безпеки оголосило про створення "Suite B", в якому

використовуються виключно алгоритми еліптичної криптографії, причому для захисту інформації, що класифікується до "Top Secret", використовуються лише 384-бітові ключі.

Еліптичною кривої називається множина точок (x, y), що задовольняють рівняння:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \quad (18.1)$$

У криптографії розглядаються два види еліптичних кривих: над скінченим полем Z_p – кільцем відрахунків за модулем простого числа. І над полем $GF(2^m)$ – бінарним скінченим полем.

У еліптичних кривих над полем $GF(2^m)$ є одна важлива перевага, елементи поля $GF(2^m)$ можуть бути легко представлені у вигляді n-бітових кодових слів, що дозволяє збільшити швидкість апаратної реалізації еліптичних алгоритмів.

Всі математичні операції на еліптичних кривих над скінченим полем виконуються за законами поля над яким побудована еліптична крива. Тобто, для обчислення, наприклад, суми двох точок кривої E над Z_p всі операції проводяться за модулем числа p.

У класичних несиметричних системах у якості односторонньої функції зазвичай використовується піднесення до степені за модулем. На заміну даній операції у криптографії на еліптичних кривих у якості односторонньої функції використовується множення точки на число.

Розглянемо, наприклад, варіант, вже відомого нам, **алгоритму генерації ключа Діффі-Хелмана на еліптичних кривих**.

Етап 1. Обидва учасники домовляються про значення параметрів еліптичної кривої, що буде використовуватись та обирають випадкову точку G на даній кривій. Ця інформація не є секретною.

Етап 2. Аліса вибирає випадкове число A, це її секретний ключ. Боб обирає випадкове число B, це його секретний ключ.

Етап 3. Аліса, використовуючи раніше згенероване число A, обчислює свій публічний ключ $G_a = A * G$. Боб, використовуючи раніше згенероване число B, обчислює свій публічний ключ $G_b = B * G$.

Етап 4. Аліса та Боб обмінюються своїми публічними ключами.

Етап 5. Аліса, використовуючи отриману від Боба точку G_b, обчислює спільний секрет $K = A * G_b$. Боб, використовуючи отриману від Аліси точку G_a, обчислює спільний секрет $K = B * G_a$.

У результаті, не обмінюючись секретними ключами, обидва учасники отримали однаковий спільний секрет K, оскільки:

$$K = A * G_b = A * (B * G) = (A * B) * G = (B * A) * G = B * (A * G) = B * G_a = K.$$

А для знаходження спільного ключа, не знаючи секретних параметрів, необхідно вирішити задачу обчислення дискретного логарифму у групі точок ЕК, тобто знаючи G_x та G знайти таке X, що $G_x = X * G$. На даний момент невідомо про субекспоненційні алгоритми вирішення даної задачі, тож криптографія на еліптичних кривих вважається більш стійкою ніж класична асиметрична криптографія.

18.7. Електронний цифровий підпис згідно ДСТУ 4145-2002

ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка» – національний стандарт України, що описує механізм формування та перевірки електронного цифрового підпису, що базується на властивостях груп точок еліптичних кривих над полями GF(2^m) та правилах застосування цих механізмів до повідомлень, що пересилаються каналами зв'язку та/або обробляються у комп'ютеризованих системах загального призначення. Застосування цього стандарту гарантує цілісність підписаного повідомлення, автентичність його автора та неспростовність авторства.

Затверджено та надано чинності з 1 липня 2003 року наказом Держспоживстандарту від 28 грудня 2002 року №31. Текст стандарту є у вільному доступі.

У стандарті за замовчанням використовується функція ґешування ГОСТ 318.311-95, та генератор випадкових послідовностей з використанням алгоритму криптографічного перетворення ДСТУ ГОСТ 28147:2009.

Згідно наказу Мінцифри від 30 жовтня 2020 року №140/614 після 1 січня 2021 року стандарт повинен використовуватися для створення кваліфікованого електронного підпису та для перевірки кваліфікованого електронного підпису разом з функцією ґешування Купина, але використання стандарту разом з ГОСТ 318.311-95 було можливе до 1 січня 2022 року.

ДСТУ 4145-2002 – стандарт, що установлює механізм цифрового підпису, заснований на властивостях груп точок еліптичних кривих над полями GF(2^m), та правила застосування цього механізму до повідомлень, що пересилаються каналами зв'язку та/або обробляються у комп'ютеризованих системах загального призначення. Застосування цього стандарту гарантує цілісність підписаного повідомлення, автентичність його автора та неспростовність авторства [текст стандарту ДСТУ 4145-2002].

Алгоритм обчислення цифрового передпідпису.

Вхідні дані алгоритму: загальні параметри цифрового підпису.

Результат виконання алгоритму – цифровий передпідпис Fe, що відповідає таємному випадковому параметру e, де e – ціле число, $0 < e < n$, $Fe \in GF(2^m)$.

Кроки алгоритму:

1. Обчислюють випадкове ціле число e згідно з розділом 6.3 [текст стандарту ДСТУ 4145-2002].

2. Обчислюють точку еліптичної кривої $R = eP = (x_R, y_R)$.

3. Якщо координата $x_R = 0$, то переходять до кроку 1, інакше приймають $F_e = x_R$ і переходять до кроку 18.

4. Результат виконання алгоритму – цифровий передпідпис F_e та таємний випадковий параметр e.

Умови обчислення й зберігання таємного параметра e мають унеможливлювати несанкціонований доступ до нього, його частин, а також до проміжних даних, які використовувались у процесі обчислення цифрового передпідпису.

Припускається попереднє обчислення довільного числа цифрових передпідписів. Умови зберігання цифрового передпідпису мають унеможливлювати його модифікацію або підміну. Після використання цифрового передпідпису його негайно знищують разом з відповідним таємним параметром е.

Алгоритм обчислення цифрового підпису

Вхідні дані алгоритму:

– загальні параметри цифрового підпису;

– особистий ключ цифрового підпису d;

– повідомлення T довжини $L_T > 0$;

– функція ґешування H згідно з розділом 6.2 [текст стандарту ДСТУ 4145-2002];

– довжина цифрового підпису L_D, що вибирається для групи користувачів, виходячи з умов конкретної реалізації алгоритму цифрового підписування, з урахуванням умов кроку 3 даного алгоритму.

Результат виконання алгоритму: повідомлення T і цифровий підпис D, що дають змогу утворити підписане повідомлення (iH, T, D).

Кроки алгоритму:

1) Перевіряють правильність загальних параметрів цифрового підпису згідно з розділів 8.1-8.3 [текст стандарту ДСТУ 4145-2002]. Якщо загальні параметри цифрового підпису обчислено неправильно, то обчислення цифрового підпису припиняють. Цю перевірку не виконують у випадках, передбачених у розділах 8.1-8.3 [текст стандарту ДСТУ 4145-2002].

2) Перевіряють правильність особистого ключа цифрового підпису згідно з розділом 10.2 [текст стандарту ДСТУ 4145-2002]. Якщо особистий ключ неправильний, то обчислення цифрового підпису припиняють. Цю перевірку не виконують у випадках, передбачених у розділі 10.2 [текст стандарту ДСТУ 4145-2002].

3) Перевіряють виконання умов: L_D – число, кратне 16, $L_D \geq 2L(n)$. Якщо хоча б одна з цих умов не виконана, то обчислення цифрового підпису припиняють.

4) Якщо використовується ідентифікатор ґеш-функції iH, то перевіряють, чи цей ідентифікатор діє у відповідній групі користувачів. Якщо ні, то обчислення цифрового підпису припиняють.

5) Якщо нормативні документи, що встановлюють обчислення функції ґешування, накладають обмеження на довжину повідомлення LT, то перевіряють виконання цих обмежень. Якщо ці обмеження не виконані, або повідомлення відсутнє, або $L_T \leq 0$, то обчислення цифрового підпису припиняють.

6) За повідомленням T обчислюють функцію ґешування $H(T)$.

7) Результат обчислення функції ґешування $H(T)$ перетворюють на елемент основного поля h згідно з розділом 5.9 [текст стандарту ДСТУ 4145-2002]. Якщо $h = 0$, то приймають $h = 1$.

8) Якщо існує набір цифрових передпідписів, обчислених заздалегідь, то беруть будь-який з них разом з відповідним таємним параметром. Інакше обчислюють цифровий передпідпис. Нехай на цьому кроці алгоритму отримано передпідпис F_e та відповідний таємний параметр e.

9) Обчислюють елемент основного поля $y = hF_e$.

10) Елемент основного поля y перетворюють на ціле число r згідно з розділом 5.8 [текст стандарту ДСТУ 4145-2002].

11) Якщо $r = 0$, то переходять до кроку 8, інакше переходять до кроку 12.

12) Обчислюють ціле число $s = (e + dr)\ mod\ n$.

13) Якщо $s = 0$, то переходять до кроку 8, інакше переходять до кроку 118.

14) Пару цілих чисел (r, s) перетворюють на цифровий підпис D довжини L_D згідно з розділом 5.10 [текст стандарту ДСТУ 4145-2002].

15) Результат виконання алгоритму – підписане повідомлення (iH, T, D).

Алгоритм перевірки цифрового підпису

Вхідні дані алгоритму:

– загальні параметри цифрового підпису;

– відкритий ключ цифрового підпису Q;

– підписане повідомлення (iH, T, D) довжини $L = L(iH) + L_T + LD$;

– функція ґешування H згідно з розділом 6.2 [текст стандарту ДСТУ 4145-2002].

Результат виконання алгоритму: повідомлення “підпис дійсний” або повідомлення “підпис недійсний”.

Кроки алгоритму:

1) Якщо використовується ідентифікатор ґеш-функції iH, то перевіряють, чи діє цей ідентифікатор у відповідній групі користувачів. Якщо ні, то видають повідомлення “підпис недійсний” і припиняють перевірку цифрового підпису.

2) Виходячи з iH (або за промовчанням) визначають L_H.

3) Перевіряють виконання умов: L_D – число, кратне 16, $L_D \geq 2L(n)$. Якщо хоча б одна з цих умов не виконана, то видають повідомлення “підпис недійсний” і припиняють перевірку цифрового підпису.

4) Перевіряють правильність обчислення загальних параметрів цифрового підпису згідно з розділів 8.1-8.3 [текст стандарту ДСТУ 4145-2002]. Якщо загальні параметри цифрового підпису обчислено неправильно, то видають повідомлення “підпис недійсний” і припиняють перевірку цифрового підпису. Цю перевірку не виконують у випадках, передбачених у розділах 8.1-8.3 [текст стандарту ДСТУ 4145-2002].

5) Перевіряють правильність відкритого ключа цифрового підпису згідно з розділом 10.1 [текст стандарту ДСТУ 4145-2002]. Якщо відкритий ключ обчислено неправильно, то видають повідомлення “підпис недійсний” і

припиняють перевірку цифрового підпису. Цю перевірку не виконують у випадках, передбачених у розділі 10.1 [текст стандарту ДСТУ 4145-2002].

6) Обчислюють $L_T = L - L_D - L(iH)$. У випадку відсутності тексту, або при $L_T \leq 0$ видають повідомлення "підпис недійсний" і припиняють перевірку цифрового підпису. Якщо нормативні документи, які встановлюють обчислення функції ґешування, накладають обмеження на довжину повідомлення L_T, то перевіряють виконання цих умов. Якщо ці умови не виконані, то видають повідомлення "підпис недійсний" і припиняють перевірку цифрового підпису.

7) За повідомленням T обчислюють функцію ґешування $H(T)$.

8) Ґеш-код $H(T)$ перетворюють на елемент основного поля h згідно з розділом 5.9 [текст стандарту ДСТУ 4145-2002]. Якщо $h = 0$, то приймають $h = 1$.

9) Цифровий підпис D перетворюють на пару цілих чисел (r, s) згідно з розділом 5.11 [текст стандарту ДСТУ 4145-2002].

10) Якщо умова $0 < r < n$ не виконана, то видають повідомлення "підпис недійсний" і припиняють перевірку цифрового підпису.

11) Якщо умова $0 < s < n$ не виконана, то видають повідомлення "підпис недійсний" і припиняють перевірку цифрового підпису.

12) Обчислюють точку еліптичної кривої $R = sP + rQ$, $R = (x_R, y_R)$.

13) Обчислюють елемент основного поля $y = hx_R$.

14) Елемент основного поля y перетворюють на ціле число $\tilde{r}$ згідно з розділом 5.8 [текст стандарту ДСТУ 4145-2002].

15) Якщо $r = \tilde{r}$, то видають повідомлення "підпис дійсний", інакше видають повідомлення "підпис недійсний".

18.8. EC-DSA згідно ISO/IEC 15946-2

У міжнародному стандарті ISO/IEC 15946-2 представлено декілька алгоритмів електронного цифрового підпису, серед яких – EC-DSA. Даний алгоритм ЕЦП також представлений у стандарті США FIPS 186-4 та був гармонізований у державному стандарті ДСТУ ISO/IEC 15946-2 тож розглянемо саме його.

Схема цифрового підпису EC-DSA є аналогом схеми цифрового підпису DSA на еліптичних кривих. Схема є прикладом механізму вироблення цифрового підпису з доповненням.

Параметри домену та параметри користувачів

Бітова довжина модуля n повинна бути більше ніж бітова довжина вихідного значення ґеш-функції $h()$. Особистий й відкритий ключі об'єкта A: d_A і P_A відповідно, повинно виробляти у відповідності із процедурою 7.1, що визначена у стандарті ISO/IEC 15946-1.

Процес вироблення цифрового підпису.

Вхідними даними для процесу вироблення цифрового підпису є такі:

– параметри домену;

– особистий ключ d_A підписувача;

– повідомлення M.

Виходом процесу вироблення цифрового підпису є пара:

$$(r, s) \in F(n) * F(n),$$

яка становить цифровий підпис повідомлення M об'єкта A.

Для **підписування повідомлення M об'єктом A виконуються такі кроки**:

1. Обчислення ґеш-значення $e = h(M)$.

2. Вибір випадкового цілого числа k в інтервалі $\{1, \ldots, n - 1\}$.

3. Обчислення точки на еліптичній кривій $(x_1, y_1) = kG$.

4. Обчислення $r = \pi(kG) \; mod \; n$.

5. Обчислення k^{-1} в полі $F(n)$.

6. Обчислення $s = (d_A r + e)k^{-1} \; mod \; n$.

Якщо у процесі вироблення цифрового підпису формується або $s = 0$, або $r = 0$, тоді процес вироблення цифрового підпису необхідно повторити з новим випадковим значенням k. (Але необхідно зазначити, що ймовірність того, що $s = 0$ або $r = 0$ є надзвичайно малою, якщо k обрано відповідно до розділів 6.2.2. та 18.2.1 [текст стандарту ISO/IEC 15946-2]).

Пара цілих чисел (r, s) становить цифровий підпис повідомлення M об'єкта A.

У зв'язку з тим, що обчислене значення r не залежить від повідомлення, що підписується, число r може обчислюватися попередньо, і надалі зберігатися та використовуватися під час вироблення цифрового підпису.

Процес перевірки цифрового підпису

Процес перевірки цифрового підпису складається з 4 кроків: перевірки розміру ЕЦП, обчислення ґеш-значення повідомлення, обчислення на еліптичних кривих та перевірка цифрового підпису.

Вхідними даними для перевірки цифрового підпису є такі:

– параметри домену;

– відкритий ключ P_A об'єкта A;

– одержане повідомлення M';

– одержаний цифровий підпис повідомлення M', представлений двома цілими числами r' та s'.

Для **перевірки цифрового підпису повідомлення** M' об'єкта A, об'єктом B виконуються такі кроки:

1. Перевіряння того, що $0 < r' < n$ та $0 < s' < n$. Якщо хоч одна умова не виконуються, то цифровий підпис відхиляється.

2. Обчислення ґеш-значення $e' = h(M')$, використовуючи ґеш-функцію $h()$.

3. Обчислення $w = (s')^{-1} \; mod \; n$.

4. Обчислення $u_1 = e'w \; mod \; n$ та $u_2 = r'w \; mod \; n$.

5. Обчислення точки на ЕК $(x_1, y_1) = u_1G + u_2P_A$.

6. Обчислення $v = \pi((x_1, y_1)) \; mod \; n$.

Якщо $r' = v$, тоді цифровий підпис повинен прийматися перевірником.

Якщо $r' \neq v$, тоді цифровий підпис повинен відхилятися перевірником.

Стандарти, що визначають вимоги до асиметричних криптографічних алгоритмів та методів (asymmetric algorithms and techniques)

1. ДСТУ 4145-2002 “Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння”.

2. ДСТУ ISO/IEC 9796-2:2015 (ISO/IEC 9796-2:2010, IDT) “Інформаційні технології. Методи захисту. Схеми цифрового підпису, які забезпечують відновлення повідомлення. Частина 2. Механізми, що ґрунтуються на факторизації цілих чисел”.

3. ДСТУ ISO/IEC 9796-3:2015 (ISO/IEC9796-3:2006, IDT) “Інформаційні технології. Методи захисту. Схеми цифрового підпису, які забезпечують відновлення повідомлення. Частина 3. Механізми, що ґрунтуються на дискретному логарифмі”.

4. ДСТУ ISO/IEC 14888-2:2015 (ISO/IEC 14888-2:2008, IDT) “Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 2. Механізми, що ґрунтуються на факторизації цілих чисел”.

5. ДСТУ ISO/IEC 14888-3:2019 (ISO/IEC 14888-3:2018, IDT) “Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 3. Механізми, що ґрунтуються на дискретному логарифмуванні”.

6. ДСТУ ISO/IEC 15946-5:2019 (ISO/IEC 15946-5:2017) “Інформаційні технології. Методи захисту. Криптографічні методи на основі еліптичних кривих. Частина 5. Генерування еліптичних кривих”.

7. ДСТУ ISO/IEC 18033-2:2015 (ISO/IEC 18033-2:2006, IDT) “Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 2. Асиметричні шифри”.

Розділ 19. Криптографічні протоколи

19.1. Протоколи захисту мережевого трафіку IPSec
19.2. Протоколи безпечної передачі даних прикладного рівня: https

19.1. Протоколи захисту мережевого трафіку IPSec

IPsec (скорочення від **IP Security**) – набір протоколів для забезпечення захисту даних, що передаються міжмережевим протоколом IP. Дозволяє здійснювати підтвердження автентичності (автентифікацію), перевірку цілісності та/або шифрування IP-пакетів. IPsec також включає протоколи для захищеного обміну ключами в мережі Інтернет. В основному застосовується для організації VPN -з'єднань.

Стандарти

– RFC 4301 (раніше RFC 2401) (Security Architecture for the Internet Protocol) – архітектура захисту для протоколу IP.

– RFC 4302 (раніше RFC 2402) (IP Authentication header) – автентифікаційний заголовок IP.

– RFC 2403 (The Use of HMAC-MD5-96 with ESP and AH) – використання алгоритму ґешування MD-5 для створення автентифікаційного заголовка.

– RFC 2404 (The Use of HMAC-SHA-1-96 with ESP and AH) – використання алгоритму ґешування SHA-1 для створення автентифікаційного заголовка.

– RFC 2405 (ESP DES-CBC Cipher Algorithm With Explicit IV) – використання алгоритму шифрування DES.

– RFC 4303 (раніше RFC 2406) (IP Encapsulating Security Payload [ESP]) – шифрування даних.

– RFC 2407 (Internet Internet Security Domain of Interpretation for ISAKMP) – область застосування протоколу управління ключами.

– RFC 2408 (Internet Security Association and Key Management Protocol [ISAKMP]) – управління ключами та автентифікаторами захищених з'єднань.

– RFC 4109 (раніше RFC 2409) – обмін ключами IKEv1.

– RFC 4306 (Internet Protocol Key Exchange (IKEv2)) – протокол обміну ключами IKEv2.

– RFC 8247 (Algorithm Implementation Requirements and Usage Guidance the Internet Key Exchange Protocol Version 2 (IKEv2)) – правила реалізації та використання криптоалгоритмів в IKEv2.

– RFC 2410 (Null Encryption Algorithm and Its Use With IPsec) – нульовий алгоритм шифрування та його використання.

– RFC 2411 (IP Security Document Roadmap) – подальший розвиток стандарту.

– RFC 2412 (The OAKLEY Key Determination Protocol) – перевірка відповідності ключа.

Архітектура IPsec

Побудова захищеного каналу зв'язку може бути реалізована на різних рівнях моделі OSI. IPsec реалізований на мережному рівні. У питанні вибору рівня реалізації захищеного каналу кілька суперечливих аргументів: з одного боку, за вибір верхніх рівнів говорить їхня незалежність від виду транспортування (вибору протоколу мережного та канального рівнів), з іншого боку, для кожного додатка необхідне окреме налаштування та конфігурація. Плюсом у виборі нижніх рівнів є їхня універсальність та наочність для додатків, мінусом – залежність від вибору конкретного протоколу (наприклад, PPP або Ethernet). Те, що IPsec розміщується на мережному рівні, є компромісом у виборі рівня OSI. IPsec використовує найпоширеніший протокол мережного рівня – IP, що робить гнучким застосування IPsec – він може використовуватися для захисту будь-яких протоколів, що базуються на IP (TCP, UDP та інші). У той же час він прозорий для більшості програм.

IPsec є набором стандартів Інтернету та свого роду «надбудовою» над IP-протоколом. Його ядро становлять три протоколи:

– Authentication Header (AH) забезпечує цілісність даних, що передаються, автентифікацію джерела інформації та функцію запобігання повторній передачі пакетів

– Encapsulating Security Payload (ESP) забезпечує конфіденційність (шифрування) інформації, що передається, обмеження потоку конфіденційного трафіку. Крім цього, він може виконувати функції AH: забезпечити цілісність переданих даних, автентифікацію джерела інформації та функцію запобігання повторній передачі пакетів. При застосуванні ESP в обов'язковому порядку повинен вказуватися набір послуг із безпеки: кожна з його функцій може включатися опціонально.

– Internet Security Association and Key Management Protocol (ISAKMP) – протокол, який використовується для первинної настройки з'єднання, взаємної автентифікації кінцевими вузлами одне одного та обміну секретними ключами. Протокол передбачає використання різних механізмів обміну ключами, включаючи завдання фіксованих ключів, використання таких протоколів, як Internet Key Exchange, Kerberized Internet Negotiation of Keys (RFC 4430) або записів DNS типу IPSECKEY (RFC 4025).

Також одним із ключових понять є Security Association (SA). За суттю SA є набором параметрів, що характеризує з'єднання. Наприклад, використовувані алгоритм шифрування та ґеш-функція, секретні ключі, номер пакету та ін.

Тунельний та транспортний режими

IPsec може функціонувати у двох режимах:

– транспортному;

– тунельному.

У транспортному режимі шифруються або підписуються лише дані IP-пакету, вихідний заголовок зберігається. Транспортний режим зазвичай використовується для встановлення з'єднання між хостами. Він може також

використовуватися між шлюзами для захисту тунелів, організованих якимось іншим способом (див., наприклад, L2TP).

У тунельному режимі шифрується весь вихідний IP-пакет: дані, заголовок, маршрутна інформація, а потім він вставляється в поле даних нового пакета, тобто відбувається інкапсуляція. Тунельний режим може використовуватися для підключення віддалених комп'ютерів до приватної віртуальної мережі або для організації безпечної передачі даних через відкриті канали зв'язку (наприклад, Інтернет) між шлюзами для об'єднання різних частин віртуальної приватної мережі.

Режими IPsec не є взаємовиключними. На тому самому вузлі деякі SA можуть використовувати транспортний режим, інші – тунельний.

Security Association

Для початку обміну даними між двома сторонами необхідно встановити з'єднання, яке зветься SA (Security Association). Концепція SA є фундаментальною для IPsec, власне, є його суттю. Вона визначає, як сторони будуть використовувати послуги для забезпечення захищеного спілкування. З'єднання SA є симплексним (односпрямованим), тому для взаємодії сторін необхідно встановити два з'єднання. Варто також відзначити, що стандарти IPsec дозволяють кінцевим точкам захищеного каналу використовувати як одне SA для передачі трафіку всіх хостів, що взаємодіють через цей канал, так і створювати для цієї мети довільне число безпечних асоціацій, наприклад, по одній на кожне TCP-з'єднання. Це дає можливість вибирати необхідний ступінь деталізації захисту.

Встановлення з'єднання починається із взаємної автентифікації сторін.

Далі відбувається вибір параметрів (чи здійснюватиметься автентифікація, шифрування, перевірка цілісності даних) та необхідного протоколу (AH або ESP) передачі даних.

Після цього вибираються конкретні алгоритми (наприклад, шифрування, ґеш-функція) з кількох можливих схем, деякі з яких визначені стандартом (для шифрування – DES, для ґеш-функцій – MD5 або SHA-1), інші додаються виробниками продуктів, що використовують IPsec (наприклад Triple DES, Blowfish, CAST).

Security Associations Database

Усі SA зберігаються у **базі даних SAD (Security Associations Database)** IPsec-модуля. Кожне SA має унікальний маркер, що складається із трьох елементів:

– індексу параметрів безпеки (Security Parameters Index, SPI);
– IP-адреси призначення;
– ідентифікатора протоколу безпеки (ESP або AH).

IPsec-модуль, маючи ці три параметри, може знайти в SAD запис про конкретний SA. До списку компонентів SA входять:

Послідовний номер

32-бітове значення, яке використовується для формування поля *Sequence Number* у заголовках AH та ESP.

Переповнення лічильника порядкового номера

Прапор, який сигналізує про переповнення лічильника номера послідовного.

Вікно для придушення атак відтворення

Використовується для визначення повторної передачі пакетів. Якщо значення поля *Sequence Number* не потрапляє в заданий діапазон, то пакет знищується.

Інформація AH

використовується алгоритм автентифікації, необхідні ключі, час життя ключів та інші параметри.

Інформація ESP

алгоритми шифрування та автентифікації, необхідні ключі, параметри ініціалізації (наприклад, IV), час життя ключів та інші параметри

Режим роботи IPsec

тунельний або транспортний

Час життя SA

Задано в секундах або байтах інформації через тунель. Визначає тривалість існування SA, при досягненні цього значення поточне SA має завершитись, при необхідності продовжити з'єднання встановлюється нове SA.

MTU

Максимальний розмір пакета, який можна передати віртуальним каналом без фрагментації.

Кожен протокол (ESP/AH) повинен мати власний SA для кожного напряму, таким чином, зв'язка AH+ESP вимагає для дуплексного каналу наявності чотирьох SA. Всі ці дані розміщуються в SAD.

У SAD містяться:

- AH: алгоритм автентифікації.
- AH: секретний ключ для автентифікації.
- ESP: алгоритм шифрування.
- ESP: таємний ключ шифрування.
- ESP: використання автентифікації (так/ні).
- Параметри для обміну ключами.
- Обмеження маршрутизації.
- Політика IP-фільтрації.

Security Policy Database

Крім бази даних SAD, реалізації IPsec підтримують базу даних SPD (Security Policy Database – база даних політики безпеки). SPD служить для співвіднесення IP-пакетів, що приходять, з правилами обробки для них. Записи SPD складаються з двох полів. У першому зберігаються характерні ознаки пакетів, якими можна назвати той чи інший потік інформації. Ці поля називаються селекторами. Приклади селекторів, які містяться в SPD:

- IP-адреса призначення.
- IP-адреса відправника.

– Ім'я користувача у форматі DNS або X.500.
– Порти відправника та одержувача.

Друге поле SPD містить політику захисту, відповідну даному потоку пакетів. Селектори використовуються для фільтрації вихідних пакетів з метою поставити кожен пакет у відповідність до певного SA. Коли пакет надходить, порівнюються значення відповідних полів у пакеті (селекторні поля) з тими, які містяться в SPD. Під час перебування збігу в полі політики захисту міститься інформація про те, як чинити з цим пакетом: передати без змін, відкинути або обробити. У разі обробки, в цьому ж полі міститься посилання на відповідний запис SAD. Потім визначається SA для пакета та сполучений з нею індекс параметрів безпеки (SPI), після чого виконуються операції IPsec (операції протоколу AH або ESP). Якщо вхідний пакет, то в ньому відразу міститься SPI – проводиться відповідна обробка.

Authentication Header

Authentication Header format

Offsets	$Octet_{16}$	0								1								2								3							
$Octet_{16}$	Bit_{10}	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	*Next Header*								*Payload Len*								*Reserved*															
4	32	*Security Parameters Index (SPI)*																															
8	64	*Sequence Number*																															
C	96	*Integrity Check Value (ICV)*																															
...	...	...																															

Рисунок 19.1 – Структура Authentication Header

Тип наступного заголовка **(8 bits)**

Тип заголовка протоколу, що йде після заголовка AH. За цим полем приймальний IP-sec модуль дізнається про протокол, що захищається верхнього рівня. Значення цього поля для різних протоколів можна переглянути в RFC 1700.

Довжина вмісту **(8 bits)**

Це поле визначає загальний розмір AH-заголовка в 32-бітових словах мінус 2. Незважаючи на це, при використанні IPv6 довжина заголовка повинна бути кратна 8 байтам.

Зарезервовано **(16 bits)**

Зарезервовано. Заповнюється нулями.

Індекс параметрів системи безпеки **(32 bits)**

Індекс параметрів безпеки. Значення цього поля разом з IP-адресою одержувача та протоколом безпеки (AH-протокол) однозначно визначає захищене віртуальне з'єднання (SA) для цього пакета. Діапазон значень SPI 1... 255 зарезервований IANA.

Порядковий номер **(32 bits)**

Послідовний номер. Для захисту від повторної передачі. Поле містить монотонно зростаюче значення параметра. Незважаючи на те, що одержувач

може відмовитися від послуги захисту від повторної передачі пакетів, воно є обов'язковим і завжди присутній в AH-заголовку. IPsec-модуль, що передає, завжди використовує це поле, але одержувач може його і не обробляти.

Дані автентифікації

Цифровий підпис. Служить для автентифікації та перевірки цілісності пакета. Повинна бути доповнена до розміру, кратного 8 байтам для IPv6, і 4 байтам для IPv4.

Протокол AH використовується для автентифікації, тобто для підтвердження того, що ми зв'язуємося саме з тим, з ким припускаємо, і дані, які ми отримуємо, не спотворені при передачі.

Обробка вихідних IP-пакетів

Якщо передавальний IPsec-модуль визначає, що пакет пов'язаний з SA, яке передбачає AH-обробку, він починає обробку. Залежно від режиму (транспортний або тунелювання) він по-різному вставляє AH-заголовок в IP-пакет. У транспортному режимі AH-заголовок розташовується після заголовка протоколу IP та перед заголовками протоколів верхнього рівня (Зазвичай, TCP або UDP). У режимі тунелювання весь вихідний IP-пакет обрамляється спочатку заголовком AH, потім заголовком IP-протоколу. Такий заголовок називається зовнішнім, а заголовок вихідного IP-пакета – внутрішнім. Після цього передавальний IPsec-модуль повинен згенерувати послідовний номер і записати його в полі *Sequence Number*. При встановленні SA послідовний номер встановлюється в 0 і перед відправкою кожного IPsec-пакета збільшується на одиницю. Крім того, відбувається перевірка – чи не зациклився лічильник. Якщо він досяг свого максимального значення, то він знову встановлюється в 0. Якщо використовується послуга запобігання повторній передачі, то при досягненні лічильником свого максимального значення передає IPsec-модуль перевстановлює SA. Таким чином забезпечується захист від повторної посилки пакета – приймальний IPsec-модуль перевірятиме поле *Sequence Number*і ігнорувати повторно приходять пакети. Далі відбувається обчислення контрольної суми ICV. Потрібно зауважити, що тут контрольна сума обчислюється із застосуванням секретного ключа, без якого зловмисник зможе заново обчислити ґеш, але, не знаючи ключа, не зможе сформувати правильну контрольну суму. Конкретні алгоритми, що використовуються для обчислення ICV, можна дізнатися із RFC 4305. В даний час можуть застосовуватись, наприклад, алгоритми HMAC-SHA1-96 або AES-XCBC-MAC-96. Протокол AH обчислює контрольну суму (ICV) за наступними полями IPsec-пакету:

– поля IP-заголовка, які не були схильні до змін у процесі транслювання або визначені як найважливіші;

– AH-заголовок (Поля: "Next Header", "Payload Len, "Reserved", "SPI", "Sequence Number", "Integrity Check Value". Поле "Integrity Check Value" встановлюється в 0 при обчисленні ICV;

– дані протоколу верхнього рівня. Якщо поле може змінюватися в процесі транспортування, його значення встановлюється в 0 перед обчисленням ICV. Винятки становлять поля, які можуть бути змінені, але значення яких можна

передбачити при прийомі. При обчисленні ICV вони заповнюються нулями. Прикладом поля, що змінюється, може бути поле контрольної суми, прикладом зміненого, але зумовленого може бути IP-адреса одержувача. Більш детальний опис того, які поля, як враховуються при обчисленні ICV, можна знайти в стандарті RFC 2402.

Обробка вхідних IP-пакетів

Після отримання пакета, що містить повідомлення AH-протоколу, приймальний IPsec-модуль шукає відповідне захищене віртуальне з'єднання (SA) SAD (Security Associations Database), використовуючи IP-адресу одержувача, протокол безпеки (AH) та індекс SPI. Якщо відповідний SA не знайдено, пакет знищується. Знайдене захищене віртуальне з'єднання (SA) вказує на те, чи використовується послуга запобігання повторній передачі пакетів, тобто на необхідність перевірки поля *Sequence Number*. Якщо послуга використовується, поле перевіряється. У цьому використовується метод ковзного вікна обмеження буферної пам'яті, необхідний роботи протоколу. Приймальний IPsec-модуль формує вікно із шириною W (зазвичай W вибирається рівним 32 або 64 пакетам). Лівий край вікна відповідає мінімальному послідовному номеру (*Sequence Number*) N правильно прийнятого пакета. Пакет із полем *Sequence Number*, В якому міститься значення, починаючи від N+1 і закінчуючи N+W, приймається коректно. Якщо отриманий пакет виявляється по ліву межу вікна, він знищується. Потім приймальний IPsec-модуль обчислює ICV за відповідними полями прийнятого пакета, використовуючи алгоритм автентифікації, який він дізнається із запису SA, і порівнює отриманий результат зі значенням ICV, розташованим у полі Integrity Check Value. Якщо обчислене значення ICV збіглося з прийнятим, то пакет вважається дійсним і приймається для подальшої IP-обробки. Якщо перевірка дала негативний результат, прийнятий пакет знищується.

Encapsulating Security Payload

Encapsulating Security Payload format

Offsets	$Octet_{16}$	0								1								2								3							
$Octet_{16}$	Bit_{10}	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	*Security Parameters Index (SPI)*																															
4	32	*Sequence Number*																															
8	64	*Payload data*																															
...	...																																
...	...																																
...	...	*Padding (0-255 octets)*																															
...	...																	*Pad Length*								*Next Header*							
...	...	*Integrity Check Value (ICV)*																															
...	...	...																															

Рисунок 19.2 – Структура Encapsulating Security Payload

***Security Parameters Index* (32 bits)**

Індекс параметрів безпеки (подібний до відповідного поля AH). Значення цього поля разом з IP-адресою одержувача та протоколом безпеки (ESP-протокол) однозначно визначає захищене віртуальне з'єднання (SA) для цього пакета. Діапазон значень SPI 1...255 зарезервований IANA для подальшого використання.

***Sequence Number* (32 bits)**

Послідовний номер (подібний до відповідного поля AH). Для захисту від повторної передачі. Поле містить монотонно зростаюче значення параметра. Незважаючи на те, що одержувач може і відмовитися від послуги захисту від повторної передачі пакетів, воно завжди присутнє в ESP-заголовку. Відправник (передаючий IPsec-модуль) повинен завжди використовувати це поле, але одержувач може і не потребуватиме його обробки.

***Payload data* (variable)**

Це поле містить дані (залежно від вибору режиму – тунельного або транспортного, тут може знаходитися весь вихідний інкапсульований пакет, або лише його дані) відповідно до поля «Next Header». Це поле обов'язкове і складається з цілого числа байтів. Якщо алгоритм, який використовується для шифрування цього поля, вимагає даних для синхронізації криптопроцесів (наприклад, вектор ініціалізації – Initialization Vector), то це поле може містити ці дані в явному вигляді.

***Padding* (0-255 octets)**

Доповнення. Необхідно, наприклад, для алгоритмів, які вимагають, щоб відкритий текст був крадений деякому числу байтів), наприклад, розмір блоку для блокового шифру.

***Pad Length* (8 bits)**

Розмір доповнення (у байтах).

***Next Header* (8 bits)**

Це поле визначає тип даних, які у полі «Payload data».

Integrity Check Value

Контрольна сума. Служить для автентифікації та перевірки цілісності пакета. Повинна бути кратна 8 байтам для IPv6 і 4 байтам для IPv4.

Обробка вихідних IPsec-пакетів

Якщо передавальний IPsec-модуль визначає, що пакет пов'язаний з SA, яке передбачає ESP-обробку, він починає обробку. Залежно від режиму (транспортний або тунелювання) вихідний IP-пакет обробляється по-різному. У транспортному режимі передавальний IPsec-модуль здійснює процедуру обрамлення протоколу верхнього рівня (наприклад, TCP або UDP), використовуючи для цього ESP-заголовок (поля Security Parameters Index і Sequence Number заголовка) та ESP-кінцевик (інші поля заголовка, що йдуть за полем даних) – Payload data), не торкаючись при цьому заголовок вихідного IP-пакету. У режимі тунелювання IP-пакет обрамляється ESP-заголовком і ESP-кінцевиком (інкапсуляція), після чого обрамляється зовнішнім IP-заголовком

(який може не збігатися з вихідним – наприклад, якщо IPsec модуль встановлений нашлюзі). Далі виконується шифрування – у транспортному режимі шифрується лише повідомлення протоколу вищого рівня (тобто все, що було після IP-заголовка у вихідному пакеті), у режимі тунелювання – весь вихідний IP-пакет. Передавальний IPsec-модуль із запису про SA визначає алгоритм шифрування та секретний ключ. Стандарти IPsec дозволяють використання алгоритмів шифрування Triple DES, AES і Blowfish, якщо їх підтримують обидві сторони. Інакше використовується DES, прописаний RFC 2405.

Так як розмір відкритого тексту повинен бути кратний певному числу байт, наприклад, розмір блоку для блокових алгоритмів, перед шифруванням проводиться ще й необхідне доповнення повідомлення, що шифрується. Зашифроване повідомлення розміщується в полі *Payload Data*. У полі *Pad Length* міститься довжина доповнення. Потім, як і AH, обчислюється *Sequence Number*, після чого вважається контрольна сума (ICV). Контрольна сума, на відміну від протоколу AH, де при її обчисленні враховуються також і деякі поля IP-заголовка, ESP обчислюється тільки по полях ESP-пакету за вирахуванням поля ICV. Перед обчисленням контрольної суми воно заповнюється нулями. Алгоритм обчислення ICV, як і в протоколі AH, передавальний IPsec-модуль дізнається із запису про SA, з яким пов'язаний пакет, що обробляється.

Обробка вхідних IPsec-пакетів

Після отримання пакета, що містить повідомлення ESP-протоколу, приймальний IPsec-модуль шукає відповідне захищене віртуальне з'єднання (SA) в SAD, використовуючи IP-адресу одержувача, протокол безпеки (ESP) та індекс SPI.

Якщо відповідний SA не знайдено, пакет знищується. Знайдене захищене віртуальне з'єднання (SA) вказує на те, чи використовується послуга запобігання повторній передачі пакетів, тобто на необхідність перевірки поля Sequence Number.

Якщо послуга використовується, поле перевіряється. Для цього, як і в AH, використовується метод ковзного вікна. Приймальний IPsec-модуль формує вікно із шириною W. Лівий край вікна відповідає мінімальному послідовному номеру (Sequence Number) N правильно прийнятого пакета. Пакет із полем Sequence Number, у якому міститься значення, починаючи від N+1 і закінчуючи N+W, приймається коректно.

Якщо отриманий пакет виявляється по ліву межу вікна, він знищується.

Потім, якщо використовується послуга автентифікації, приймальний IPsec-модуль обчислює ICV за відповідними полями прийнятого пакета, використовуючи алгоритм автентифікації, який він дізнається із запису про SA, і порівнює отриманий результат зі значенням ICV, розташованим у полі Integrity Check Value.

Якщо обчислене значення ICV збіглося з прийнятим, то пакет, що прийшов, вважається дійсним.

Якщо перевірка дала негативний результат, то пакет приймається знищується.

Далі проводиться розшифрування пакета. Приймальний IPsec-модуль дізнається із запису про SA, який алгоритм шифрування використовується та секретний ключ. Слід зазначити, що перевірка контрольної суми та процедура розшифрування можуть проводитися не тільки послідовно, а й паралельно. В останньому випадку процедура перевірки контрольної суми повинна закінчитися раніше за процедуру розшифрування, і якщо перевірка ICV провалилася, процедура розшифрування так само має припинитися.DOS-атаки).

Далі розшифроване повідомлення відповідно до поля *Next Header* передається для подальшої обробки.

IKE

IKE (вимовляється *айк*, аббр. від Internet Key Exchange) – протокол, що зв'язує всі компоненти IPsec в працююче ціле. Зокрема, IKE забезпечує початкову автентифікацію сторін, а також обмін спільними секретними ключами.

Існує можливість вручну встановити ключ сесії (не плутати з pre-shared key [PSK] для автентифікації). У цьому випадку IKE не використовується. Однак, цей варіант не рекомендується і використовується рідко. Традиційно IKE працює через порт 500 UDP.

Існує IKE і новіша версія протоколу: IKEv2. У специфікаціях та функціонуванні цих протоколів є деякі відмінності. IKEv2 визначає параметри з'єднання за одну фазу, що складається з декількох кроків. Процес роботи IKE можна розбити дві фази.

Перша фаза

IKE створює безпечний канал між двома вузлами, що називається IKE security association (IKE SA). Також у цій фазі два вузли узгодять сесійний ключ за алгоритмом Діффі-Хеллмана. Перша фаза IKE може проходити в одному з двох режимів:

– Основний режим

Складається з трьох двосторонніх обмінів між відправником та одержувачем:

1. Під час першого обміну узгоджуються алгоритми та ґеш-функції, які будуть використовуватися для захисту IKE з'єднання за допомогою зіставлення IKE SA кожного вузла.

2. Використовуючи алгоритм Діффі-Хеллмана, сторони обмінюються спільним секретним ключем. Також вузли перевіряють ідентифікацію один одного шляхом передачі та підтвердження послідовності псевдовипадкових чисел.

3. За зашифрованою IP-адресою перевіряється ідентичність протилежної сторони. В результаті виконання основного режиму створюється безпечний канал для наступного обміну ISAKMP (цей протокол визначає порядок дій для автентифікації з'єднання вузлів, створення та управління SA, генерації ключів, а також зменшення загроз, таких як DoS-атака або атака повторного відтворення).

– Агресивний режим

Цей режим обходиться меншою кількістю обмінів і, відповідно, кількістю пакетів. У першому повідомленні міститься практично вся потрібна для встановлення IKE SA інформація: відкритий ключ Діффі-Хеллмана для синхронізації пакетів, що підтверджується іншим учасником, ідентифікатор пакета. Одержувач посилає у відповідь усе, що треба завершення обміну. Першому вузлу потрібно лише підтвердити з'єднання.

З точки зору безпеки агресивний режим слабший, оскільки учасники починають обмінюватися інформацією до встановлення безпечного каналу, тому можливе несанкціоноване перехоплення даних. Однак цей режим швидше, ніж основний. За стандартом IKE будь-яка реалізація *має* підтримувати *основний режим*, а *агресивний режим* підтримувати вкрай бажано.

Друга фаза

У фазі два IKE існує лише один, швидкий режим. Швидкий режим виконується лише після створення безпечного каналу під час першої фази. Він узгодить загальну політику IPsec, отримує спільні секретні ключі для алгоритмів протоколів IPsec (AH чи ESP), встановлює IPsec SA. Використання послідовних номерів забезпечує захист від атак повторної передачі. Також швидкий режим використовується для перегляду поточної IPsec SA та вибору нової, коли час життя SA спливає. Стандартно швидкий режим здійснює оновлення загальних секретних ключів, використовуючи алгоритм Діффі-Хеллмана з першої фази.

Як працює IPsec

У роботі протоколів IPsec можна виділити п'ять етапів:

1. Перший етап починається зі створення на кожному вузлі, який підтримує стандарт IPsec, політики безпеки. На цьому етапі визначається, який трафік підлягає шифруванню, які функції та алгоритми можуть бути використані.

2. Другий етап є, за суттю, першою фазою IKE. Її мета – організувати безпечний канал між сторонами для другої фази IKE. На другому етапі виконуються:

– Автентифікація та захист ідентифікаційної інформації вузлів

– Перевірка відповідності політик IKE SA вузлів для безпечного обміну ключами

– Обмін Діффі-Хеллмана, в результаті якого у кожного вузла буде спільний секретний ключ

– Створення безпечного каналу для другої фази IKE

3. Третій етап є другою фазою IKE. Його завданням є створення IPsec-тунелю. На третьому етапі виконуються такі функції:

– Узгоджуються параметри IPsec SA по каналу, що захищається IKE SA, створеному в першій фазі IKE

– Встановлюється IPsec SA

– Періодично здійснюється перегляд IPsec SA, щоб переконатися у її безпеці

– (Опціонально) виконується додатковий обмін Діффі-Хеллмана

4. Робочий етап. Після створення IPsec SA починається обмін інформацією між вузлами через IPsec-тунель, використовуються протоколи та параметри, встановлені SA.

5. Припиняють діяти поточні IPsec SA. Це відбувається при їх видаленні або при закінченні часу життя (певне SA в байтах інформації, що передається через канал, або в секундах), значення якого міститься в SAD на кожному вузлі. Якщо потрібно продовжити передачу, запускається фаза два IKE (якщо потрібно, то і перша фаза) і далі створюються нові IPsec SA. Процес створення нових SA може відбуватися і до завершення дії поточних, якщо потрібна безперервна передача даних.

Використання

Протокол IPsec використовується в основному для організації VPN-тунелів. У цьому випадку протоколи ESP та AH працюють у режимі тунелювання. Крім того, встановлюючи політики безпеки певним чином, протокол можна використовувати для створення міжмережевого екрану. Сенс міжмережевого екрану полягає в тому, що він контролює і фільтрує пакети, що проходять через нього, відповідно до заданих правил. Встановлюється набір правил, і екран переглядає всі пакети, що проходять через нього. Якщо пакети, що передаються, потрапляють під дію цих правил, міжмережевий екран обробляє їх відповідним чином. Наприклад, він може відхиляти певні пакети, тим самим уриваючи небезпечні з'єднання. Налаштувавши політику безпеки відповідно, можна, наприклад, заборонити веб-трафік. Для цього достатньо заборонити відсилання пакетів, в які вкладаються повідомлення HTTP і HTTPS. IPsec можна використовувати й захисту серверів – для цього відкидаються всі пакети, крім пакетів, необхідні коректного виконання функцій сервера. Наприклад, для Web-сервера можна блокувати весь трафік, за винятком з'єднань через 80-й порт TCP або через порт TCP 443 у випадках, коли застосовується HTTPS.

Приклад:

За допомогою IPsec тут забезпечується безпечний доступ користувачів до сервера. При використанні протоколу ESP всі звернення до сервера та його відповіді шифруються. Однак за VPN-шлюзом (в домені шифрування) надсилаються відкриті повідомлення.

Інші приклади використання IPsec:

– шифрування трафіку між файловим сервером та комп'ютерами у локальній мережі, використовуючи IPsec у транспортному режимі;

– з'єднання двох офісів із використанням IPsec у тунельному режимі.

19.2. Протоколи безпечної передачі даних прикладного рівня: https

HTTPS (аббр. від англ. *HyperText Transfer Protocol Secure*) – розширення протоколу HTTP для підтримки шифрування з метою підвищення безпеки. Дані в протоколі HTTPS передаються поверх криптографічних протоколів TLS або SSL застарілого в 2015 році. На відміну від HTTP з TCP – портом 80, для HTTPS за замовчуванням використовується TCP-порт 443.

HTTP (англ. *HyperText Transfer Protocol* – "протокол передачі гіпертексту") – протокол прикладного рівня передачі даних, спочатку – у вигляді гіпертекстових документів у форматі HTML, в даний час використовується для передачі довільних даних.

Принцип роботи

HTTPS не є окремим протоколом. Це звичайний HTTP, що працює через шифровані транспортні механізми SSL та TLS. Він забезпечує захист від атак, заснованих на прослуховуванні мережного з'єднання – від сніфферських атак і атак типу man-in-the-middle, за умови, що будуть використовуватися шифруючі засоби та *сертифікат сервера перевірений і йому довіряють.*

За умовчанням **HTTPS URL** використовує **443 TCP –** порт (для незахищеного HTTP – 80). Щоб підготувати веб-сервер для обробки https-з'єднань, адміністратор повинен отримати та встановити сертифікат відкритого та закритого ключа для цього веб-сервера. У **TLS** використовується як асиметрична схема шифрування (для вироблення загального секретного ключа), так і симетрична (для обміну даними, зашифрованими загальним ключем). Сертифікат відкритого ключа підтверджує належність цього відкритого ключа власнику сайту. Сертифікат відкритого ключа та сам відкритий ключ надсилаються клієнту під час встановлення з'єднання; закритий ключ використовується для розшифровування повідомлень від клієнта.

Існує можливість створити такий сертифікат, не звертаючись до центру сертифікації. Підписуються такі сертифікати тим самим сертифікатом і називаються самопідписаними (*self-signed*). Без перевірки сертифіката якимось іншим способом (наприклад, дзвінок власнику та перевірка контрольної суми сертифіката) таке використання HTTPS піддається атаці посередника.

Ця система також може використовуватися для автентифікації клієнта, щоб забезпечити доступ до сервера лише авторизованим користувачам. Для цього адміністратор зазвичай створює сертифікати для кожного користувача та завантажує їх у браузер кожного користувача. Також прийматимуться всі сертифікати, підписані організаціями, яким довіряє сервер. Такий сертифікат зазвичай містить ім'я та адресу електронної пошти авторизованого користувача, які перевіряються під час кожного з'єднання, щоб перевірити особу користувача без введення пароля.

У HTTPS для шифрування використовується довжина ключа 40, 56, 128 чи 256 біт. Деякі старі версії браузерів використовують довжину ключа 40 біт

(наприклад, IE версій до 4.0), що пов'язано з експортними обмеженнями в США. Довжина ключа 40 біт не є надійною. Багато сучасних сайтів вимагають використання нових версій браузерів, що підтримують шифрування з довжиною ключа 128 біт, щоб забезпечити достатній рівень безпеки. Шифрування з довжиною ключа 128 біт значно ускладнює підбір паролів та доступ до особистої інформації.

Традиційно на одній IP-адресі може працювати лише один HTTPS-сайт. Для роботи кількох HTTPS-сайтів із різними сертифікатами застосовується розширення TLS під назвою Server Name Indication (SNI).

Ідентифікація в HTTPS

Ідентифікація сервера

HTTP/TLS запити генеруються шляхом розіменування URI, внаслідок чого ім'я хоста стає відоме клієнту. На початку спілкування сервер посилає клієнту свій сертифікат, щоб клієнт ідентифікував його. Це дозволяє запобігти атаці посередника. У сертифікаті вказується сервер URI. Узгодження імені хоста та даних, зазначених у сертифікаті, відбувається відповідно до протоколу RFC2459.

Якщо ім'я сервера не співпадає із зазначеним у сертифікаті, то програми користувача, наприклад браузери, повідомляють про це користувачеві. В основному браузери надають користувачеві вибір: продовжити незахищене з'єднання або перервати його.

Ідентифікація клієнта

Зазвичай сервер не має інформації про клієнта, достатньої для його ідентифікації. Однак для забезпечення підвищеної захищеності з'єднання використовується так звана 2-way authentication. При цьому сервер після підтвердження сертифіката клієнтом також запитує сертифікат. Таким чином, схема підтвердження клієнта аналогічна ідентифікації сервера.

Уразливості HTTPS

Спільне використання HTTP та HTTPS

Коли сайти використовують змішану функціональність HTTP та HTTPS, це потенційно призводить до інформаційної загрози для користувача. Наприклад, якщо основні сторінки сайту завантажуються, використовуючи HTTPS, а CSS і JavaScript завантажуються по HTTP, то зловмисник у момент завантаження останніх може підвантажити свій код і отримати дані HTML-сторінки. Багато сайтів, незважаючи на такі вразливості, завантажують контент через інші сервіси, які не підтримують HTTPS. Механізм HSTS дозволяє запобігти подібним уразливості, змушуючи примусово використовувати HTTPS з'єднання навіть там, де за умовчанням використовується HTTP.

Атаки з використанням аналізу трафіку

У HTTPS було виявлено уразливості, пов'язані з аналізом трафіку. Атака з аналізом трафіку – це тип атаки, при якій виводяться властивості захищених даних каналу шляхом вимірювання розміру трафіку та часу передачі повідомлень у ньому. Аналіз трафіку можливий, оскільки шифрування SSL/TLS змінює вміст трафіку, але мінімально впливає на розмір і час проходження трафіку. У травні 2010 року дослідники з Microsoft Research та Університету

Індіани виявили, що докладні конфіденційні дані користувача можуть бути отримані з другорядних даних, таких, наприклад, як розміри пакетів. Аналізатор трафіку зміг отримати історію хвороб, дані про медикаменти і проведені операції користувача, дані про сімейний дохід та ін.

Атака людина в середині (атака посередника)

При **«атаці людина в середині (атаці посередника)»** використовується те, що сервер HTTPS надсилає сертифікат з відкритим ключем до браузера. Якщо цей сертифікат не заслуговує на довіру, то канал передачі буде вразливим для атаки зловмисника. Така атака замінює оригінальний сертифікат, що засвідчує HTTPS-сервер модифікованим сертифікатом. Атака проходить успішно, якщо користувач нехтує подвійною перевіркою сертифіката, коли браузер надсилає попередження. Це особливо поширене серед користувачів, які часто стикаються із самозавіреними сертифікатами при доступі до сайтів усередині мережі приватних організацій.

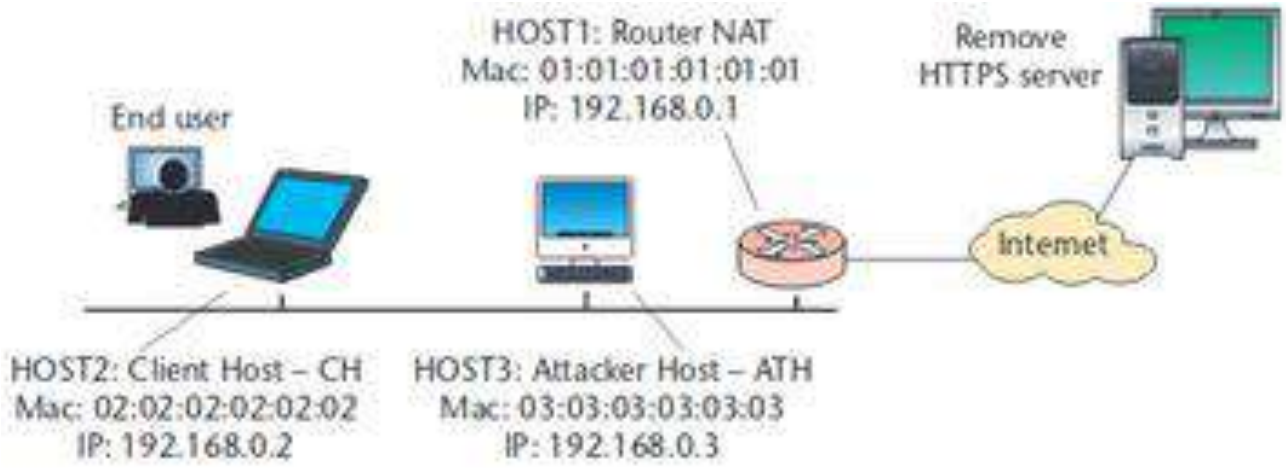


Рисунок 19.3 – Стандартна конфігурація мережі. Користувач на хості клієнта (CH) хоче здійснити безпечну транзакцію, але вразливий для атаки "**людина в середині**".

На рис. 19.3 представлена ситуація, коли зловмисник є шлюзом між клієнтом, який здійснює безпечну транзакцію, та сервером. Таким чином, через зловмисника проходить весь трафік клієнта і він може перенаправити його на свій розсуд. Тут робляться такі кроки:

1. Зловмисник вбудовується між клієнтом та сервером.
2. Пересилає всі повідомлення від клієнта серверу без змін.
3. Перехоплення повідомлень від сервера, надісланих за шлюзом за замовчуванням.
4. Створення самозавіреного сертифіката та заміна ним сертифіката сервера.
5. Надсилання помилкового сертифіката клієнту.
6. Коли клієнт підтвердить сертифікат, буде встановлено захищені з'єднання: між зловмисником і сервером та інше між зловмисником і клієнтом.

В результаті такої атаки клієнт і сервер думають, що здійснюють безпечне з'єднання, проте зловмисник тепер також має закритий ключ і може розшифрувати будь-яке повідомлення в каналі.

Розділ 20. Цифрова стеганографія.

20.1. Поняття цифрової стеганографії.
20.2. Модель стеганосистеми та класифікація методів стеганографічного захисту
20.3. Основні вимоги до стеганосистеми.
20.3. Відкриті, напівзакриті, закриті стеганосистеми.
20.4. Поняття ЦВЗ, класифікація.
20.5. Метод модифікації найменшого значущого біта та інші методи приховання даних у зображенні, відео та аудіо.
20.6. Атаки на стеганосистеми.

20.1. Поняття цифрової стеганографії

Стеганографія – (греч. steganos – таємниця, секрет; graphy – запис, тобто тайнопис) набір засобів і методів приховання факту передачі повідомлення.

Стеганографія приховує сам факт передачі повідомлення, а криптографія вважає, що повідомлення (у шифрованому виді) доступно незаконному користувачеві, але він не може витягти із цього повідомлення інформацію, яка захищена.

Перші сліди стеганографічних методів губляться в далекій давнині. Відомий такий спосіб приховання письмового повідомлення: рабу голили голову, на шкірі писали повідомлення й після відростання волосу раба відправляли до адресата. Відомі різні способи схованого листа серед рядків звичайного, незахищеного листа: від молока до складних хімічних реактивів з наступною обробкою.

У цей час розвиваються методи *комп'ютерної стеганографії* – самостійного наукового напрямку інформаційної безпеки, що вивчає проблеми створення компонентів приховуваної інформації у відкритому інформаційному середовищі, що може бути сформована обчислювальними системами й мережами.

Цифрова стеганографія – напрям класичної стеганографії, заснований на прихованні або впровадження додаткової інформації в цифрові об'єкти, викликаючи деякі спотворення цих об'єктів. Але, як правило, дані об'єкти є мультимедіа-об'єктами (зображення, відео, аудіо, текстури 3D-об'єктів) і внесення спотворень, що знаходяться нижче за поріг чутливості середньостатистичної людини, не призводить до помітних змін цих об'єктів. Крім того, в оцифрованих об'єктах, що спочатку мають аналогову природу, завжди присутній шум квантування; Далі, при відтворенні цих об'єктів з'являється додатковий аналоговий шум і нелінійні спотворення апаратури, все це сприяє більшій непомітності прихованої інформації.

Цифрова стеганографія – раніше малодосліджена область захисту інформації, яка стрімко почала розвиватися в останні десятиріччя. Вона використовується для наступних цілей:

1. Вбудовування інформації з метою її прихованої передачі:

– використання спецслужбами для зв'язку з агентами без дипломатичного прикриття за рубежем;

– використання терористичними організаціями для передачі схованих повідомлень у кіберпросторі;

– використання фізичними і юридичними особами для приховування конфіденційної інформації.

2. Вбудовування цифрових водяних знаків (watermarking):

– для систем захисту авторських прав і DRM систем;

– у якості аналогового ЕЦП, забезпечуючи зберігання інформації про переданий підпис і спроби порушення цілісності контейнера.

3. Вбудовування ідентифікаційних номерів (fingerprinting), наприклад, у програмних продуктах, у системах цифрового друку й т.д.

4. Вбудовування заголовків (captioning), наприклад, у медичних картах, у системах цифрового друку й т.д.

При поєднанні з криптографією, стеганографія дозволяє значно підвищити захист інформації від несанкціонованого доступу.

20.2. Модель стеганосистеми та класифікація методів стеганографічного захисту

Модель стеганосистеми

Основними стеганографічними поняттями є повідомлення і контейнер.

Повідомленням $m \in M$, називають секретну інформацію, наявність якої необхідно приховати, де M – множина всіх повідомлень, зазвичай $M = Z^{2n}$ для $n \in Z$.

Контейнером $b \in B$ називають несекретну інформацію, яку використовують для приховування повідомлень, де B – безліч всіх контейнерів, зазвичай $B = Z^{2q}$, при цьому $q >> n$.

Порожній контейнер (контейнер-оригінал) – це контейнер b, що не містить повідомлення.

Заповнений контейнер (контейнер-результат) b_m – це контейнер b, що містить повідомлення m.

Стеганографічні перетворенням прийнято називати залежності:

$$F: M \times B \times K \to B,\ F^{-1}: B \times K \to M,$$

які зіставляють трійці (повідомлення, порожній контейнер, ключ) контейнер-результат, і пари (заповнений контейнер, ключ) вихідне повідомлення, тобто:

$$F(m, b, k) = b_m,\ k,\ F^{-1}(b_m, k) = m, \text{ де } m \in M,\ b, b_m \in B,\ k \in K$$

Стеганографічної системою називають (F, F^{-1}, M, B, K) сукупність повідомлень, контейнерів перетворень що їх зв’язують.

Контейнери бувають двох типів: потокові та фіксовані:

– Потокові контейнери – це послідовність бітів, яка постійно змінюється. Повідомлення вбудовується у нього в реальному режимі часу, тому заздалегідь невідомо, чи вистачить розміру даного контейнера для передачі повідомлення повністю.

– Фіксовані контейнери мають фіксований розмір, тому є можливість обрати оптимальний контейнер для передачі повідомлення. Розмір контейнера повинен, принаймні, у декілька разів перевищувати розмір повідомлення, і, чим більше дане співвідношення, тим надійніше приховане повідомлення. Для підвищення рівня захищеності секретної інформації повідомлення можна попередньо зашифрувати стійким криптографічним алгоритмом. Також часто використовується завадостійке кодування.

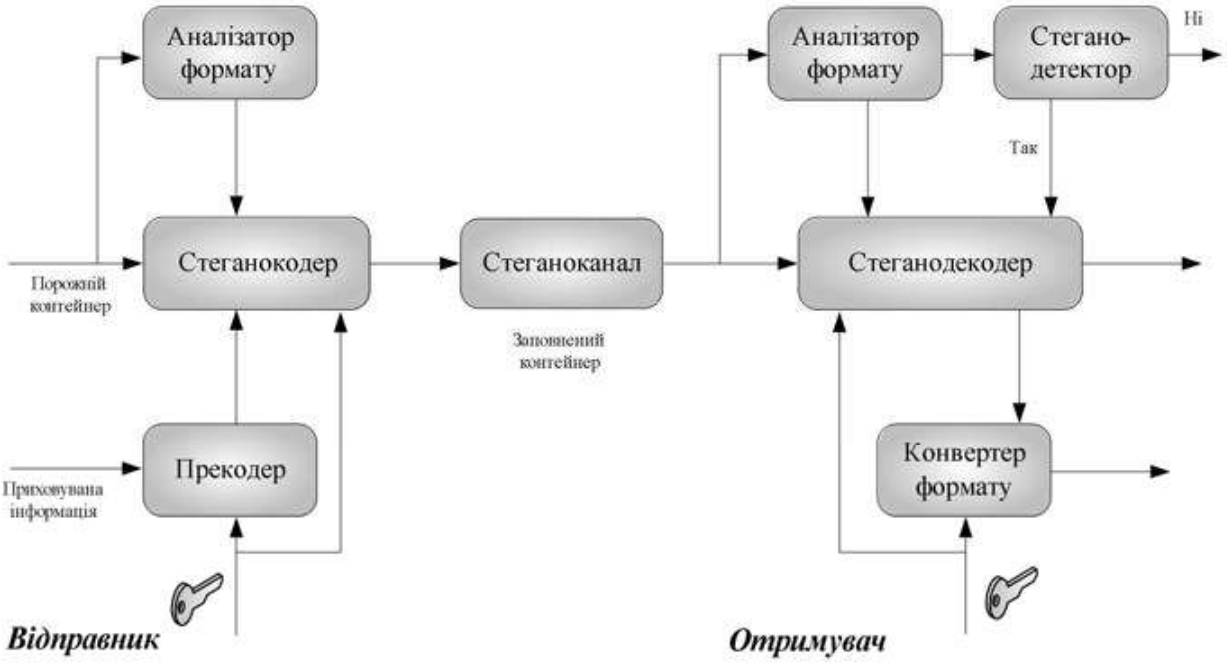


Рисунок 20.1 – Структурна схема типової стеганосистеми

Сучасне застосування стеганографії:

– вбудовування інформації з метою сховати незаконну передачу;

– захист інформації від несанкціонованого доступу;

– вбудовування цифрових водяних знаків для захисту авторських прав (watermarking);

– вбудовування ідентифікаційних номерів (fingerprinting);

– вбудовування заголовків (captioning).

– камуфляж програмного забезпечення;

Цифрові водяні знаки **(ЦВЗ)** застосовуються для захисту від копіювання й несанкціонованого використання мультимедійної інформації й полягає у вбудовуванні в об’єкт, який захищається, невидимих міток – ЦВЗ. ЦВЗ можуть містити деякий автентичний код, інформацію про власника, або яку-небудь керуючу інформацію. Найбільш підходящими об'єктами захисту за допомогою ЦВЗ є нерухливі зображення, файли аудио й відеоданих.

Технологія ***вбудовування ідентифікаційних номерів*** виробників має багато загального з технологією ЦВЗ. Відмінність полягає в тім, що в першому випадку кожна захищена копія має свій унікально вбудовуваний номер, (звідси й назва – дослівно «відбитки пальців»). Цей ідентифікаційний номер дозволяє виробникові відслідковувати подальшу долю свого дітища: чи не зайнявся хто-небудь із покупців незаконним тиражуванням. Якщо так, то «відбитки пальців» швидко вкажуть на винного.

Вбудовування заголовків **(невидиме)** може застосовуватися, наприклад, для підпису медичних знімків, нанесення легенди на карту й т.і. Метою є зберігання різнорідно представленої інформації в єдиному цілому. Це, мабуть, єдиний додаток стеганографії, де в явному виді відсутній порушник.

Нерідко методи стеганографії використовують для ***камуфлювання програмного забезпечення.*** У тих випадках, коли використання програм незареєстрованними користувачами є небажаним, воно може бути закамуфльоване під стандартні універсальні програмні продукти (наприклад, текстові редактори) або приховано у файлах мультимедіа (наприклад, у звуковому супроводі комп'ютерних ігор).

Класифікація стеганографічних **методів**

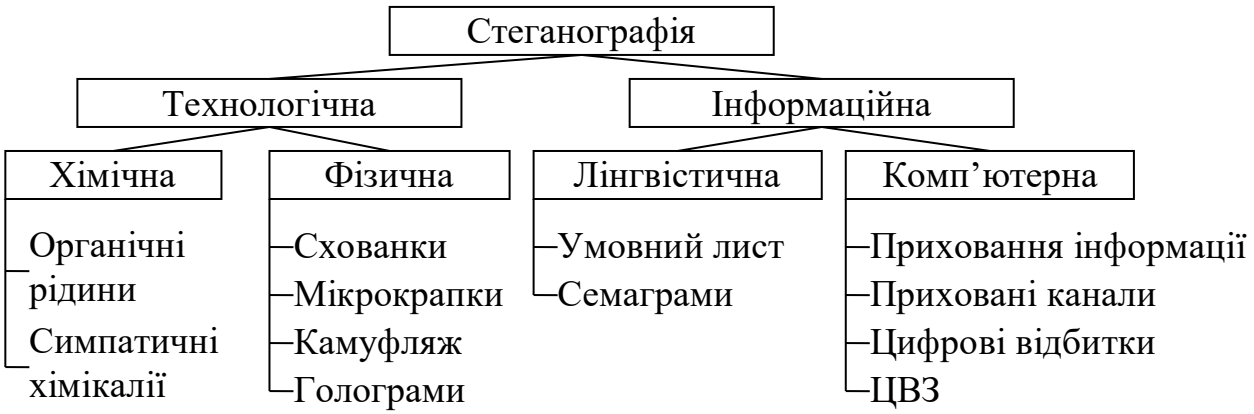


Рисунок 20.2 – Класифікація методів стеганографічного захисту

У сучасній стеганографії, у цілому, можна виділити в напрямки: ***технологічну стеганографію*** й ***інформаційну стеганографію*** (рисунок 20.2).

Технологічна стеганографія

До методів ***технологічної стеганографії*** ставляться методи, які засновані на використанні хімічних або фізичних властивостей різних матеріальних носіїв інформації.

Хімічні методи стеганографії зводиться майже винятково до застосування невидимого чорнила, до яких ставляться органічні рідини й симпатичні хімікалії.

До фізичних методів можна віднести мікрокрапки, різного виду схованки й методи камуфляжу. У цей час фізичні методи становлять інтерес в області дослідження різний носіїв інформації з метою запису на них даних, які б не виявлялися звичайними методами зчитування. Особливий інтерес є до стандартних носіїв інформації засобів обчислювальної, аудіо й відео техніки. Крім цього, з'явився цілий ряд нових технологій, які, базуючись на традиційної стеганографії, використовують останні досягнення мікроелектроніки (голограми, кинеграми).

Інформаційна стеганографія

До ***інформаційного стеганографії*** можна віднести методи ***лінгвістичної й комп'ютерної стеганографії***.

Лінгвістичні методи стеганографії підрозділяються на дві основні категорії:

– умовний лист;

– семаграми.

Існують три види *умовного листа*: *жаргонний код, пустишечний шифр* і *геометрична система*:

– *Жаргонний код* – зовні необразливе слово має зовсім інше реальне значення, а текст складається так, щоб виглядати як можна більш безневинно й правдоподібно.

– *Пустишечний шифр* – у тексті мають значення лише деякі певні букви або слова.

– *Геометрична форма* – при її застосуванні слова, що мають значення, розташовуються на сторінці в певних місцях або в крапках перетинання геометричної фігури заданого розміру.

Семаграми – таємні повідомлення, у яких шифропозаченням є будь-які символи, крім букв і цифр. Ці повідомлення можуть бути передані, наприклад, у рисунку, що містить крапки й тирі для читання за кодом Морзе.

Комп'ютерна стеганографія – сукупність стеганографічних методів, які реалізуються на основі комп'ютерної техніки й програмного забезпечення в рамках окремих обчислювальних або керуючих систем, корпоративних або глобальних обчислювальних мереж.

При використанні методів комп'ютерної стеганографії повинні враховуватися наступні умови:

– супротивник може мати повне подання про стеганографичну систему й деталі її реалізації. Єдиною інформацією, що повинна залишатися йому невідомою, – це ключ, за допомогою якого можна встановити факт присутності схованого повідомлення і його зміст;

– якщо супротивникові якимось образом удалося довідатися про факт існування схованого повідомлення, то це не повинне дозволити йому витягти подібні повідомлення з інших стеганограм доти, поки ключ зберігається в таємниці;

– потенційний супротивник повинен бути позбавлений яких-небудь технічних і інших переваг у розпізнаванні або розкритті змісту таємних повідомлень.

Нижче буде обговорено **основні теоретичні положення комп'ютерної стеганографії й розглянуті деякі методи приховання даних в інформаційному середовищі,** що може бути підтримана обчислювальними системами й мережами.

Класифікація стегосистем

За аналогією із криптографічними системами, у стеганографії розрізняють ***системи із секретним ключем*** і ***системи з відкритим ключем***.

У стеганографічній системі із *секретним ключем* використовується один ключ, що повинен бути заздалегідь відомий абонентам до початку схованого обміну секретними повідомленнями або пересланий по захищеному каналу.

У стегосистемі з *відкритим ключем* для вбудовування й добування таємного повідомлення використовуються різні ключі, причому вивести один ключ із іншого за допомогою обчислень неможливо. Один із ключів (відкритий) може передаватися вільно по незахищеному каналу зв'язку, а другий, секретний ключ, – по захищеному каналу. Дана схема добре працює при взаємній недовірі відправника й одержувача.

З огляду на все різноманіття стеганографічних систем, зведемо їх до наступних типів: ***безключових стегосистем***, ***систем із секретним ключем***, ***систем з відкритим ключем*** і ***змішаних стегосистем***.

Безключові стегосистем

Для функціонування *безключових стегосистем* не потрібно ніяких додаткових даних у вигляді стегоключа крім алгоритму стеганографічного перетворення.

Безпека безключових стегосистем заснована на таємності використовуваних стеганографічних перетворень. Це суперечить основному принципу Керкхоффса для систем захисту інформації. Найчастіше для підвищення безпеки безключових систем, перед початком процесу стеганографічного приховання попередньо виконується шифрування приховуваної інформації. Ясно, що такий підхід збільшує захищеність усього процесу зв'язку, оскільки це ускладнює виявлення схованого повідомлення. Однак, “сильні” стеганографічні системи, як правило, не мають потреби в попередньому шифруванні приховуваних повідомлень.

Стегосистеми із секретним ключем

Дотримуючись закону Керкхоффса, безпека системи повинна ґрунтуватися на деякій секретній інформації, без знання якої не можна витягти з контейнера секретну інформацію. У стегосистемах така інформація називається ***стегоключем***. Відправник, вбудовуючи секретне повідомлення в обраний

контейнер **C**, використовує секретний стегоключ **k**. Якщо використовуваний у стеганографическом перетворенні ключ **k** відомий одержувачеві, то він зможе витягти сховане повідомлення з контейнера. Без знання такого ключа будь-який інший користувач цього зробити не зможе.

Даний тип стегосистем припускає наявність безпечного каналу для обміну стегоключами.

Іноді стегоключ **k** обчислюють за допомогою секретної ґеш-функції **Hash**, використовуючи деякі характерні риси контейнера: **k = Hash** (особливості контейнера). Якщо стеганографічне перетворення **E** не змінює в результуючій стеганограмі обрані особливості контейнера, то одержувач також зможе обчислити стегоключ (хоча й у цьому випадку захист залежить від таємності функції Hash, і таким чином, знову порушується принцип Керкхоффса). Очевидно, що для досягнення адекватного рівня захисту, таку особливість у контейнері необхідно вибирати дуже акуратно.

У деяких алгоритмах при добуванні схованої інформації додатково потрібні відомості про вихідний контейнер або деякі інші дані, які відсутні у стеганограмі. Такі системи становлять обмежений інтерес, оскільки вони вимагають передачі первісного виду контейнера, що еквівалентно традиційній задачі ключового обміну. Подібні алгоритми можуть бути відзначені як окремий випадок стегосистем із секретним ключем, у яких **K=C** або **K=C×K'**, де **K'** – означає додатковий набір секретних ключів.

Стегосистеми з відкритим ключем

Стеганографічні системи з відкритим ключем не мають потреби в додатковому каналі ключового обміну. Для їхнього функціонування необхідно мати два стегоключі: один секретний, котрий користувачі повинен зберігати в таємниці, а другий – відкритий, котрий зберігається в доступному для всіх місці. При цьому відкритий ключ використовується в процесі приховання інформації, а секретний – для її добування.

Стегосистеми з відкритими ключами використовують той факт, що функція добування схованої інформації **D** може бути застосовна до будь-якого контейнера поза залежністю від того, чи перебуває в ньому сховане чи повідомлення ні. Якщо в контейнері відсутнє сховане повідомлення, то завжди буде відновлюватися деяка випадкова послідовність. Якщо ця послідовність статистично не відрізняється від шифртекста криптосистеми з відкритим ключем, тоді в безпечній стегосистемі можна приховувати отриманий у такий спосіб шифртекст, а не відкритий.

Класифікація методів приховання інформації

Більшість методів комп'ютерної стеганографії базується на наступних принципах.

– Перший полягає в тому, що файли, які не вимагають абсолютної точності (наприклад, файли із зображенням, звуковою інформацією та ін.), можуть бути до певного ступеня видозмінені без втрати функціональності.

– Другий принцип заснований на відсутності спеціального інструментарію або нездатності органів почуттів людини надійно розрізняти незначні зміни в таких вихідних файлах.

Для методів комп'ютерної стеганографії можна ввести певну класифікацію (рисунок 20.3).

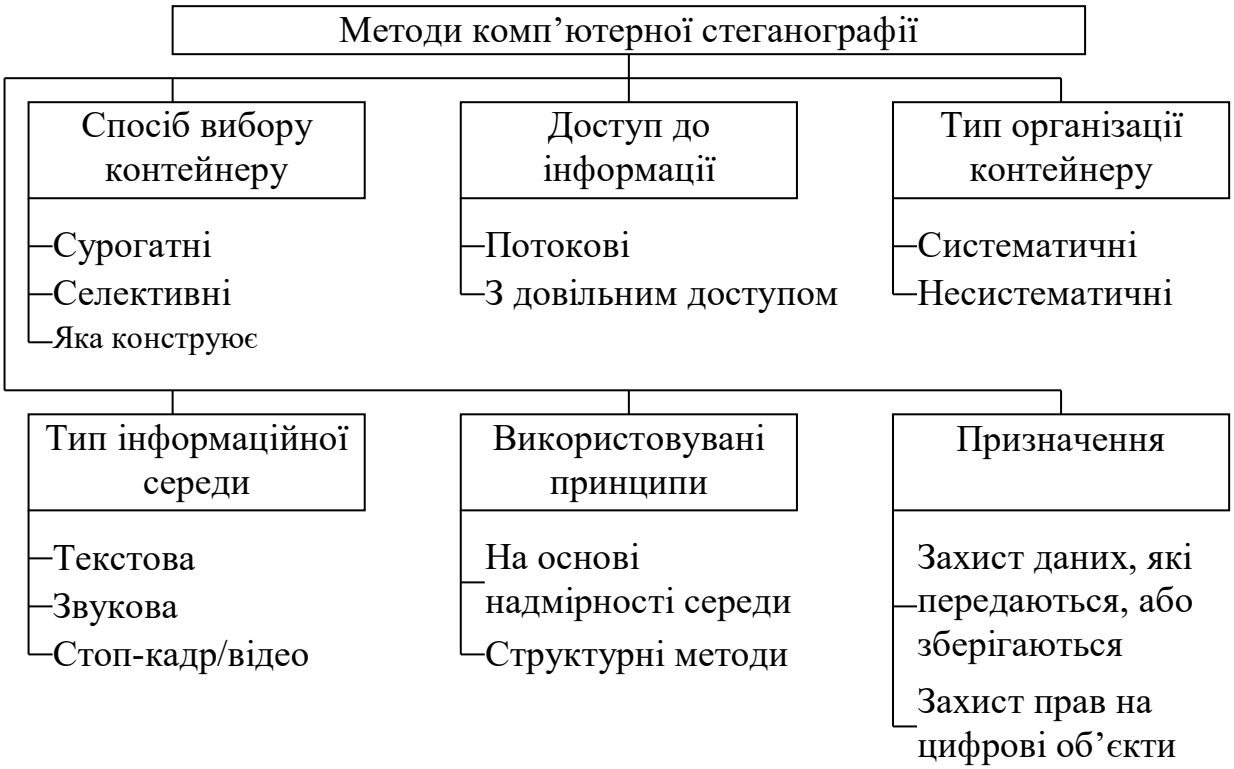


Рисунок 20.3 – Класифікація методів приховання інформації

За способом відбору контейнера розрізняють методи *сурогатної стеганографії, селективної стеганографії* й *стеганографії, яка конструює*.

У методах *сурогатної (безальтернативної) стеганографії* відсутня можливість вибору контейнера й для приховання повідомлення вибирається перший контейнер, що попався.

У методах *селективної стеганографії* передбачається, що заховане повідомлення повинне відтворювати спеціальні статистичні характеристики шуму контейнера. Для цього генерують велику кількість альтернативних контейнерів, щоб потім вибрати найбільш підходящий з них для конкретного повідомлення. Частковим випадком такого підходу є обчислення деякої ґеш-функції для кожного контейнера. При цьому для приховання повідомлення вибирається той контейнер, ґеш-функція якого збігається зі значенням ґеш-функції повідомлення (тобто стеганограмою є обраний контейнер).

У методах стеганографії, *яка конструює* контейнер генерується самою стегосистемою. Тут може бути кілька варіантів реалізації. Так, наприклад, шум контейнера може моделюватися приховуваним повідомленням. Це реалізується за допомогою процедур, які не тільки кодують приховуване повідомлення під шум, але й зберігають модель первісного шуму. У граничному випадку по моделі

шуму може будуватися ціле повідомлення. Прикладами можуть служити метод, що реалізований у програмі MandelSteg, де як контейнер для вбудовування повідомлення генерується фрактал Мандельброта, або ж апарат *функцій імітації* (mumic function).

За способом доступу до приховуваної інформації розрізняють методи для *потокових* (безперервних) контейнерів і методи для контейнерів *з довільним доступом* (обмеженої довжини).

Методи, що використовують потокові контейнери, працюють із потоками безперервних даних (наприклад, інтернет-телефонія). У цьому випадку приховувані біти необхідно в режимі реального часу включати в інформаційний потік.

Методи, які використовуються для контейнерів з довільним доступом, призначені для роботи з файлами фіксованої довжини (текстова інформація, програми, графічні або звукові файли).

За типом організації контейнери, подібно перешкодозахищеним кодам, можуть бути *систематичними* й *несистематичними*. *У систематично організованих контейнерах* можна вказати конкретні місця стеганограми, де перебувають інформаційні біти самого контейнера, а де – шумові біти, призначені для приховуваної інформації (як, наприклад, у широко розповсюдженому методі найменшого значущого біта). *При несистематичній організації контейнера* такого поділу зробити не можна. У цьому випадку для виділення схованої інформації необхідно обробляти вміст всієї стеганограми.

За використовуваними принципами стеганометоди можна розбити на два класи: *цифрові* методи й *структурні* методи. Якщо *цифрові методи* стеганографії, використовуючи надмірність інформаційного середовища, в основному, маніпулюють із цифровим поданням елементів середовища, куди впроваджуються приховувані дані (наприклад, у пікселі, у різні коефіцієнти косинусних перетворень, перетворень Фур'є, Уолша-Радемахера або Лапласа), то *структурні методи* стеганографії для приховання даних використовують семантично значимі структурні елементи інформаційного середовища.

Основним напрямком комп'ютерної стеганографії є використання властивостей надмірності інформаційного середовища. Варто врахувати, що при прихованні інформації відбувається перекручування деяких статистичних властивостей середовища або порушення її структури, які необхідно враховувати для зменшення демаскуючих ознак.

В особливу групу можна також виділити ***методи, які використовують спеціальні властивості форматів подання файлів***:

– зарезервовані для розширення поля комп'ютерних форматів файлів, які звичайно заповнюються нулями й не враховуються програмою;

– спеціальне форматування даних (зсув слів, пропозицій, абзаців або вибір певних позицій букв);

– використання незадіяних місць на магнітних носіях;

– видалення ідентифікуючих заголовків для файлу.

В основному, для таких методів характерний низький ступінь скритності, низька пропускна здатність і слабка продуктивність.

За призначенням розрізняють стеганографічні методи властиво для схованої передачі або схованого зберігання даних і методи для приховання даних у цифрових об'єктах з метою захисту самих цифрових об'єктів.

За типом інформаційного середовища виділяються стеганографічні методи для текстового середовища, для аудіо середовища, а також для зображень (стоп-кадрів) і відео середовища.

Текстові стеганографи

Рідко використовуються Так як текст містить малу кількість надлишкової інформації, яку можна використовувати для приховання даних.

Можна виділити наступні методи, які зустрічаються в сучасних лінгвістичних стеганографах:

– методи перекручування формату текстового документа;

– синтаксичні методи;

– семантичні методи;

– методи генерації стеганограм за допомогою приховуваного повідомлення.

Методи перекручування формату текстового документа

Дані методи маніпулюють інтервалами між словами й пропозиціями або ж пробілами наприкінці текстових рядків. Приклад – використання пробілів. Один додатковий пробіл кодує значення біта “0”, а два – “1. Приклад приховання бітового повідомлення 0110100011010110: У_людини__набаго__більше_ворогів_таємних_ніж_явних.__Сховану_ворожне чу__частіше_усього_породжує__заздрість._Заздрість__викликають_розум,_вро да,_заможність_та__здоров’я._Ви__будете__мати_мало_ворогів__й__знати__їх до__обличчя,__якщо_позбавлені__усіх__цих_вдач.

Синтаксичні методи

До синтаксичних методів лінгвістичної стеганографії відносяться методи зміни пунктуації й методи зміни стилю й структури тексту.

У будь-якій мові існують випадки, коли правила пунктуації є неоднозначними й мають слабкий вплив на зміст тексту. Наприклад, обидві форми перерахування “хліб, масло й молоко” і “хліб, масло, молоко” є припустимими. Можна використовувати той факт, що вибір таких форм є довільним і використовувати альтернативний вибір для кодування даних у двійковому виді. Наприклад, якщо з'являється форма перерахування із союзом “і”, те кодується 1, інакше – 0. Для приховання можна також застосовувати скорочення й абревіатури.

Семантичні методи

Використовуються таблиці синонімів. Кодування секретного повідомлення проводиться вибором синоніма з необхідного місця таблиці. Наприклад, першому слову-синоніму відповідає 1, а другому – 0 (табл. 20.1). Якщо слову відповідає велика кількість синонімів, то можна кодувати більша кількість біт одночасно.

Фрагмент таблиці синонімів

1	0
слід	відбиток
дірка	отвір
оборона	захист
овація	оплески

Методи генерації стеганограм

На відміну від розглянутих вище стеганометодів, де приховувана інформація впроваджується в текстовий контейнер, існують методи, які повністю породжують стеганограмму на основі даних, що захищаються. У таких методах секретна інформація не впроваджується в текст, а представляється повністю всією стеганограмою. Теоретичну основу для методів генерації стеганограм розробив П. Вайнер у теорії функцій імітації. У стеганографії функції імітації застосовуються для того, щоб сховати ідентичність повідомлення шляхом зміни його статистичних властивостей.

Можна запропонувати кілька типів функції імітації, які, залежно від складності, моделюються регулярною, контекстно-вільною або рекурсивно-рахунковою граматиками. Стеганографічні перетворення першого типу описуються в термінах процедур стиску інформації; другого – контекстно-вільними граматиками, у яких приховувані біти управляють несуперечливими продукціями; для опису функцій третього типу застосовується апарат машин Тьюринга.

Регулярні функції імітації можна змоделювати за допомогою схеми кодування за Хаффманом.

Регулярні функції імітації створюють стеганограми, які мають заданий статистичний розподіл символів, однак при цьому ігнорується семантика отриманого тексту. Для людини такі тексти виглядають повною нісенітницею із граматичними помилками й помилками. Для генерування більше осмислених текстів використовуються контекстно-вільні граматики (КВГ).

20.3. Основні вимоги до стеганосистеми

Для того щоб стегосистема була надійною, необхідне виконання при її проектуванні низки вимог:

– Безпека системи має повністю визначатися секретністю ключа. Це означає, що порушник може повністю знати всі алгоритми роботи стегосистеми та статистичні характеристики множин повідомлень та контейнерів, і це не дасть

йому жодної додаткової інформації про наявність або відсутність повідомлення у цьому контейнері.

– Знання порушником факту наявності повідомлення у будь-якому контейнері не повинно допомогти йому при виявленні повідомлень в інших контейнерах.

– Заповнений контейнер повинен бути візуально відмінним від незаповненого. Для задоволення цієї вимоги треба, здавалося б, впроваджувати приховане повідомлення візуально незначущі області сигналу. Однак ці ж області використовують і алгоритми стиснення. Тому, якщо зображення буде надалі стискатися, то приховане повідомлення може зруйнуватися. Отже, біти повинні вбудовуватися у візуально значущі області, а відносна непомітність може бути досягнута за рахунок використання спеціальних методів, наприклад модуляції з розширенням спектра.

– Стегосистема ЦВЗ повинна мати низьку ймовірність помилкового виявлення прихованого повідомлення у сигналі, що його не містить. У деяких програмах таке виявлення може призвести до серйозних наслідків. Наприклад, помилкове виявлення ЦВЗ на DVD-диску або стрімінговому сервісі може викликати відмову від його відтворення плеєром.

– Повинна забезпечуватися необхідна пропускна спроможність (ця вимога є актуальною, в основному, для стегосистем прихованої передачі інформації).

– Стегосистема повинна мати прийнятну обчислювальну складність реалізації. При цьому можлива асиметрична за складністю реалізації система ЦВЗ, тобто складний стегокодер та простий стегодекодер.

До ЦВЗ пред'являються такі вимоги:

– ЦВЗ повинен легко (обчислювально) витягуватись законним користувачем.

– ЦВЗ може бути стійким чи нестійким до навмисних і випадковим впливам (залежно додатка). Якщо ЦВЗ використовується для підтвердження справжності, то неприпустима зміна контейнера повинна призводити до руйнування ЦВЗ (тендітний ЦВЗ). Якщо ж ЦВЗ містить ідентифікаційний код, логотип фірми і т.п., він повинен зберегтися при максимальних спотвореннях контейнера, звичайно, що не призводять до суттєвих спотворень вихідного сигналу. Наприклад, зображення можуть бути відредаговані кольорова гама або яскравість, аудіозапис – посилено звучання низьких тонів і т.д. Крім того, ЦВЗ повинен бути робастним по відношенню до афінних перетворень зображення, тобто його поворотів, масштабування. При цьому треба розрізняти стійкість самого ЦВЗ і здатність декодера правильно його виявити. Скажімо, при повороті зображення ЦВЗ не зруйнується, а декодер може бути нездатним виділити його. Існують додатки, коли ЦВЗ має бути стійким по відношенню до одних перетворень і нестійким по відношенню до інших. Наприклад, можна копіювати зображення (ксерокс, сканер), але накладено заборону на внесення до нього будь-яких змін.

– Повинна бути можливість додавання до цього додаткових ЦВЗ. Наприклад, на DVD-диску або стрімінговому сервісі є мітка про допустимість одноразового копіювання. Після такого копіювання необхідно

додати мітку про заборону подальшого копіювання. Можна було б, звичайно, видалити перший ЦВЗ та записати на його місце другий. Однак, це суперечить припущенню про труднощатність ЦВЗ. Найкращим виходом є додавання ще одного ЦВЗ, після якого перший не братиметься до уваги. Однак, наявність кількох ЦВЗ на одному повідомленні може полегшити атаку з боку порушника, якщо не вжити спеціальних заходів.

20.4. Відкриті, напівзакриті, закриті стеганосистеми

Стеганосистеми за видом детекторів діляться на: відкриті, напівзакриті, закриті:

1. У **відкритих стеганосистемах** для детектування інформації використовують як вхідні дані лише отриману оцінку з виходу стеганодекодера.

2. У **напівзакритих стеганосистемах** для детектування використовують, окрім отриманої оцінки, ще й вихідний ЦВЗ.

3. У **закритих стеганосистемах** для детектування необхідно, крім оцінки з виходу декодера і вихідного ЦВЗ, наявність порожнього контейнера. Існують два типи закритих систем:

– У першому типі детектору потрібні і вихідний контейнер, і вихідний ЦВЗ, а на виході система видає рішення про наявність або відсутність ЦВЗ (такі стегосистеми мають найбільшу стійкість до зовнішніх впливів). У другому типі детектору потрібен лише вихідний контейнер, але в виході система видає відновлений ЦВЗ.

– У напівзакритих системах детектору потрібен вихідний ЦВЗ, на виході видається рішення про наявність чи відсутність ЦВЗ.

Ця класифікація наведена у таблиці 20.1.

Таблиця 20.1 – Класифікація систем вбудовування ЦВЗ

		Що потрібно детектору		Вихід детектора	
		Вихідний сигнал	Вихідний ЦВЗ	Так/ні	ЦВЗ
Закриті	Тип I	+	+	+	-
	Тип II	+	-	-	+
Напівзакриті		-	+	+	-
Відкриті		-	-	-	+

Найбільше застосування можуть мати відкриті стегосистеми ЦВЗ, які аналогічні системам прихованої передачі. Найбільшу стійкість до зовнішніх впливів мають закриті стегосистеми I типу.

20.5. Поняття ЦВЗ, класифікація

Цифровий водяний знак (ЦВЗ) – технологія, створена для захисту авторських прав мультимедійних файлів. Зазвичай цифрові водяні знаки невидимі. Однак ЦВЗ можуть бути видимими на зображенні або відео. Зазвичай це інформація являє собою текст або логотип, який ідентифікує автора.

Невидимі ЦВЗ впроваджуються в цифрові дані, але не можуть бути сприйняті як такі. Найважливіше застосування цифрові водяні знаки знайшли в системах захисту від копіювання, які прагнуть запобігти або утримати від несанкційованого копіювання цифрових даних. Стеганографія застосовує ЦВЗ, коли сторони обмінюються секретними повідомленнями, впровадженими в цифровий сигнал. Використовується як засіб захисту документів з фотографіями – паспортів, водійських посвідчень, кредитних карток з фотографіями. Коментарі до цифрових фотографій з описовою інформацією – ще один приклад невидимих ЦВЗ. Хоча деякі формати цифрових даних можуть також нести в собі додаткову інформацію, звану метадані, ЦВЗ відрізняються тим, що інформація «зашита» прямо в сигнал. Об'єкти мультимедіа в цьому випадку будуть являти собою контейнери (носії) даних. Основна перевага полягає в наявності умовної залежності між подією підміни об'єкта ідентифікації та наявності елемента захисту – прихованого водяного знака. Підміна об'єкта ідентифікації призведе до висновку про підробку всього документа. Цифрові водяні знаки отримали свою назву від старого поняття водяних знаків на папері (грошах, документах).

Властивості цифрових водяних знаків

Зазвичай ЦВЗ класифікуються за 7 основними параметрами:

– обсяг;
– складність;
– оборотність;
– прозорість;
– надійність;
– безпека;
– верифікація.

Розглянемо їх біль детально.

Обсяг інформації

Розрізняють впроваджуваний і обсяг, що видобувається:

– Впроваджуваний обсяг. Об'єм, що впроваджується, – це просто розмір повідомлення, що впроваджується у сигнал.

– Об'єм, що видобувається. Об'єм, що видобувається, – це кількість інформації витягнутої із повідомлення. У випадку, якщо метою ЦВЗ не є передача інформації, то інформація, що видобувається, дорівнює нулю. Для не порожніх повідомлень об'єм, що видобувається, рахується після видобування.

Складність

Складність заданої функції завжди можна виміряти. Будь-які витрачені зусилля на впровадження, атаку, детектування чи розшифрування вимірюються складністю. Нехай складність визначимо як складність процесу впровадження інформації у сигнал. Залежно від реалізації функція вимірює витрачений час кількість операцій введення-виведення, кількість рядків коду і т.д. Складність залежить від сигналу. Тому часто розглядається нормована функція, що не залежить від Нормалізація може проводитись як за довжиною сигналу (вимірюється наприклад, в секундах, або бітах) сигналу так і за обсягом, що впроваджується:

Оборотність

Технологія передбачає можливість видалити ЦВЗіз позначеного сигналу. Якщо отриманий сигнал збігається з вихідним, то говорять про оборотність. Можливість звернутися надається спеціальними алгоритмами. Ці алгоритми використовують секретні ключі захисту від несанкціонованого доступу до контенту.

Прозорість

За даними еталонного та тестового сигналів, функція прозорості T вимірює розбіжність між цими сигналами. Результат обчислення укладено в інтервалі [0,1], де 0 відповідає випадку, коли система не може розпізнати в тестовому версію еталонного сигналу, та 1, якщо спостерігач не може відрізнити ці два сигнали.

Надійність

У цьому розділі описується надійність ЦВЗ. Спочатку треба запровадити поняття «успішного виявлення». Для виміру успіху функцій виявлення та дешифрування вводиться функція «успішного виявлення». Для ЦВЗ без закодованого повідомлення детектор повертає 0, якщо водяні знаки не можуть бути виявлені та 1 інакше. Міра надійності ЦВЗ – це число, укладене в інтервалі [0,1], де 0 найгірше можливе значення та 1 найкраще. Для вимірювання надійності використовуються поняття числа помилкових байтів та частоти помилкових бітів. Вимірюється відстань між рядками вилученого та впровадженого повідомлень чи відсоток збігів для побітового порівняння. Якщо рядки збігаються, то метод надійний. ЦВЗ схема вважається ненадійною, якщо більш ніж порогова кількість біт пошкоджені і прозорість атак вище визначеного порогового значення.

Безпека

Описує стійкість ЦВЗ по відношенню до певних атак.

Верифікація

Визначає тип додаткової інформації необхідної функції виявлення/вилучення для роботи.

– Необхідний вихідний сигнал S.

– Необхідне повідомлення m і деяка додаткова інформація, крім вихідного сигналу.

– Немає потреби у додатковій інформації.

Класифікація

ЦВЗ називають **надійним** по відношенню до класу перетворень T, якщо інформації з позначеного сигналу можна довіряти навіть після впливу на нього погіршення з T. Типові перетворення зображення: JPEG компресія, поворот, обрізання, додавання шуму і т.д. Для відеоконтенту до цього списку додається MPEG компресія та тимчасові перетворення. ЦВЗ називають **непомітним**, якщо вихідний і позначений сигнали за певними критеріями сприйняття невідмінні. Зазвичай легко зробити надійний чи непомітний ЦВЗ. Але, зазвичай, важко зробити ЦВЗ непомітний і надійний одночасно.

Технології ЦВЗ можуть бути класифіковані у різний спосіб

Надійність

ЦВЗ називається **крихким**, якщо за найменшої модифікації його не можна виявити. Такі ЦВЗ зазвичай використовують для перевірки цілісності.

ЦВЗ називається **напівкрихким**, якщо він витримує незначні модифікації сигналу, але шкідливі перетворення не витримує. Напівтенкі ЦВЗ використовуються зазвичай для виявлення атаки на сигнал.

ЦВЗ називається **надійним**, якщо він протистоїть всім відомим видам атак. Такі ЦВЗ зазвичай використовуються в системах захисту від копіювання та ідентифікації.

Метод нанесення ЦВЗ

Методи нанесення ЦВЗ поділяються на просторові та частотні. До просторових методів відноситься метод LSB. До частотним – методом розширення спектра. Позначений сигнал виходить адитивною модифікацією. Такі ЦВЗ відрізняються середньою надійністю, але дуже невеликою інформаційною ємністю. Спосіб амплітудної модуляції, схожий з шляхом розширення діапазону, також застосовується для застосування. Метод квантування не надто надійний, але дозволяє впровадити великий обсяг інформації.

Застосування:

- Відстеження розповсюдження копій даних:
  - Боротьба з відеопіратством та «ранній» доступ до новинок кіно. При співпраці з кіностудіями Голлівуду оператори телевізійних мереж можуть надавати своїм глядачам платний доступ до преміум-контенту – фільмів, які щойно з'явилися в кінотеатрах і ще не вийшли на DVD або стрімінговому сервісі. Обов'язковою умовою студій є вбудовування водяного знака, що дозволяє виявити джерело витоку – конкретного глядача – при попаданні фільму в нелегальний оборот.
  - Відстеження трансляцій (телевізійні новини часто містять водяні знаки, залишені міжнародними інформаційними агентствами; рекламні агенції використовують водяні знаки для контролю виходу своєї реклами в ефір в обумовленому обсязі).
- Метадані, електронний цифровий підпис
- Приховування факту обміну інформації (Стеганографія).

20.6. Метод модифікації найменшого значущого біта та інші методи приховання даних у зображенні, відео та аудіо

Приховання даних у зображенні й відео

Розвиток мультимедійних засобів супроводжується великим потоком графічної інформації в обчислювальних мережах. При генерації зображення, як правило, використовуються значна кількість елементарних графічних примітивів, що становить особливий інтерес для стеганографічних методів захисту. Візуальне середовище (цифрові зображення й відео) мають велику надмірність різної природи:

– кодовою надмірністю, що виникає при неоптимальному описі зображення;

– міжпіксельною надмірністю, що обумовлена наявністю сильною кореляційною залежністю між пікселями реального зображення;

– психовізуальною залежністю, що виникає через те, що орган зору людини не адаптований для точного сприйняття зображення пікселя за пікселем і сприймає кожну ділянку з різною чутливістю.

Інформаційним відеопотокам, які складаються з послідовності окремих кадрів зображення, крім зазначених вище, властива також надмірність, обумовлена інформаційною, технічною, часовою і функціональною (значеннєвою) залежністю між кадрами.

Останнім часом створена достатня кількість методів приховання інформації в цифрових зображеннях і відео, що дозволило провести їхню систематизацію й виділити наступні групи:

- методи заміни в часовій (просторової) області;
- методи приховання в частотній області зображення;
- широкополосні методи;
- статистичні методи;
- методи перекручування;
- структурні методи.

Розглянемо деякі особливості, які характерні для кожної з виділених груп стеганометодів.

Методи заміни

Загальний принцип даних методів полягає в заміні надлишкової, малозначимої частини зображення бітами секретного повідомлення. Для добування повідомлення необхідно знати місце, де була розміщена приховувана інформація.

Найпоширенішим методом цього класу є ***метод заміни найменшого значущого біта*** (НЗБ).

Даний метод працює з растровими зображеннями, які представлені у форматі без стиску (наприклад, GIF і BMP). Основним його недоліком є сильна чутливість до найменших перекручувань контейнера. Для ослаблення цієї чутливості часто застосовують завадостійке кодування.

Суть методу НЗБ полягає в заміні найменш значущих біт пікселів зображення бітами секретного повідомлення. У найпростішому випадку проводиться заміна НЗБ всіх послідовно розташованих пікселів зображення. Однак, так як довжина секретного повідомлення звичайно менше кількості пікселів зображення, то після його впровадження в контейнері будуть присутні дві області з різними статистичними властивостями (область, у якій незначні біти були змінені, і область, у якій вони не мінялися). Це може бути легко виявлене за допомогою статистичних тестів. Для створення еквівалентної зміни ймовірності всього контейнера секретне повідомлення звичайно доповнюють випадковими бітами так, щоб його довжина в бітах була дорівнює кількості пікселів у вихідному зображенні.

Інший підхід, ***метод випадкового інтервалу***, полягає у випадковому розподілі біт секретного повідомлення по контейнері, у результаті чого відстань між двома убудованими бітами визначається псевдовипадково. Ця методика найбільш ефективна при використанні потокових контейнерів (відео).

Методи заміни палітри. Для приховання даних можна також скористатися палітрою кольорів, що є присутньою у форматі зображення.

Палітра з N кольорів визначається як список пар індексів **(i, c_i)**, що визначає відповідність між індексом **i** і його вектором кольоровості $\mathbf{c_i}$. У зображенні кожному пікселю привласнюється індекс у палітрі. Так як кольори в палітрі не завжди впорядковані, то приховувану інформацію можна кодувати послідовністю зберігання кольорів у палітрі. Існує **N!** різних способів перестановки N-**кольорової** палітри, що цілком достатньо для приховання невеликого повідомлення. Однак методи приховання, в основі яких лежить порядок формування палітри, також нестійкі: будь-яка атака, пов'язана зі змінами палітри, знищує секретне повідомлення.

До методів заміни можна також віднести ***метод квантування зображень***. Даний метод заснований на міжпіксельній залежності, яку можна описати деякою функцією **Q**. У найпростішому випадку, можна розрахувати різницю $\mathbf{e_i}$ між суміжними пікселями $\mathbf{x_i}$ і $\mathbf{x_{i+1}}$ і задати її як параметр для функції **Q**: $\mathbf{\Delta_i = Q(x_i - x_{i-1})}$, де $\mathbf{\Delta_i}$ – дискретна апроксимація різниці сигналів $\mathbf{x_i - x_{i-1}}$. Так як $\mathbf{\Delta_i}$ є цілим числом, а реальна різниця $\mathbf{x_i - x_{i-1}}$ – речовинним, то з'являється помилка квантування $\mathbf{\delta_i = \Delta_i - e_i}$. Для сильно корельованих сигналів ця помилка близька до нуля: $\mathbf{\delta_i \approx 0}$. У даному методі приховання інформації проводиться шляхом коректування різницевого сигналу $\mathbf{\Delta_i}$. Стегоключ являє собою таблицю, яка кожному можливому значенню $\mathbf{\Delta_i}$ ставить у відповідність певний біт наприклад:

$\mathbf{\Delta_i}$	–4	–3	–2	–1	0	1	2	3	4
	0	1	0	1	1	1	0	0	1

Для приховання і-**го** біта повідомлення обчислюється $\mathbf{\Delta_i}$. Якщо $\mathbf{\Delta_i}$ не відповідає секретному біту, якому необхідно сховати, то його значення $\mathbf{\Delta_i}$ заміняється найближчим $\mathbf{\Delta_j}$, для якого ця умова виконується. Добування секретного повідомлення проводиться відповідно до різниці між $\mathbf{\Delta_i}$ і стегоключем.

Методи приховання в частотній області зображення

Стеганографічні методи заміни нестійкі до будь-яких перекручувань, а застосування операції стиску із втратами приводить до повного знищення всієї секретної інформації, схованої методом НЗБ у зображенні, а це значить що для таких форматів як JPEG вони не підходять. Більш стійкими до різних перекручувань, у тому числі стиску, є методи, які використовують для приховання даних не часову область, а частотну.

Існують кілька способів подання зображення в частотній області, наприклад:

– з використанням дискретного косинусного перетворення (ДКП),
– швидкого перетворення Фур'є,
– вейвлет-перетворення.

Дані перетворення можуть застосовуватися як до всього зображення, так і до деяких його частин. При цифровій обробці зображення часто використовується двовимірна версія дискретного косинусного перетворення:

$$\mathbf{S(u,\ v) = \frac{2}{N} C(u)\ C(v) \sum_{x=0}^{N1} \sum_{y=0}^{N1} S(x,y) \cos\left(\frac{\eth u(2x+1)}{2N}\right) \cos\left(\frac{\eth u(2y+1)}{2N}\right)},$$

$$\mathbf{S(x,\ y) = \frac{2}{N} \sum_{x=0}^{N1} \sum_{y=0}^{N1} C(u)C(v)S(u,v) \cos\left(\frac{\eth u(2x+1)}{2N}\right) \cos\left(\frac{\eth u(2y+1)}{2N}\right)},$$

де $\mathbf{C(u)=1/\sqrt{2}}$, якщо $\mathbf{u=0}$ і $\mathbf{C(u)=1}$ у противному випадку.

Один з найбільш популярних методів приховання секретної інформації в частотній області зображення заснований на відносній зміні величин коефіцієнтів ДКП. Для цього зображення розбивається на блоки розміром 8×8 пікселів. Кожний блок призначений для приховання одного біта секретного повідомлення. Процес приховання починається з випадкового вибору блоку $\mathbf{b_i}$, призначеного для кодування і-**го** біта повідомлення. Для обраного блоку зображення $\mathbf{b_i}$ проводиться ДКП: $\mathbf{B_i = D\{b_i\}}$. При організації секретного каналу абоненти повинні попередньо домовитися про конкретні два коефіцієнти ДКП, які будуть використовуватися для приховання секретних даних. Позначимо їх як $\mathbf{(u_1,\ v_1)}$ і $\mathbf{(u_2,\ v_2)}$. Ці два коефіцієнти повинні відповідати косинус-функціям із середніми частотами, що забезпечить схоронність інформації в істотних областях сигналу, що не буде знищуватися при JPEG-стиску. Так як коефіцієнти ДКП-середніх є подібними, то процес приховання не внесе помітних змін у зображення.

Якщо для блоку виконується умова $\mathbf{B_i(u_1,\ v_1) > B_i(u_2,v_2)}$, то вважається, що блок кодує значення 1, у противному випадку – 0. На етапі вбудовування інформації обрані коефіцієнти міняють між собою значення, якщо їхній відносний розмір не відповідає кодуємому біту. На кроці квантування JPEG-стиск може впливати на відносні розміри коефіцієнтів, тому, додаючи випадкові значення до обох величин, алгоритм гарантує що $\mathbf{|B_i(u_1,\ v_1) - B_i(u_2,v_2)| > x}$, де $\mathbf{x > 0}$. Чим більше **x**, тим алгоритм буде більш стійким до стиску, але при цьому якість зображення погіршується. Після відповідного коректування коефіцієнтів виконується зворотне ДКП.

Добування схованої інформації проводиться шляхом порівняння обраних двох коефіцієнтів для кожного блоку.

Широкополосні методи

Широкополосні методи передачі застосовуються в техніку зв'язку для забезпечення високої завадостійкості й утруднення процесу перехоплення. Суть широкополосних методів складається в значному розширенні смуги частот сигналу, більш ніж це необхідно для передачі реальної інформації. Розширення діапазону виконується в основному за допомогою коду, що не залежить від переданих даних. Корисна інформація розподіляється по всьому діапазоні, тому при втраті сигналу в деяких смугах частот в інших смугах присутня досить інформації для її відновлення.

Таким чином, застосування широкополосних методів у стеганографії утрудняє виявлення схованих даних і їхнє видалення. Ціль широкополосних методів подібна до задач, які вирішує стегосистема: спробувати "розчинити" секретне повідомлення в контейнері й унеможливити його виявлення. Оскільки сигнали, розподілені по всій смузі спектра, важко видалити, стеганографічні методи, побудовані на основі широкополосних методів, є стійкими до випадкових і навмисних перекручувань.

Для приховання інформації застосовують два основних способи розширення спектра:

– за допомогою псевдовипадкової послідовності, коли секретний сигнал, що відрізняється на константу, модулюється псевдовипадковим сигналом;

– за допомогою стрибучих частот, коли частота несучого сигналу змінюється по деякому псевдовипадковому законі.

Статистичні методи

Статистичні методи приховують інформацію шляхом зміни деяких статистичних властивостей зображення. Вони засновані на перевірці статистичних гіпотез. Суть методу полягає в такій зміні деяких статистичних характеристик контейнера, при якому одержувач зможе відрізнити модифіковане зображення від немодифікованого.

Дані методи ставляться до "однобітових" схем, тобто орієнтовані на приховання одного біта секретної інформації. **l(m)**-розрядна статистична стегосистема утвориться із множини однорозрядних шляхом розбивки зображення на **l(m)** непересічних блоків $\mathbf{B_1},\ldots,\mathbf{B_{l(m)}}$. При цьому секретний біт повідомлення $\mathbf{m_i}$ вбудовується в і-**й** блок контейнера. Виявлення захованого біта в блоці виробляється за допомогою перевірочної функції, що відрізняє модифікований блок від немодифікованого:

$$f(B_i)=\begin{cases}1, \textit{ якщо блок } B_i \textit{ був модифікований}\\ 0, \textit{ у іншому випадку}\end{cases}$$

Основна задача при розробці статистичного методу – це створення відповідної функції **f**. Побудова функції **f** робиться на основі теорії перевірки статистичних гіпотез (наприклад: основної гіпотези "блок $\mathbf{B_i}$ не змінений" і альтернативної – "блок $\mathbf{B_i}$ змінений"). При добуванні схованої інформації необхідно послідовно застосовувати функцію **f** до всіх блоків контейнера $\mathbf{B_i}$.

Припустимо, що відомо статистику розподілу елементів немодифікованого блоку зображення $\mathbf{h(B_i)}$. Тоді, використовуючи стандартні процедури, можна перевірити, чи перевищує статистика $\mathbf{h(B_i)}$ аналізованого блоку деяке граничне значення. Якщо не перевищує, то передбачається, що в блоці зберігається біт 0, у противному випадку – 1.

Найчастіше статистичні методи стеганографії складно застосовувати на практиці. По-перше, необхідно мати гарну статистику $\mathbf{h(B_i)}$, на основі якої приймається рішення про те, чи є аналізований блок зображення зміненим чи ні. По-друге, розподіл $\mathbf{h(B_i)}$ для "нормального" контейнера повинне бути заздалегідь відомо, що в більшості випадків є досить складною задачею.

Розглянемо приклад статистичного методу. Припустимо, що кожний блок контейнера $\mathbf{B_i}$ являє собою прямокутник пікселів $\mathbf{p^{(i)}_{n,m}}$. Нехай є псевдовипадкова двійкова модель того ж розміру $\mathbf{S = \{ S^{(i)}_{n,m} \}}$, у якій кількість одиниць і нулів збігається. Модель $\mathbf{S}$ у цьому випадку являє собою стегоключ. Для приховання інформації кожний блок зображення $\mathbf{B_i}$ ділиться на дві рівних підмножини $\mathbf{C_i}$ і $\mathbf{D_i}$, де $\mathbf{C_i = \{ p^{(i)}_{n,m} \in B_i \mid S_{n,m} = 1\}}$ і $\mathbf{D_i = \{ p^{(i)}_{n,m} \in B_i \mid S_{n,m} = 0\}}$. Потім до всім пікселям множини $\mathbf{C_i}$ додається значення $\mathbf{k > 0}$. Для добування повідомлення необхідно реконструювати підмножини $\mathbf{C_i}$ і $\mathbf{D_i}$ і знайти розходження між ними. Якщо блок містить повідомлення, то всі значення підмножини $\mathbf{C_i}$ будуть більше, ніж відповідні значення на етапі вбудовування повідомлення. Якщо припустити, що всі пікселі $\mathbf{C_i}$ і $\mathbf{D_i}$ незалежні, випадково розподілені величини, то можна застосувати статистичний тест:

$$\mathbf{q_i} = \frac{\mathrm{Ci} - \mathrm{Di}}{\hat{\sigma}_t}, \text{ де } \hat{\sigma}_t = \sqrt{\frac{\mathbf{Var[Ci]Var[Di]}}{|\mathbf{S}|/2}},$$

де Ci – середнє значення всіх пікселів множини $\mathbf{C_i}$, а $\mathbf{Var[C_i]}$ – оцінка дисперсії випадкових змінних в $\mathbf{C_i}$. Відповідно до центральної граничної теореми, статистика $\mathbf{q}$ буде асимптотично прагнути до нормального розподілу $\mathbf{N(0, 1)}$. Якщо повідомлення убудоване в блок зображення $\mathbf{B_i}$, то математичне очікування $\mathbf{q}$ буде більше нуля. Таким чином, **і-й** біт секретного повідомлення відновлюється шляхом перевірки статистики $\mathbf{q_i}$ блоку $\mathbf{B_i}$ на рівність нулю.

Методи перекручування

Методи перекручування, на відміну від попередніх методів, вимагають знання про первісний вид контейнера. Схема приховання полягає в послідовному проведенні ряду модифікацій контейнера, які вибираються відповідно до секретного повідомлення. Для добування схованих даних необхідно визначити всі розходження між стеганограмою і вихідним контейнером. По цих розходженнях відновлюється послідовність модифікацій, які виконувалися при прихованні секретної інформації. У більшості додатків такі системи марні, оскільки для добування даних необхідно мати доступ до набору первісних контейнерів: якщо супротивник також буде мати доступ до цього набору, то він зможе легко виявити модифікації контейнера й одержати докази схованої переписки. Таким чином, основною вимогою при використанні таких методів є необхідність поширення набору вихідних контейнерів між абонентами мережі через секретний канал доставки.

Структурні методи

Розглянуті вище методи в основному використовували інформаційну надмірність на рівні пікселів або ж проводили перетворення в частотній області зображення. Нижче розглядається метод, у якому приховання інформації проводиться на змістовному рівні з використанням структурних і інформаційних параметрів зображення. За суттю, він є розвитком відомої стеганографічної технології – семаграм. Суть методу полягає в проведенні послідовних перетворень фрагментів графічного зображення, які в остаточному підсумку приводять до формування приховуваного тексту.

У цей час з'явилося безліч графічних пакетів програм і баз даних, за допомогою яких можна створювати різні графічні зображення, презентації, мультиплікацію та ін. У кожному графічному зображенні можна виділити окремі компоненти, які відповідно до його області інтерпретації мають своє інформаційне навантаження. Візуальний образ S можна представити у вигляді цифрової послідовності, що потім легко перетвориться в текстове повідомлення. Це можливо, наприклад, у процесі покриття образа деяким графом, використовуючи інформаційну інтерпретацію його окремих компонентів. У першому наближенні вершинами такого графа можуть служити окремі компоненти рисунка, а ребрами – їхнього з'єднання. При кодуванні приховуваної інформації отриманий граф можна перетворювати досить широким спектром відомих у теорії графів перетвореннями. В остаточному підсумку такий граф може бути розмічений відповідно до певного алгоритму й представлений у вигляді його числового інваріанта. Найпростішим інваріантом є матриця суміжності графа (послідовність нумерації вершин). Можна використовувати кілька інваріантів, які описуються у вигляді багаточлена. Секретний ключ при такому підході – це спосіб нумерації графа. Відомо, що можлива кількість перенумерованих графів для довільного графа досить велике. Ця обставина робить запропонований спосіб приховання повідомлень досить стійким проти атак розкриття.

У структурних методах можна виділити окремі етапи стеганографічного перетворення.

Першим етапом є перетворення секретного повідомлення, що захищається**,** m у цифрову **форму CH**. Це перетворення може бути, наприклад, будь-яким криптографічним перетворенням. Воно являє собою шифрування тексту з усіма відповідними атрибутами, включаючи ключі шифрування.

Другий етап являє собою перетворення послідовності чисел **CH** у графічну структуру **GS**. Як графічні структури найчастіше використовуються графи. Крім графів, можна використовувати різні піктограми або інші структури, які піддаються формальному опису тим або іншому способу.

На *третьому етапі* здійснюється перетворення графічної структури **GS** у візуальне інформаційне середовище **WS**. У загальному випадку як таке середовище може використовуватися, наприклад, будь-яке мультимедійне або програмне середовище.

Четвертий етап являє собою сукупність методів і відповідних процедур, за допомогою яких формується сюжет з візуальних образів із впровадженими в них таємними повідомленнями.

У рамках даного підходу візуальний образ складається із графічних елементів, які ідентифікуються з елементами **GS**. Дані елементи являють собою позначені вершини, позначені або непомічені ребра й інші елементи, що ідентифікують компоненти з **CH**. Необхідним етапом функціонування такої стегосистеми є формування деякого сюжету для фрагмента інформаційного середовища з окремих графічних образів.

Таким чином, весь ланцюжок перетворень, що реалізується стегосистемою на рівні окремих етапів перетворення, може бути записана у вигляді: **S⇒CH⇒GS⇒WS⇒SJ**, де **SJ** – опис сюжету, що складається з окремих графічних образів. Слід зазначити, що розглянутий підхід застосуємо як для перетворення зображення з метою розміщення в ньому приховуваного повідомлення, так і для генерування візуального зображення по секретному повідомленню.

Приховання інформації у звуковому середовищі

Метод найменших значущих біт застосовується при цифровому поданні аудіосигнала й придатний для використання при будь-яких швидкостях зв'язку. При перетворенні звукового сигналу в цифрову форму завжди присутній шум дискретизації, що не вносить істотних перекручувань. “Шумовим” бітам відповідають молодші біти цифрового подання сигналу, які можна замінити приховуваними даними. Наприклад, якщо звуковий сигнал представлений в 16-бітовому виді, то зміна чотирьох молодших біт не приведе до помітного на слух перекручуванням. У якості стегоключа звичайно використовується покажчик місця розташування біт, у яких утримуються приховувані дані.

Методи широкополосного кодування використовують ті ж принципи, що методи приховання даних у зображеннях. Їхня суть полягає в незначній одночасній модифікації цілого ряду певних біт контейнера при прихованні одного біта інформації.

Метод приховання в луна-сигналі. Приховувати дані можна також шляхом впровадження луни у звуковий сигнал. Відомо, що при невеликих тимчасових зрушеннях луна-сигнал практично нерозрізнений на слух. У цьому методі для кодування послідовності значень використовуються нерівномірні проміжки між лунами-сигналами.

Фазові методи приховання застосовуються як для аналогового, так і для цифрового сигналу. Вони використовують той факт, що плавна зміна фази на слух визначити не можна. У таких методах данні, що захищаються, кодуються або певним значенням фази, або зміною фаз у спектрі. Якщо розбити звуковий сигнал на сегменти, то дані звичайно приховують тільки в першому сегменті при дотриманні двох умов:

– схоронність відносних фаз між послідовними сегментами;

– результуючий фазовий спектр стегосигналу повинен бути гладким, оскільки різкі перегони фази є демаскуючим чинником.

Аудіо стегосистеми

Музична форма звукового середовища займає більшу частину інформаційного простору Internet і широко використовується в радіомережах загального призначення. Для приховання даних крім методів, описаних вище, можна застосовувати методи, засновані на модифікації тих параметрів музичного середовища, які в теорії музики можна описати якісно. Музичне середовище має своє текстове відображення у вигляді нот і інших знаків, які дозволяють досить адекватно відображати музичний твір і його внутрішню структуру такими елементами, як ноти, гами, періоди, такти, каденції, акорди, мотиви, модуляції, тональності, різні види розвитку, секвенції та ін. Побудови музичних фрагментів підкоряються синтаксичним правилам, які можна описати, що дозволяє будувати логічні взаємини й, відповідно, опис структур музичних добутків.

Музичні стегосистеми забезпечують приховання інформації в музичному середовищі за аналогією з імпровізацією музичних добутків. За суттю імпровізація являє собою таку зміну музичного твору або його фрагментів, що зберігає основні теми первісного твору у вигляді мелодій, але при цьому розширює образ музичної теми іншими, що доповнюють основний образ рисами, яких не було в основному музичному твору. Основна відмінність музичної стеганографії від імпровізації полягає в тому, що метою є не розширення образів базового музичного твору, а внесення змін, які зберігають мелодію основного твору, відповідають всім правилам побудови даного твору й при цьому кодують приховуване повідомлення, не спотворюючи головної теми твору.

20.7. Атаки на стеганосистеми

Стегоаналіз дозволяє виявити факт наявності прихованого повідомлення. Він як правило дає не точну відповідь про факт приховання повідомлення, а лише відповідь з певною ймовірністю. Помилкою першого роду являється випадок, коли порожній контейнер приймається за заповнений, помилкою другого роду – коли непорожній контейнер приймається за пустий. Деякі методи стегоаналізу також дозволяють одержати додаткову інформацію, таку як, наприклад, довжина стегоповідомлення. За певних умов також можливе вилучення повідомлення із стегоконтейнера.

Введемо наступну класифікацію методів стегоаналізу цифрових зображень.

1. За наявністю інформації про алгоритм стеганографії:

– направлені методи, призначені для виявлення даних прихованих конкретним алгоритмом;

– універсальні (або «сліпі») методи, що використовуються, коли алгоритм приховування даних невідомий.

2. За вихідними даними:

– методи пасивного стегоаналізу, що дозволяють визначити лише присутність або відсутність прихованих даних у контейнері;

– методи активного стеганоаналізу, що крім наявності прихованого повідомлення здатні визначити його довжину, місце розміщення у контейнері, деякі параметри алгоритму стеганографії, а також навіть вилучити повідомлення з контейнера у випадку застосування простих алгоритмів приховування інформації.

3. За способом визначення наявності прихованої інформації:

– візуальні методи, засновані на пошуку видимих викривлень зображень, а також візуальному аналізі їх бітових зрізів;

– статистичні методи, засновані на понятті «природного» контейнеру, їх суть полягає в оцінці ймовірності існування стегоповідомлення на основі критерію оцінки близькості досліджуваного контейнера до «природного»;

– методи засновані на стисненні даних, базуються на тому, що приховані дані статистично незалежні від контейнера, тому при стисненні об’єм одержаного архіву зростає в порівнянні з початковим порожнім контейнером;

– методи стегоаналізу засновані на використанні нейронних мереж.

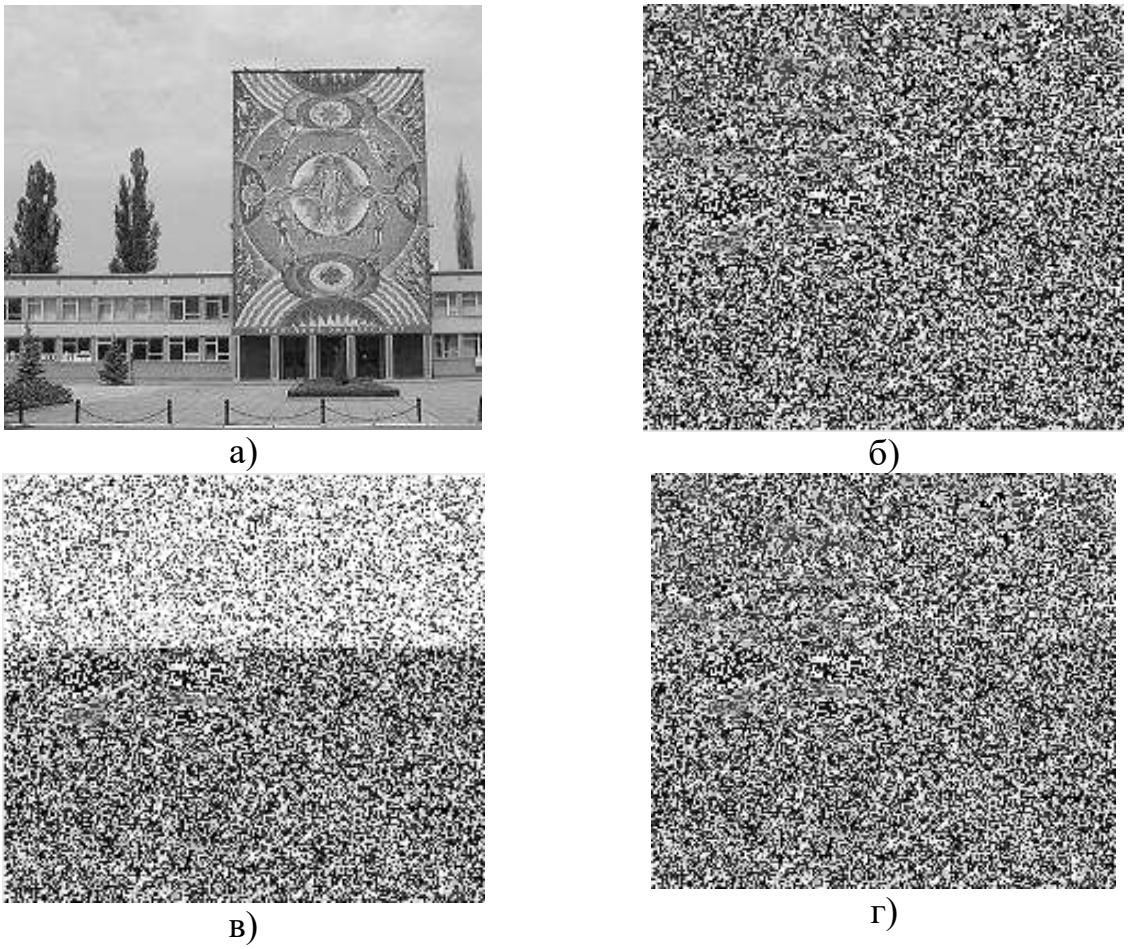
Розглянемо універсальні методи стегоаналізу розділені на групи в залежності від способу виявлення прихованої інформації.

Дослідження візуальних методів стегоаналізу

Візуальні методи засновані на здатності зорової системи людини аналізувати графічні образи та виявляти відмінності в порівнюваних зображеннях. Візуальні атаки ефективні при повному заповненні контейнеру: чим менше заповнений контейнер, тим складніше виявити факт прихованого повідомлення. Але частіше досліджується не саме зображення, а його бітові зрізи, тому що відмінності між порожнім та заповненим контейнером як правило візуально не проявляються. Якщо розглянути бітовий зріз, що містить найменші значимі біти, в деяких випадках можна побачити сліди прихованого повідомлення.

Для методів візуального аналізу бітових зрізів велике значення має алгоритм запису прихованої інформації та вид контейнеру. Якщо стегоповідомлення записувалося послідовно в кожний піксель контейнеру, то факт його наявності може бути встановлений з високою ймовірністю. Якщо пікселі для запису прихованої інформації вибиралися за допомогою генератора псевдовипадкових чисел, то дане завдання значно ускладнюється і залежить від того наскільки первісно був зашумлений контейнер. На рисунках 20.4 та 20.5 наведені контейнери та їхні бітові зрізи, що містять найменш значимі біти у випадках порожніх, послідовно заповнених та хаотично заповнених контейнерів. Як видно з рисунків найменші значимі біти (НЗБ) зображень (рис. 20.4) самі по собі містять шум, що ускладнює візуальний аналіз. У випадку послідовного запису стегоповідомлення в даний контейнер, якщо він заповнений не повністю, різниця між заповненою та порожньою частинами помітна візуально, у хаотично заповненому контейнері наявність стегоповідомлення вже не помітна. Графічне

зображення на рис. 20.5 не містить шуму у найменш значимих бітах. Приховати у ньому стегоповідомлення від візуального аналізу бітових зрізів видається малоймовірним. В обох наведених випадках, для послідовного та хаотичного заповнення контейнеру, сліди стегоповідомлення досить помітні.



а) б) в) г)

Рисунок 20.4 – Візуальний стегоаналіз контейнеру з великою первісною зашумленістю:

а) зображення-контейнер; б) бітовий зріз НЗБ порожнього контейнеру; в) бітовий зріз НЗБ частково заповненого контейнеру, стегоповідомлення записане послідовно в кожний піксель; г) бітовий зріз НЗБ частково заповненого контейнеру, стегоповідомлення записане у пікселі, які обрані генератором псевдовипадкових чисел

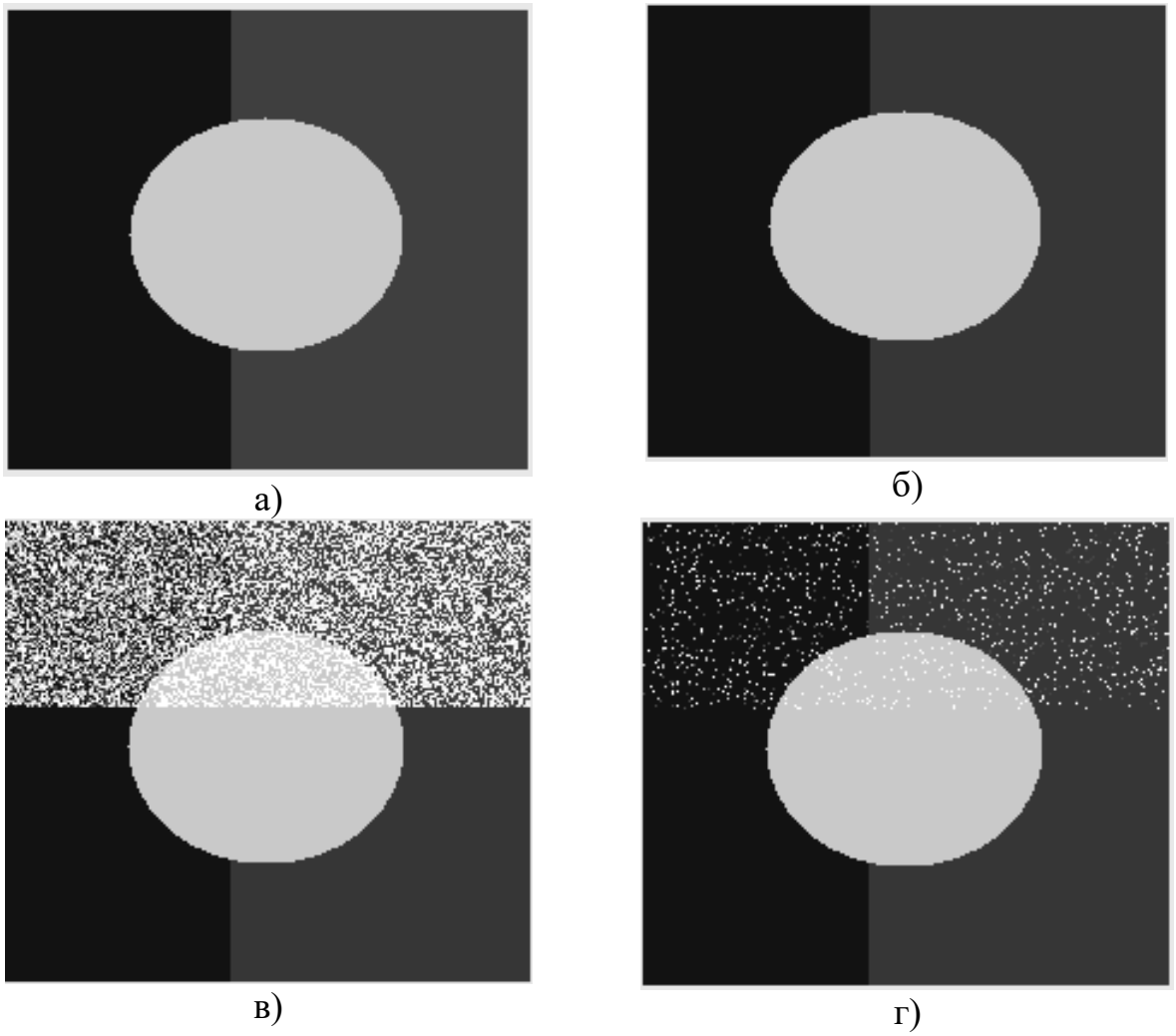


Рисунок 20.5 – Візуальний стегоаналіз контейнеру без первісної зашумленості:

а) зображення-контейнер; б) бітовий зріз НЗБ порожнього контейнеру; в) бітовий зріз НЗБ частково заповненого контейнеру, стегоповідомлення записане послідовно в кожний піксель; г) бітовий зріз НЗБ частково заповненого контейнеру, стегоповідомлення записане у пікселі, які обрані генератором псевдовипадкових чисел

Візуальні методи найбільш прості в реалізації, але малоефективні та незручні у використанні, так як зводиться до звичайного перегляду людиною зображення-контейнеру та його бітових зрізів з метою виявлення спотворень. Дозволяють виявити наявність стегоповідомлення тільки у випадку застосування найпростіших алгоритмів приховування даних та при значній заповненості контейнеру.

Дослідження статистичних методів стегоаналізу

Найбільш поширені та різноманітні методи статистичного стегоаналізу. Статистичні методи базуються на понятті «природного» контейнера. Суть методів полягає в оцінюванні ймовірності існування стегоповідомлення на основі критерію оцінки близькості досліджуваного контейнера до «природного».

Основним недоліком методів цього класу є саме припущення про існування «природного» контейнера.

Розглянемо методи розташовані у порядку убування ступеня довіри позитивним результатам їхнього застосування (виявлення прихованої інформації).

Метод оцінки числа переходів значень молодших біт у сусідніх елементах зображення

У методі використовується знання, що між молодшими бітами сусідніх елементів і між ними й іншими бітами природних контейнерів є кореляційні зв'язки. При аналізі графічних файлів формату BMP як елементи аналізованої послідовності вибираються найменш значущі біти складових кольору поруч розташованих пікселів зображення. При дослідженні файлів формату JPEG – молодші біти сусідніх дискретних косинусних коефіцієнтів**,** відмінних від 0 і 1.

Залежність між бітами у відповідних розрядах елементів контейнера має марківский характер. При цьому параметри залежності визначаються номером розряду. Під «переходом» розуміють перехід значення i-го елемента послідовності в значення i + 1 елемента послідовності x, i = 1, 2,..., n – 1, де n – довжина послідовності. Так як послідовності є двійковими, то аналізується чотири види переходів: з 0 в 0, з 0 в 1, з 1 в 0 і з 1 в 1. За отриманими результатами будується гістограма. Для кожного розряду перший стовбчик гістограми показує число переходів у потоці НЗБ із 0 в 0, другий стовбчик – з 0 в 1, третій стовбчик – з 1 в 0, четвертий стовбчик – з 1 в 1.

Для порожнього контейнера й контейнера, що містить вбудовану інформацію, число переходів у потоці НЗБ буде різним. Розподіл НЗБ стеганоконтейнера має, як правило, випадковий характер. Відповідно число переходів у потоці НЗБ для всіх станів буде приблизно однаковим, що не властиво порожньому контейнеру.

Метод оцінки частот появи k-бітових серій у потоці НЗБ елементів контейнера

Метод дозволяє оцінити рівномірність розподілу елементів у досліджуваній послідовності на основі аналізу частоти появи нулів і одиниць, і серій, що складаються з k біт. У бітовому представленні досліджуваної послідовності x підраховується, скільки разів зустрічаються нулі й одиниці (k = 1), серії-двійки (00, 01, 10, 11: k = 2), серії-трійки (000, 001, 010, 011, 100, 101, 110, 111: k = 3) і т.д. На основі результатів будується гістограма.

Для JPEG-зображень гістограма будується за значеннями частот появи бітових серій у потоці НЗБ дискретних косинусних коефіцієнтів, відмінних від -1, 0, 1.

Для незаповнених BMP і JPEG зображень не є характерним, щоб значення частот всіх компонентів перебували досить близько. При вбудовуванні інформації значення частот зближаються. Цей факт використовується при аналізі.

Результати роботи методу залежать від стеганографического перетворення, застосованого для вбудовування приховуваних даних, а також від їхнього обсягу. Як правило, виявлення факту приховування можливе при заповненості контейнера на 60% і вище.

Метод аналізу розподілу пар значень на основі критерію χ^2

У методі використовується аналіз гістограми, отриманої за елементами зображення й оцінка розподілу пар значень цієї гістограми. Для BMP-файлів пари значень формуються значеннями пікселів зображення, для JPEG – квантуємими коефіцієнтами дискретного косинусного перетворення, які відрізняються за молодшим бітом. Молодші біти зображень не є випадковими. Частоти двох сусідніх елементів контейнера повинні перебувати досить далеко від значення частоти середнього арифметичного цих елементів. В «порожньому» зображенні ситуація, коли частоти елементів зі значеннями 2N і 2N + 1 близькі за значенням, зустрічається досить рідко. При вбудовуванні інформації дані частоти зближаються або стають рівними. Ідея атаки хі-квадрат полягає в пошуку цих близьких значень і підрахунку ймовірності вбудовування на основі того, як близько розташовуються значення частот парних і непарних елементів аналізуємого контейнера. Особливістю алгоритму є послідовний аналіз усього зображення й, відповідно, нагромадження частот елементів.

Результати роботи методу за критерієм хі-квадрат значною мірою залежать від способу приховування даних. При послідовному записі в НЗБ елементів контейнера метод забезпечує гарні результати, а при псевдовипадковому виборі молодших біт і розсіюванні повідомлення по всій довжині контейнера метод не спрацьовує.

Існує «блоковий» варіант даного методу. Від класичного методу він відрізняється тим, що аналізоване зображення розбивається на блоки певного розміру, які можуть як перетинатися, так і не перетинатися, і для кожного блоку розраховуються свої набори частот елементів і свої ймовірності приховування. Крім того, існує можливість вибору окремих областей зображення для їхнього наступного аналізу. Такий підхід дозволяє виявляти наявність інформації, прихованої псевдовипадковим чином.

Метод аналізу гістограм, побудованих за частотами елементів зображення

Метод дозволяє оцінити рівномірність розподілу елементів аналізованого зображення, а також визначити частоту появи конкретного елемента.

Якщо розкид частот появи елементів у кольорових складових BMP-зображення прагне до нуля, то контейнер містить приховані дані. У протилежному випадку контейнер вважається порожнім.

Для зображень у JPEG-форматі будується гістограма частот квантованих дискретних косинусних коефіцієнтів. Експериментально виявлено, що огибаюча гістограми порожнього зображення має більш гладкий характер у порівнянні з гістограмами зображень, що містять стегоповідомлення. Звичайно, залежно від характеру й ступеня стиснення зображення, гістограми можуть змінюватися – у

них можуть з'являтися скачки й провали, але важливо те, що приховування інформації міняє загальний вид гістограм. Більшість стеганографічних програм, що працюють із JPEG, приховують дані в молодші біти дискретних коефіцієнтів, відмінних від 0 і 1. Як наслідок, частоти 0-х і 1-х DCT не змінюються, у той час як всі інші частоти або зменшуються, або збільшуються залежно від алгоритму вбудовування. При значних обсягах приховуваної інформації гістограми часто приймають східчастий характер, що нетипово для звичайних JPEG-зображень.

Метод аналізу розподілу елементів зображення на площині

Метод призначений для визначення залежностей між елементами досліджуваної послідовності.

На площину (поле) розміром $(2^R - 1)(2^R - 1)$, де R – розрядність елемента послідовності, наносяться точки з координатами (x_i, x_{i+1}), x_i – елементи досліджуваної послідовності x, i = 1, 2, …, n – 1, де n – довжина послідовності. За отриманою «картиною» проводиться аналіз

Якщо точки по всьому полю розташовані хаотично, то між елементами послідовності відсутні залежності, що характерно для контейнерів з вбудованими даними. У випадку незаповненого контейнера точки на полі будуть розташовані нерівномірно або утворювати «візерунки».

Метод перевірки розподілу елементів на монотонність

Метод дозволяє оцінити рівномірність розподілу елементів зображення за результатами аналізу довжин ділянок незростання й неубування елементів послідовності.

Досліджувана послідовність x графічно представляється у вигляді слідуючих один за одним непересічних ділянок незростання й неубування елементів послідовності.

Так як статистичні властивості стегоконтейнера близькі до властивостей випадкової послідовності, то ймовірність появи ділянки незростання (неубування) буде тим менше, чим більше його довжина n.

Метод «аналіз пар»

Даний метод заснований на пошуку закономірності в ймовірностях появи значень яскравості в природних зображеннях і зображеннях з вбудованим стегоповідомленням. При заміні молодшого біта компонента кольору чергового пікселя зображення на черговий біт попередньо зашифрованого або стиснутого стегоповідомлення (тобто стегоповідомлення, що має властивості псевдовипадкової послідовності), значення яскравості пікселя модифікованого зображення або дорівнює значенню яскравості пікселя контейнера, або змінюється на одиницю з імовірністю ~1/2. Для пошуку слідів вбудовування відбувається аналіз закономірностей у частотах появи «сусідніх» значень яскравості. Такі пари значень («Pair of Values») розрізняються тільки значенням найменш значущого біта.

Значення яскравості, двійкове представлення якого закінчується нульовим бітом 1, називається «лівим» (L), а сусіднє з ним значення яскравості, двійкове

представлення якого закінчується одиничним бітом – «правим» (R). Нехай кольорова гама вихідного контейнера включає 8 кольорів. Отже, при вбудовуванні повідомлення в НЗБ компонента кольору пікселів необхідно досліджувати статистичні характеристики в 4 парах номерів кольору.

Ймовірності появи лівих і правих номерів кольору в природних контейнерах, істотно відрізняються між собою у всіх парах, а в зображенні з убудованим стегоповідомлення ці ймовірності рівні. Це є явною ознакою наявності приховуваної інформації. Ступінь розходження між ймовірнісними розподілами елементів природних контейнерів і зображень із вбудованим стегоповідомлення може бути використана для оцінки ймовірності наявності стегоповідомлення у зображенні. Дану ймовірність зручно визначати з використанням критерію згоди χ^2.

Метод RS-аналізу

Одним з оригінальних методів статистичного стегоанализу є метод RS, вперше опублікований в 2001 р. колективом учених під керівництвом Дж. Фрідріх. Скорочення в назві розшифровується як Regular-Singular, тобто «регулярно-сингулярний».

Суть методу. Все зображення розбивається на групи по n пікселів $G(x_1, x_2,...,x_n)$ де n парне число, наприклад по 2 пікселя, що перебувають поруч по горизонталі. Для групи пікселів визначається функція регулярності або «гладкості» f(G), в якості такої функції можна вибрати, наприклад, дисперсію значень всередині групи, або просто суму перепадів значень суміжних пікселів. Під значенням пікселя розуміється ціле число від 0 до 255.

$$f(x_1, x_2,..., x_n) = \sum_{i=1}^{n-1} |x_{i+1} - x_i| .$$

Функція F(x) називається фліпінгом і має властивість F(F(x)) = x. Визначаються дві функції фліпінгу – F_1, відповідає інверсії молодшого біта пікселя, і F_2, що представляє собою інверсію з переносом у старший біт (додавання одиниці):

F_1: 0 ↔1, 2↔3, …, 254↔255,

F_2: 255↔0, 1↔2, 3↔4,..., 253↔254, 255↔0.

При застосуванні фліпінгу до групи одержуємо перетворену групу пікселів. Далі, всі групи пікселів розділяються на класи в такий спосіб:

(1) Регулярні групи: $G \in R \Leftrightarrow f(F(G)) > f(G)$,

(2) Сингулярні групи: $G \in S \Leftrightarrow f(F(G)) < f(G)$,

(3) Невикористовувані групи: $G \in U \Leftrightarrow f(F(G)) > f(G)$.

Метод ґрунтується на статистичному припущенні, що для природного зображення, тобто незаповненого контейнера, характерно наступне:

$$R_M \cong R_{-M} \text{ та } S_M \cong S_{-M} .$$

Припущення засноване на тому, що застосування F_{-1} дасть той же розподіл, що й F_1 на зображенні, значення пікселів якого зсунуті на одиницю. Для звичайного зображення співвідношення між групами не повинне істотно

змінюватися. Значна розбіжність між значеннями свідчить про застосування LSB-стеганографії для молодших біт зображення.

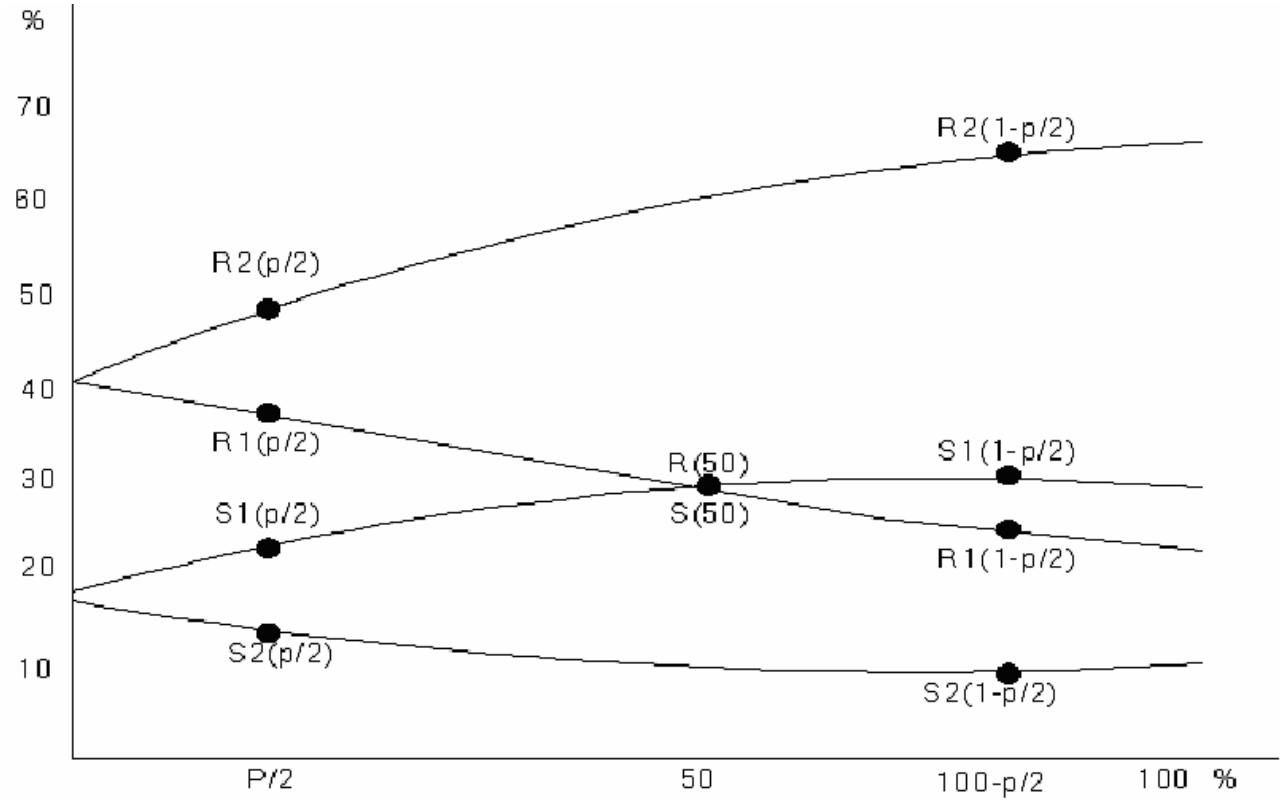


Рисунок 20.6 – RS-діаграма типового зображення

Розглянемо зміни молодших біт зображення при 100% перезаписі їх бітами повідомлення. Вбудовування випадкового повідомлення довжиною, рівною розміру зображення, призведе до того, що 50% молодших біт будуть інвертовані. Це, у свою чергу зведе до нуля різницю між значеннями R_M і S_M. Однак на R_{-M} і S_{-M} вбудовування повідомлення буде впливати прямо протилежно, і різниця цих величин буде пропорційна ступеню заповнювання контейнера, іншими словами довжині повідомлення. На рис. 20.6 наведена діаграма для типового зображення. На осі абсцис розташована кількість інвертованих біт x, шукана довжина повідомлення p, на осі ординат – відносні значення регулярних і сингулярних груп по відношенню до спільного числа груп зображення.

Припускаючи, що в зображення внесене повідомлення довжиною p біт, і при цьому 50% молодших біт, використаних для запису, будуть інвертовані, значення статистик буде одержане у точці p/2. Потім, якщо інвертувати всі молодші біти зображення й перерахувати статистики, на діаграмі вони будуть відповідати точкам кривих при x = 100-p/2. Повній рандомізації молодшої бітової площини відповідає точка 1/2**.** Тепер, якщо прийняти p/2 за нуль, а 100-p/2 за одиницю, а також використовувати апроксимацію кривих R_{-M} і S_{-M} прямими, а R_M і S_M параболами, можна вивести квадратне рівняння для знаходження координати точки перетину кривих R_M і S_M:

$$2(d_1 + d_0)x^2 + (d_{-0} - d_{-1} - d_1 - 3d_0)x + d_0 - d_{-0} = 0\,.$$

Потім, довжина повідомлення p обчислюється як p = x/(x-1/2). Таким чином, вихідне значення довжини є відповіддю для даного методу.

Для дуже зашумлених і дрібнотекстурованих зображень різниця між кількістю регулярних і сингулярних груп контейнера мала. Відповідно, лінії в RS-діаграмі перетнуться під малим кутом і точність зменшиться. Методика RS-стегоаналізу точніша для повідомлень, стегоповідомлення-біти яких випадково розміщені в площині стегоконтейнера, чим для повідомлень, вбудованих локально.

У табл. 20.2 наведено типові значення розмірів виявлених повідомлень у пустих контейнерах для зображень різних типів.

Таблиця 20.2 – Типові відсотки значень розмірів хибно виявлених повідомлень RS-аналізом

Тип зображення	Хибно визначена довжина повідомлення у відсотках від об'єму контейнера
Фотографії, скановані зображення	= 1 %
Зображення з Інтернету, підготовлені до друку	= 15... 20 %
Дрібнотекстуровані зображення, високодеталізовані зображення	= 30... 100 %

Дослідження методів стегоаналізу заснованих на стисненні даних

Існує метод стегоанализу цифрових зображень на основі стиснення даних. В даному методі можуть застосовуватися широко розповсюджені програми-архіватори.

Ідея методу полягає в наступному: потік випадкових даних стискається гірше, ніж потік, де зустрічаються повторювані послідовності. Інформація, що включається в молодші біти контейнера, як правило, попередньо шифрується й, можливо, стискається, тому є псевдовипадковою. Ступінь стиснення контейнерів використовується для визначення наявності в них прихованої інформації.

Формально даний алгоритм виглядає в такий спосіб. Нехай $X = \{x_1,..., x_N\}$ – послідовність байтів у полі даних зображення BMP, де $|X| = N$ – довжина послідовності.

Послідовність X розбивається на d рівних відрізків, а кожний відрізок позначається X_i, де i = 1, 2,..., d. Нехай ψ(X) – алгоритм стиснення, застосований до послідовності X. Далі визначається коефіцієнт стиснення відрізка n послідовності X алгоритмом ψ за наступною формулою:

$$f(X,n) = \frac{|\psi(X_n)|}{|X_n|}.$$

Нехай φ(X) – псевдовипадкова зміна молодших біт всіх байтів послідовності X, що подається на вхід програми, а Y = φ(X) – отримана з неї нова послідовність ("заповнений" контейнер). Початкова послідовність X повинна стискатися "сильніше" у порівнянні зі зміненою послідовністю Y.

Якщо відрізок X_i послідовності X містить "приховану" інформацію, то коефіцієнт f(X,i) і відповідний йому f(Y,i) відрізняються несуттєво, і навпроти, "порожня" ділянка стискається краще "заповненої". Для визначення факту вбудовування інформації обчислюється різниця коефіцієнтів стиснення:

$$\delta(X,n) = \left| f(X,n) - f(Y,n) \right|,$$

та вибирається граничне значення для величини δ і здійснюється оцінка кількості відрізків, на яких значення величини не перевищує поріг. Якщо таких відрізків більше d/2, то вважається, що вхідна послідовність X містила приховані дані, у протилежному випадку послідовність X вважається "порожньою". Поріг можна варіювати, регулюючи тим самим частоту помилок програми на порожніх і непустих контейнерах.

Є експериментальний аналіз алгоритму. У якості архіваторів використовувалися RAR, ZIP, GZIP, BZIP2. RAR показав мінімальну в порівнянні з іншими помилку 1-го роду. Архіватори ZIP і BZIP2 продемонстрували мінімальні помилки другого роду, для заповнених наполовину контейнерів. Найкращі результати були отримані з використанням архіватора ZIP, оскільки він найбільш вдало сполучив малі значення обох помилок тестів.

Даний метод дозволяє виявляти факт внесення прихованих даних у зображення формату 24-біт BMP. Особливістю методу є наявність параметрів, що дозволяють регулювати чутливість алгоритму. Помилка при заповненні контейнера на 50% і більше не перевищує 3%. При заповненні контейнера менше ніж на 40% метод дає більше хибних, ніж вірних відповідей як видно з наведених рисунків.

Дослідження методів стегоаналізу заснованих на використанні нейронних мереж

Методи стегоаналізу засновані на використанні нейронних мереж малодосліджені. Вони використовують статистичні методи стегоаналізу в поєднанні з можливостями нейронних мереж до навчання та класифікації. Існуючі методи засновані на алгоритмах навчання з учителем. В якості векторів вхідних даних використовуються частотні форми представлення зображень, отримані за допомогою вейвлет-перетворень.

Було запропоновано використати для стегоаналізу нейронні мережі RBF. Даний метод відноситься до «сліпих» методів виявлення вбудованої інформації. Одним з найважливіших етапів алгоритмів стегоаналізу заснованих на використанні нейронних мереж є вибір ознак за якими нейромережа буде робити висновок про наявність стеговставки. Простір пікселів зображення перетворюється в простір ознак і визначення наявності вбудованого повідомлення відбувається вже в просторі ознак. Як ознаки були використані статистичні моменти в частотній області гістограм вейвлет-коефіцієнтів.

Використання статистичних характеристик гістограм зображень пояснюється легкістю моделювання гістограм за допомогою суми, як правило, двох випадкових нормальних змінних і повнотою представлення зображення. В

частотній області відмінність стегоповідомлення від контейнера легше розрізнити.

Статистичні моменти в частотній області гістограм визначаються в такий спосіб:

$$M_n = \sum_{k=-N/2}^{N/2} |f_k|^n p(f_k),$$

де n – порядок моменту, N – кількість відліків коефіцієнтів дискретного перетворення Фур'є (ДПФ) для гістограми, $f_к$ – k-та частота в ДПФ (k = -N/2,...-1,0,1,..N/2).

$$p(f_k) = \frac{|H(f_k)|}{\sum_{k=-N/2}^{N/2} |H(f_k)|},$$

де, $|H(f_k)|$ – амплітуда ДПФ гістограми $h(x_k)$,

$$H(f) = \int_{-\infty}^{\infty} h(x) e^{-j2\pi fx} dx,$$

де h(x) – гістограма зображення, або інакше кажучи, кількість пікселів, що приймають значення x.

Кожний з n компонентів вхідного вектора подається на вхід m базисних функцій RBF-мережі і їхні виходи лінійно підсумовуються з вагами:

$$\{w_j\}_{j=1}^{m}.$$

Вихід RBF-мережі є лінійною комбінацією набору базисних функцій:

$$f(\bar{x}) = \sum_{j=1}^{m} w_j h_j(\bar{x}).$$

Якщо припустити, що параметри функції, зсув *c* і радіус *r* фіксовані, то завдання знаходження ваг вирішується методами лінійної алгебри. Цей метод називається методом псевдообернених матриць і він мінімізує середній квадрат помилки. Суть цього методу полягає в наступному.

Знаходиться інтерполяційна матриця H:

$$H = \begin{bmatrix} h_1(\bar{x_1}) \ldots . h_m(\bar{x_1}) \\ \ldots\ldots\ldots\ldots\ldots \\ h_1(\bar{x_p}) \ldots . h_m(\bar{x_p}) \end{bmatrix},$$

де m – число нейронів у прихованому шарі, p – розмір навчальної вибірки, n – число входів мережі.

На наступному етапі обчислюється інверсія добутку матриці H на транспортовану матрицю H^T:

$$A^{-1} = (H^T H)^{-1}.$$

Вектор ваг:

$$\overline{W} = A^{-1} H^T \overline{y}.$$

Якщо припущення про фіксовані параметри функції не виконуються, тобто крім ваг необхідно налаштувати параметри активаційної функції кожного нейрона (зсув функції й радіус) і задача стає нелінійною. Вирішувати її доводиться з використанням ітеративних чисельних методів оптимізації, зокрема, градієнтних методів.

Для навчання нейронних мереж було використано алгоритм навчання з учителем. Навчання без вчителя не було досліджене.

Для адекватного навчання RBF-мережі необхідно підготувати вхідні дані – провести аналіз за допомогою методу головних компонентів і стиснути діапазон по кожній ознаці до інтервалу [0,1].

Наводяться наступні результати роботи RBF-мережі – ймовірність помилки в навчальній вибірці склала 0%, була побудована мережа, що складається з 400 нейронів. Імовірність помилки на контрольній вибірці – 10%.

Висновки щодо стегоаналізу

В ході проведених досліджень було розглянуто основні методи стегоаналізу цифрових зображень, досліджено їх можливості та введено класифікацію. Перспективним напрямком подальших досліджень є вдосконалення існуючих методів статистичного стегоаналізу та стегоаналізу з використанням нейронних мереж. Дослідження кількісних та якісних показників ефективності даних методів стегоаналізу.

Розділ 21. Технічний захист інформації

21.1. Технічні канали витоку інформації: Акустичний (мовний) канал витоку інформації. Електричний канал витоку інформації. Електромагнітний канал витоку інформації. Методи прослуховування мобільного зв'язку. Оптичний та оптоелектронний канал витоку інформації. Параметричний канал витоку інформації.

21.2.Методи та засоби технічного захисту інформації: Пасивні та активні методи і засоби захисту інформації від витоку технічними каналами. Захист від прослуховування мобільного зв'язку. Система контролю та управління доступом (СКУД). Системи відеоспостереження. Пожежна сигналізація

21.1. Технічні канали витоку інформації: Акустичний (мовний) канал витоку інформації. Електричний канал витоку інформації. Електромагнітний канал витоку інформації. Оптичний та оптоелектронний канал витоку інформації. Параметричний канал витоку інформації

Технічні канали витоку інформації

Розглянемо найпоширеніші засоби несанкціонованого одержання інформації, з якими фахівцям з захисту інформації (ЗІ) часто доводиться зіштовхуватися на практиці.

1. ***Радіозакладки*** – мікропередавачі, радіус дії яких, як правило, не перевищує кількох сотень метрів. Сучасна елементна база дозволяє створювати радіозакладки в домашніх умовах.

2. ***Гостронаправлені мікрофони***, що мають голчасту діаграму спрямованості. За допомогою такого мікрофона можна прослухати розмова на відстані до 1 км у межах прямої видимості. За автомобілем, що рухається, аудіоконтроль вести можна тільки в тому випадку, якщо в ньому заздалегідь була встановлена закладка. На тривалих зупинках бесіду можна прослуховувати спрямованим мікрофоном за умови, що автомобіль перебуває в зоні прямої видимості й у ньому опущене одне зі стекол. У громадських місцях (кафе, ресторани й т.п.) прослуховування можна здійснювати спрямованим мікрофоном або закладкою. У таких випадках голосна музика, як втім і шум води, що ллється, не рятують, тому що в спрямованого мікрофона дуже вузька діаграма спрямованості.

3. ***Засоби прослуховування телефонних розмов*** можуть здійснювати несанкціоноване одержання інформації з телефонної лінії декількома методами:

– *установка записуючої апаратури (ЗА) на автоматизованій телефонній станції (АТС)* із використанням несумлінності або недбалості обслуговуючого персоналу;

– *безпосереднє підключення ЗА до телефонної лінії* (наприклад, у розподільній коробці);

– *вбудовування схеми несанкціонованого підключення в телефонний апарат* (для цього необхідний доступ у місця, у якому він встановлений).

Телефони, де як викличний пристрій використовується електромагнітний дзвінок можна прослуховувати *через дзвінковий ланцюг*. Це можливо й у тому випадку, якщо трубка лежить на апараті, – *через мікрофон*. Ще одним пристроєм прослуховування телефонних розмов і аудіоконтроля приміщень може служити *закладка, що живлеться енергією самої лінії*. Цей пристрій зручний тим, що не вимагає заміни живлення – установивши його один раз, зловмисник може користуватися ним можна нескінченно довго. Працює він тільки при знятій трубці. Якщо ж схема несанкціонованого підключення *убудована в телефонний апарат*, то зловмисникові досить набрати номер цього телефону й пустити в лінію звуковий код, після чого заставна схема імітує підняття трубки й підключає телефон до лінії.

4. Якщо в приміщенні шибки не завішені, то розмова за такими вікнами можна прослухати, направивши на скло ***лазерний промінь***. Звукові коливання в приміщенні приводять до синхронної вібрації стекол, а вони модулюють лазерний промінь, відбиваний від скла й прийнятий прийомним пристроєм.

5. У приміщеннях, у яких не були проведені спеціальні заходи щодо ЗІ (готельні номери, кафе, ресторани й т.п.), можна прослуховувати за допомогою ***пристроїв, що реєструють коливання елементів конструкції будинку*** (розетки, батареї центрального опалення, вентиляція, тонкі перегородки й т.п.).

6. Найбільш серйозну погрозу з погляду ЗІ, можуть нанести зловмисники, що вживають спроби несанкціонованого доступу до інформації, що обробляється автоматизованими системами (АС) (окремими комп'ютерами, інтелектуальними мережними пристроями, локальними й розподіленими комп'ютерними мережами й т.п.). Для одержання такої інформації можуть застосовуватися ***пристрої, що реєструють випромінювання*** комп'ютера і його периферії, а також комп'ютерних ліній передачі інформації. Для дистанційного зняття інформації за рахунок побічного випромінювання комп'ютера і його периферії застосовують високочутливі широкополосні приймачі, що дозволяють виконувати наступну цифрову обробку перехопленого сигналу.

Другий метод несанкціонованого одержання інформації з автоматизованих систем полягає в застосуванні ***методів несанкціонованого доступу до автоматизованої системи*** на локальному або мережному рівні.

Засоби проникнення

Ці засоби не відносяться безпосередньо до засобів несанкціонованого одержання інформації з технічних каналів, але в багатьох випадках застосовуються зловмисниками для таємного фізичного проникнення (ТФП) в охоронювані приміщення. До таких засобів відносяться: відмички, піроленти, різаки й спеціальні засоби. Найперше, із чим доводитися зіштовхуватися службам безпеки – це обмеження доступу сторонніх осіб. Ця проблема істотно ускладнюється з удосконалюванням технічних засобів проникнення. Сьогодні багато компаній пропонують комплекти, що дозволяють відкривати будь-які двері, а іноді й зламати її або швидко виготовити копії ключів.

Не становить праці прочитати будь-який запечатаний лист, використовуючи спеціальний спрей, за допомогою якого можна зробити прозорим на час конверт, не залишивши слідів. Крім цього існує безліч інших спеціальних приладь, таких як комплекти, що відновлюють стерті записи, або комплекти для відновлення записів по відбитках, залишеним пишучими предметами.

Акустичний (мовний) канал витоку інформації

Пристрої прослуховування приміщень

До цієї групи пристроїв відносяться: прийомопередаюча апаратура, мікрофони, електронні стетоскопи, магнітофони й апаратура прослуховування телефонів, факсів, телексів.

Прослуховування – спосіб ведення розвідки, застосовуваний агентами, спостерігачами, спеціальними постами прослуховування. Це один з розповсюджених способів одержання (добування) інформації.

Прослуховування може здійснюватися безпосереднім сприйняттям акустичних коливань при прямому сприйнятті мовної інформації, або сприйнятті звукових коливань, що надходять через елементи будинків і приміщень (стіни, підлоги, стелі, дверні й віконні прорізи, вентиляційні канали, системи опалення), а також за допомогою досить різноманітних технічних засобів. До цьому варто додати, що прослуховування ведеться в реальному масштабі часу й деякою мірою може дозволити вчасно прийняти важливі оперативні рішення.

Прослуховування можна класифікувати в такий спосіб (рисунок 21.1).



Рисунок 21.1 – Класифікація засобів прослуховування

Один з головних каналів витоку інформації – телефонні та інші розмови, які при сучасному рівні розвитку техніки прослуховуються без особливих утруднень. Розмови можуть прослуховуватися як у приміщенні, так і в автомобілях. Пристрій аудіонагляду, за допомогою якого ведеться

прослуховування, легко встановити й украй важко виявити, оскільки сучасна апаратура мініатюрна, надійна й має тривалий термін дії.

Для прослуховування широко використовуються різні прилади: радіомікрофони, спеціальні магнітофони, замасковані диктофони, стетоскопи й різні приймально-передавальні системи. Найпростіша й найбільш популярна система звукозапису складається з ***мікрофона, радіопередавача й джерела живлення.*** Деякі типи мікрофонів розраховані на збір інформації в радіусі 20 м і передачу її на відстань до 1 км. Щоб виключити можливість виявлення, потужність передавача робиться невеликою. Цієї ж мети можна досягти шляхом правильного вибору робочої частоти. Широке поширення одержали пристрої, що перехоплюють, працюючі в гігагерцовому діапазоні, що забезпечує велике проникнення в бетонних будинках.

У деяких випадках зручно працювати із ***кварцовими пристроями****, що* перехоплюють, які встановлюються на транспортних засобах, причому шум мотора й інших сторонніх шумів усуваються. Частота передачі залишається постійною завдяки введенню кристала кварцу в ланцюг, що рятує від необхідності настроювати частоту приймача тюнером після включення передавача. Одна з переваг кварцових систем спостереження – вузький діапазон частот, завдяки чому поліпшується якість передачі. Джерелами живлення для цих пристроїв можуть служити гальванічні елементи, електромережа або телефонна мережа. Широке поширення одержали системи, що прослуховують, з акустоавтоматикою, що включаються автоматично при звуці голосу.

Якщо немає можливості встановити пристрій спостереження безпосередньо в приміщенні, інформація може бути отримана за допомогою ***електронних стетоскопів***, що дозволяють прослуховувати розмови через двері, стелі, вікна й бетонні стіни товщиною 50–70 см. Установка передавача-стетоскопа зводиться до притискання його присоска до стіни, стелі або вікну, які прилягають до контрольованого приміщення.

Складно виявити прилади, що передають інформацію ***через електричну мережу***, від якої одночасно й живляться, оскільки приймач включається в будь-яку розетку в цьому будинку, що обслуговується тією же підстанцією.

Існують мініатюрні й економічні системи, у яких передача інформації відбувається в ***оптичному діапазоні*** й приймачами є ***фотооб'єктиви***. Так інфрачервона передавальна система далекої дії прослуховує розмови на відстані до 500 м. Інфрачервоний передавач перетворить звук у світлові імпульси, прийняті фотооб'єктивом.

Найбільш дорогими пристроями, що перехоплюють, *є* ***лазерні*** системи. На вікно направляється невидимий промінь, що модулюється коливаннями скла й відбивається на оптичний приймач, що перетворить його в аудіосигнали.

Часто для перехоплення розмов використовуються ***мініатюрні магнітофони*** розміром із кредитну картку. Такі пристрої вловлюють мову з відстані 8-10 м и в більшості випадків мають убудований акустоматик. Форма й розміри таких пристроїв дозволяють їх легко сховати, наприклад, у книзі середнього обсягу. Час запису 2 години, але в різних моделях він може бути збільшений.

Важливе джерело одержання інформації – лінія зв'язку, зокрема, телефон. Прилади ***телефонного прослуховування*** можуть підключатися до будь-якої точки лінії, і часто замасковані під різні деталі апарата. Закладки мають необмежений термін служби, оскільки живляться від телефонної лінії, причому функціонування телефону й лінії не порушується. Особливий інтерес представляють передавачі телефонного й кімнатного прослуховування, які по закінченню телефонної розмови автоматично перемикаються на спостереження за контрольованим приміщенням.

Сполучення щодо невисокої ціни й винятково високої ефективності таких пристроїв, а також відсутність строгих правових норм, роблять даний канал витоку інформації ***одним із самих небезпечних***.

До основних типів радіопередаючих пристроїв прослуховування відносяться:

– радіомікрофони;

– телефонні закладки (можливі комбіновані варіанти з радіомікрофонами);

– радіостетоскопи.

Закладки представлені широким спектром найрізноманітніших варіантів виконання.

Установка ***радіозакладок*** у технічні засоби забезпечення виробничої діяльності виконується з метою одержання конфіденційної інформації акустичного характеру або інформації, переданої (оброблюваної) такими технічними засобами в електронній або електромагнітній формі.

По конструктивному виконанню й тактичному використанню **радіозакладки** підрозділяються на ***телефонні*** (установлювані безпосередньо в телефонних апаратах) і ***мікрофонні*** (використовуються для акустичного прослуховування розмов).

Випромінюваний радіозакладкою сигнал приймається звичайними або спеціальними радіоприймачами й фіксується на відповідній окінцевій апаратурі.

Радіозакладки забезпечують реалізацію одного з найпоширеніших способів несанкціонованого доступу до джерел інформації – прослуховування. При цьому перехоплюються розмови або звукові сигнали, техніки й устаткування надходять до зловмисника на радіочастотах по радіо- або провідному каналам. По конструктивних особливостях радіозакладки, як ми вже відзначали, підрозділяються на мікрофонні й телефонні.

Мікрофонні радіозакладки – це мініатюрні радіопередавачі з убудованим або винесеним мікрофоном. Останні застосовуються, якщо радіопередавач по яких-небудь умовах не може передавати інформацію з певної зони, наприклад, через особливості поширення радіохвиль або твердого режиму радіоконтроля.

Телефонні радіозакладки встановлюються в телефонні апарати або в телефонну лінію в будь-якій точці між телефоном і автоматизованою телефоною станцією (АТС). Вони призначаються для прослуховування розмов з передачею їхнього змісту зловмисникові на радіочастотах по ефірі або по проводам самої ж телефонної лінії. Телефонні радіозакладки також являють собою мініатюрний радіопередавач, як мікрофон якого використовується мікрофон слухавки.

Зручність такого рішення полягає в тому, що джерелом електроживлення закладки є сама телефонна лінія, що забезпечує її роботу доти, поки працює АТС. Включатися телефонна радіозакладка може не тільки в телефонний апарат, але й у телефонну лінію й установлюватися навіть поза приміщенням, де розташований телефонний апарат: у телефонній розетці, у коридорі на комутаційній коробці, у розподільній шафі й навіть на самій АТС.

За ***конструктивними особливостями і принципом дії*** радіовипромінюючі пристрої, що прослуховують, можна класифікувати в такий спосіб.

За живленням:

– з автономним живленням (від акумуляторів або гальванічних елементів);

– з зовнішнім живленням (від мережі змінного струму, від телефонної лінії й т.п.).

За тривалістю роботи:

– необмежено (живлення від зовнішнього джерела);

– від декількох годин до декількох тижнів.

За дальністю дії: від одиниць до сотень метрів.

За конструктивним виконанням:

– с камуфляжем під різні електро- і побутові предмети;

– без елементів камуфляжу.

*За частотним діапазон*ом: від десятків кГц до сотень, а в окремих випадках і тисяч МГц (найчастіше використовуються наступні діапазони: 60-170, 250-290, 310-335, 360-430 і 470-1300 МГц).

За видом модуляції:

– частотні;

– амплітудні;

– спеціальні види.

За часом включення (роботи):

– по запиту;

– безупинно.

Малі габаритні розміри, маса й використання елементів камуфляжу визначають широкий діапазон варіантів використання пристроїв, що прослуховують, і утрудняє їхнє виявлення. Радіозакладки підбираються індивідуально для конкретного приміщення. Це необхідно для того, щоб максимально ефективно використовувати можливості закладки.

Електричний канал витоку інформації

Пристрої для прослуховування проводових телефонних ліній

Безпосереднє підключення до телефонної лінії – найбільш простий і надійний спосіб одержання інформації. У найпростішому випадку застосовується трубка ремонтника-телефоніста й навушники, підключені до лінії в розподільній коробці, де відбувається розведення кабелів. Найчастіше це почерк нижчої ланки “фахівців” з карного миру (верхня ланка оснащена апаратурою не гірше державних спецслужб).

Доречно нагадати, що АТС перемикає лінію на розмову при шунтуванні її опором близько 1 кОм. Тому застосування апаратури прослуховування з малим вхідним опором приводить до виявлення прослуховування. Якщо при розмові чутні клацання в лінії, відбуваються перепади гучності й т.п. явища, це цілком може говорити про спробу прослуховування на непрофесійному рівні.

Підкуп обслуговуючого персоналу на АТС – ще один досить розповсюджений спосіб одержання інформації, використовуваний зловмисниками. Особливо це стосується невеликих міст, де як і раніше використовують старі АТС із мінімумом автоматики.

Прослуховування через електромагнітний дзвінок ТА. Телефонні апарати, де як викличний пристрій використовується електромагнітний дзвінок, ще зустрічаються у державах, що входили в колишній СРСР. Дзвінок має властивість дуальности, тобто якщо на електромагнітний дзвінок діють звукові хвилі, він починає виробляти відповідним чином модульований струм. Амплітуда його достатня для подальшої обробки. Експерименти показали, що амплітуда наводиться в лінії ЕРС для деяких типів ТА може досягати декількох мВ. Корпус апарата є додатковим резонуючим пристроєм.

Прослуховування через мікрофон ТА не є синонімом безпосереднього підключення до лінії – цей спосіб набагато складніше. Мікрофон є частиною електричної схеми ТА. Він або з'єднаний з лінією (через окремі елементи схеми) при розмові, або відключений від лінії, коли ТА перебуває в готовності до прийому виклику (трубка перебуває на апарату). На перший погляд, коли трубка лежить на апарату, немає ніякої можливості використовувати мікрофон як джерело знімання інформації. Але в дійсності це не так.

Для знімання інформації використовується *високочастотне нав'язування*. Під високочастотним (ВЧ) нав'язуванням розуміється спосіб одержання інформації, при якому в телефонну лінію телефону, у бік що прослуховується, подають від спеціального генератора ВЧ коливання. Ці коливання за рахунок нелінійних елементів телефонного апарата взаємодіють із мовними сигналами при розмові (піднята слухавка) або з електрорушійної сили (ЕРС) мікрофонного ефекту дзвінка (покладена трубка). Звуковий і ВЧ сигнали утворять складну поліноміальну залежність, тому що нелінійність виконує роль модулятора. Виходить щось начебто квазителефоної радіозакладки, у якій генератор ВЧ коливань винесений, а нелінійність апарата виконує роль модулятора.

Методи й засоби підключення до проводових ліній зв’язку

Найпростішим є ***контактне підключення***, наприклад паралельне підключення телефонного апарата, досить широко розповсюджене в побуті. Але контактне підключення такого типу легко виявляється за рахунок істотного спадання напруги, що приводить до погіршення чутності в основному телефонному апарату. У технічному відношенні метод контактного підключення полягає в тому, що він реалізується безпосереднім включенням у проведення телефонного або телеграфного апаратів.

Безконтактне підключення до лінії зв'язку здійснюється двома способами:

– за рахунок електромагнітних наведень на паралельно прокладених проводах рамки;

– за допомогою зосередженої індуктивності, що охоплює контрольовану лінію.

В обох випадках прослуховування реалізується за рахунок електромагнітної індукції.

Методи й засоби віддаленого одержання інформації

Дистанційний спрямований мікрофон

Використання явища резонансу звукових хвиль у спрямованих системах приводить до збільшення звукової енергії, що надходить у мікрофон.

Системи схованого відеоспостереження

Сучасна електроніка дозволяє не тільки прослуховувати розмови, але й бачити те, що відбувається в контрольованих приміщеннях. Багатьма фірмами випускається висококласна відео- і фотоапаратура, що володіє колосальними можливостями в області схованого спостереження. Розроблено системи, здатні проводити зйомку практично в абсолютній темряві, що дозволяють фотографувати через найменші отвори. Пристрої можуть бути постачені встаткуванням для передачі відеосигналу й передавати зображення на відстань до декількох кілометрів

Акустичний контроль приміщень через засоби проводового телефонного зв'язку

Засоби телефонного зв'язку можна використовувати для контролю акустичних сигналів, сприйманих установленим у контрольованому приміщенні мікрофоном. Для цього мікрофон установлюється в телефонну розетку. Туди ж установлюється й пристрій дистанційного керування. Управляти пристроєм можна практично з будь-якого іншого телефону, не тільки міського, але й міжміського й міжнародного.

Принцип роботи пристрою зводиться до наступного.

1. Пристрій приймає перший виклик (дзвінок), не пропускаючи його в телефонний апарат.

2. Якщо треба другий і наступний дзвінки, пристрій їх пропускає, нічим не виявляючи себе й не порушуючи звичайний режим роботи телефонного зв'язку.

3. Якщо другий дзвінок не пішов, пристрій переходить у режим готовності. У цьому режимі при повторному дзвінку через 10-15 с пристрій видає в лінію сигнал “зайнятості” (короткі гудки) протягом 40-45 с, після чого гудки припиняються й пристрій відключає телефонний апарат і підключає до телефонної лінії встановлений у розетці мікрофон. Із цього моменту починається прослуховування розмов, що ведуться в приміщенні.

4. Для вимикання мікрофона після закінчення прослуховування досить на стороні зловмисника покласти слухавку. Пристрій вимикається й приводить всю систему телефонного зв'язку у звичайний режим.

5. Якщо абонент контрольованого приміщення в період його прослуховування вирішив подзвонити й підняв трубку свого телефонного апарата, пристрій моментально відключить мікрофон і підключить телефонний апарат до лінії.

6. Для продовження контролю приміщення операція підключення мікрофона повторюється.

Електромагнітний канал витоку інформації.
Перехоплення електромагнітних випромінювань

Під перехопленням електромагнітних випромінювань розуміють одержання розвідувальної інформації за рахунок прийому сигналів електромагнітної енергії пасивними пристроями, розташованими на досить безпечній відстані від засобів обробки інформації з обмеженим доступом.

Слід зазначити, що перехоплення інформації володіє рядом наступних особливостей у порівнянні з іншими способами добування інформації:

– інформація добувається без безпосереднього контакту із джерелом;

– на прийом сигналів не впливають ні пора року, ні час доби;

– інформація виходить у реальному масштабі часу, у момент її передачі або випромінювання;

– добування ведеться потай, джерело інформації найчастіше й не підозрює, що його прослуховують;

– дальність прослуховування обмежується тільки особливостями поширення радіохвиль відповідних діапазонів.

Методи прослуховування мобільного зв’язку

Під час розробки технології GSM, а як і стадії її застосування, враховувалися всі вимоги від контролюючих державних органів рівня забезпечення захисту. Саме через ці вимоги в багатьох країнах світу заборонено продаж і купівлю спеціального обладнання, начебто потужних шифраторів, криптообладнання, скремблерів, а також дуже захищені технології для публічного зв'язку. А ось оператори мобільного зв'язку самі забезпечують захист власних радіоканалів, використовуючи способи шифрування сигналу. Під час шифрування використовуються дуже складні алгоритми. Яким саме криптоалгоритмом здійснюватиметься шифрування вибирається на етапі, коли встановлюється з'єднання між базовою станцією та самим абонентом. Ступінь ймовірності виникнення витоку інформації про абонента з обладнання оператора дорівнює практично нулю, через складність та контроль за доступом до об'єктів та обладнання оператора.

Активний метод і пасивний метод прослуховування мобільних телефонів

Технологічно є два методи прослуховування абонентів – це активний метод і пасивний метод. **При пасивному прослуховуванні** абонента потрібно використовувати дуже дороге обладнання та мати спеціально навчених працівників. За наявності грошей (читайте – великих грошей) на «чорному

ринку» можна придбати спеціальні комплекси, використовуючи які можна прослуховувати розмови будь-якого абонента в радіусі до 500 метрів.

Як переконують виробники подібних систем прослуховування, їх системи можуть відслідковувати GSM-розмови в режимі реального часу, тому що принцип роботи обладнання ґрунтується на доступі до SIM-картки абонента мобільного зв'язку або прямо до бази даних самого оператора стільникового зв'язку. Хоча, якщо такого доступу у тих, хто вас слухає, вони можуть прослуховувати всі ваші розмови з деякою затримкою. Розмір затримки залежить від рівня шифрування каналу зв'язку, який використовує той чи інший оператор. Подібні системи також можуть бути мобільними центрами для забезпечення прослуховування та відстеження пересування об'єктів.

Другим способом прослуховування є **активне втручання** прямо в ефірі на процес автентифікації та протоколи керування. Для цього використовують спеціальні мобільні комплекси. Такі мобільні системи, які, за суттю, є парою спеціально модифікованих телефонів і ноутбука, незважаючи на свою зовнішню простоту і малогабаритність, теж є недешевим задоволенням – їхня ціна варіюється від кількох десятків тисяч і до кількох сотень тисяч американських доларів. І знову ж таки – працювати на такому устаткуванні можуть лише фахівці високої кваліфікації в галузі зв'язку.

Атака на абонента здійснюється за таким принципом: оскільки комплекс є мобільним і знаходиться до абонента на близькій відстані – до 500 метрів, він «перехоплює» сигнали для встановлення з'єднання та передачі даних, замінюючи собою базову станцію оператора. За суттю, сам комплекс стає «мостом-посередником» між найближчою базовою станцією та самим абонентом.

Після «захоплення» таким чином потрібного абонента мобільного зв'язку цей комплекс фактично може виконати будь-яку функцію управління над перехопленим каналом: наприклад, з'єднати прослуховуваного з будь-яким необхідним для тих, хто слухає номером, знизити алгоритм криптошифрування або взагалі відключити це шифрування для конкретного сеансу зв'язку тощо.

Крім того існують наступні підходи до прослуховування мобільних телефонів

Легальне прослуховування правоохоронними органами

За кримінальним кодексом правоохоронці можуть прослуховувати телефонні розмови під час слідства і не повідомляти про це. Це відбувається у тих випадках, коли людину підозрюють у скоєнні тяжкого злочину.

Спеціалісти роблять такі висновки:

– Не можна за якимись непрямими ознаками зрозуміти, що телефон прослуховують правоохоронці.

– Шум, луна чи тріск під час розмови свідчать лише про проблеми зі зв'язком і ні про що більше.

– Єдиний спосіб з'ясувати, чи слухають вас, це подати адвокатський запит.

Деякі сайти публікують список спеціальних кодів, за допомогою яких можна виявити прослуховування телефону. Фахівці спростовують цей міф і наголошують, що виявити таким чином прослуховування телефону неможливо.

Хакерський злам телефону через шпигунські програми

Для того, щоб встановити прослуховування, достатньо заразити ваш пристрій. Наприклад, надіслати шпигунський файл електронною поштою, в месенджер або SMS. Коли такий вірус потрапляє у телефон, йому відкривається доступом до всієї інформації. Більш того, гаджетом можна керувати віддалено: дивитися листування, через увімкнений мікрофон слухати розмови та записувати їх.

Дублювання SIM-картки

Для цього потрібно надати персональні дані оператору стільникового зв'язку. Такі дані людини можна купити через спеціальні Telegram-канали, форуми та на чорному ринку.

Злам персонального кабінету на сайті або у додатку оператора стільникового зв'язку

Це дозволить переадресувати всі вхідні дзвінки та SMS абонента на пристрій зловмисника.

Хибні базові станції – прослуховування через підставні станції зв'язку

Незаконно прослуховувати дзвінки можна і за допомогою хибної базової станції. Суть цього методу полягає в наступному: зазвичай телефон ловить найближчу базову станцію оператора зв'язку. Якщо така станція – це спецобладнання зловмисника, то ваш телефон направлятиме весь трафік на неї. Чим ближче ви знаходитесь до помилкового пристрою, тим вірогідніше, що ви до нього підключитеся. Як переконує фахівець, телефон буде відсвічувати спеціальними індикаторами – повідомляти, що з'єднання не захищене.

Оптичний та оптоелектронний канал витоку інформації.

Оптичний канал

В оптичному каналі отримання інформації можливо шляхом:

– візуального спостереження;

– фото-відеозйомки;

– використання видимого та інфрачервоного діапазонів для передачі інформації від приховано встановлених мікрофонів та інших датчиків.

Як середовище поширення в оптичному каналі витоку інформації виступають:

– безповітряний простір;

– атмосфера;

– оптичні світловоди.

Безповітряний простір, що є середовищем поширення витоку інформації, виникає під час спостереження за наземними об'єктами з космічних апаратів.

До властивостей середовища поширення, що впливають на довжину каналу витоку, належать:

– характеристики прозорості середовища розповсюдження;

– спектральні характеристики світла.

Оптоелектронний канал витоку інформації

Волоконно-оптичний зв'язок, що отримав розвиток після винаходу в 1960 лазера – висококогерентного джерела випромінювання оптичного діапазону, і демонстрації в 1970 оптичних волокон з низькими втратами (20 дБ/км), що дозволили здійснювати передачу інформації на середні відстані, на сьогодні є основним видом високошвидкісної комунікацій на довгі та наддовгі дистанції. Використання як носії інформації коротких лазерних імпульсів інфрачервоного діапазону (~200 ТГц) забезпечує швидкість передачі в кілька десятків Гбіт/с, що перевищує максимальні швидкості радіозв'язку та зв'язку за допомогою електричних кабелів. Результатом стало створення трансокеанських та трансконтинентальних ліній зв'язку завдовжки десятки тисяч кілометрів. Слід очікувати, що найближчими роками волоконно-оптичні лінії зв'язку (ВОЛЗ) замінять й інші види магістральних ліній передачі. У зв'язку з цим постає питання про захищеність ВОЛЗ.

Оптичне волокно являє собою діелектричний шаруватий циліндричний хвилевід круглого перерізу, який зазвичай знаходиться всередині захисної оболонки. Показник заломлення серцевини волокна (n_1) більший за показник заломлення оболонки (n_2). Хвильові властивості волокна засновані на явищі повного внутрішнього відбиття. Якщо кут падіння світла на межу розділу серцевина-оболонка (φ_1) задовольняє умові:

$$n_1 \sin(\varphi_1) > n_2$$

то світло не може залишити серцевину хвилеводу.

Волоконно-оптичні лінії передачі відрізняються високою захищеністю через те, що:

1. Електромагнітне поле напрямної хвилі локалізовано поблизу серцевини волокна на масштабах десятків мікрометрів, що ускладнює доступ до інформації в порівнянні з надвисокими частотами (НВЧ) хвилеводами і радіосигналами.

2. Пошкодження хвилеводу в більшості випадків призводить до обриву з'єднання та миттєвого виявлення несанкціонованого доступу

3. Компанії, що займаються волоконно-оптичними лініями передачі забезпечують високу фізичну захищеність кабелів. Так, наприклад, трансокеанські лінії зв'язку на шельфі покриті товстою металевою оболонкою.

4. Оптичні канали зв'язку характеризуються високою швидкістю передачі (сотні Гбіт/с), що досягається використанням коротких світлових імпульсів (десятки і сотні пікосекунд). У зв'язку з цим для перехоплення інформації потрібні високочутливі та швидкі детектори, що робить несанкціонований доступ надзвичайно дорогим.

5. У кабелі лінії зв'язку зазвичай знаходиться значна кількість окремих волокон, що призводить до того, що доступ до кожного з хвилеводів окремо дуже утруднений.

6. Волоконно-оптичні лінії передач (ВОЛП) захищені від перешкод, створюваних джерелами електромагнітного випромінювання, стійкі до коливань температури та вологості.

Раніше вважалося, що ВОЛП мають підвищену скритність, проте завжди існує принципова можливість знімання інформації, що передається по оптичних

каналах зв'язку. Тим не менш, існують методи, які потенційно дозволяють здійснити перехоплення інформації. Волоконно-оптичні лінії зв’язку (ВОЛЗ) складаються із стаціонарного обладнання, що розміщується на сертифікованих об'єктах, та лінійного тракту, що представляє собою волоконно-оптичні кабелі та підсилювачі оптичного сигналу, які встановлюються кожні 50-80 км. Захист першої складової забезпечується так само як і захист будь-якого аналогічного об'єкта і має мало особливостей, тоді як другу складову захистити на всьому її протязі неможливо, через неможливість охопити десятки тисяч кілометрів.

Очевидним способом підвищення захищеності ВОЛП є зниження рівня сигналу, що передається аж до використання одного або кількох фотонів для кодування одного біта інформації, проте цей метод впирається у фізичні обмеження джерел і детекторів сигналів, а також у шумозахищеність і не дасть принципових поліпшень безпеки оптичних з'єднань найближчим часом.

Методи знімання інформації

Основні фізичні принципи формування каналів витоку інформації у ВОЛП можна поділити на такі типи:

– пасивні методи (засновані на реєстрації випромінювання з бокової поверхні волокна);

– активні методи (засновані на реєстрації випромінювання, що виводиться через бічну поверхню волокна за допомогою спеціальних засобів);

– компенсаційні методи (базуються на реєстрації випромінювання, що виводиться через бічну поверхню за допомогою спеціальних засобів, з подальшим формуванням випромінювання та введення його у волокно, яке компенсує втрати потужності при виведенні випромінювання).

Методи першого типу засновані на тому, що навіть у стаціонарному режимі в звичайних умовах невелика частина розсіяного випромінювання все ж таки проникає за межі волокна (тобто випромінюється) і може бути каналом витоку інформації. Основною ідеєю є збільшення інтенсивності цього випромінювання. Для несанкціонованого доступу до інформації з використанням таких методів необхідно використовувати місця посиленого бічного випромінювання, тобто слід знімати випромінювання в місцях згинів, а також у місцях зварних з'єднань і з'єднань волокна з підсилювачами. Однак значна потужність випромінювання спостерігається лише в місцях роз'ємних з'єднань, тобто в комутаційних центрах, що ускладнює несанкціонований доступ.

Методи другого типу виводять зазвичай більшу потужність, але при цьому відбувається зміна параметрів хвилі, що поширюється в хвилеводі (значно падає потік енергії, виникає відбита хвиля, змінюється модова структура хвилі і т. д.), що може призвести до виявлення несанкціонованого доступу. Такими методами є, наприклад: механічний вигин волокна, підключення фотоприймача за допомогою відгалужувача, вдавлювання зондів в оболонку, безконтактне з'єднання волокна, шліфування та розчинення оболонки.

Природним бажанням є поєднати скритність та ефективність. Методи третього типу покликані реалізувати цю ідею. Однак їх реалізація є достатньо складною у зв'язку з наявністю принципових обмежень. Так, наприклад,

виведення випромінювання з бічної поверхні волокна, формування і зворотне введення хвилі, яка компенсує потужність, що виводиться, повинні здійснюватися з високою ефективністю до одиниці, проте, розподіл параметрів волокна носить імовірнісний характер, що заважає досягти бажаної скритності. Технічні реалізації таких пристроїв, що дозволяють на практиці використовувати компенсаційні способи знімання інформації, в даний час не відомі.

Способи захисту

У зв'язку з наявністю потенційної загрози несанкціонованого знімання інформації у всьому світі ведуться роботи із захисту ВОЛП. Виділяють три основних напрямки:

– розробка технічних засобів захисту від несанкціонованого доступу до інформаційних сигналів;

– розробка технічних засобів контролю за несанкціонованим доступом до інформаційного оптичного випромінювання.

До першого і другого напрямку відноситься метод, заснований на використанні «кодового зашумлення» сигналів, що передаються. Принцип роботи методу полягає в тому, що при вже невеликому зниженні потужності сигналу, що детектується, яке може бути викликане підключенням до лінії пристрою знімання інформації, в детектованому на одному з кінців волокна цифровому сигналі значно зростає кількість помилок, далі або передача інформації обривається, або швидко виявляється порушник.

Система **IDOC** (Intrusion Detection Optical Communications System) – один із ефективних методів захисту, розроблений у США в 1991 році компанією Hughes Aircraft. В основу методу творці поклали аналіз модового складу оптичного випромінювання, що передається. Система IDOC дозволяла захищати ВОЛЗ малої протяжності. Система захисту складалася з розроблених компанією спеціальних волокон та двох модемів FAM-131 (Fiber Alarmed Modem). IDOC-система легко виявляє несанкціоновані підключення та миттєво припиняє передачу інформації. IDOC стала першою некриптографічною системою для секретного зв'язку, яка була сертифікована Агентством національної безпеки США.. Єдиним недоліком стала нездатність системи передачі інформації на великі відстані, оскільки використовувалося одномодовое волокно.

Ведуться розробки з впровадження методів з використанням режиму динамічного хаосу, який дозволяє забезпечити передачу інформаційних сигналів у вигляді псевдохаотичних коливань частоти та оптичної амплітуди несучої. Накладення на такий сигнал, що знімається з бокової поверхні волокна, шумового сигналу, який обов'язково буде присутній, дуже ускладнює несанкціонований доступ.

Актуальним поки що залишається і механічний захист волокна. Так, наприклад, може бути використаний захист від вигину (волокно ламається при сильному згинанні). Оптичні кабелі упаковуються в спеціальну оболонку, яка при ушкодженні просигналізує вплив.

Методи квантової криптографії можуть забезпечити високий рівень захисту від несанкціонованого доступу до інформації, що досягається завдяки передачі сигналів у вигляді окремих фотонів. Така схема дозволяє виявити факт

перехоплення фотонів зміни ймовірнісних характеристик послідовності фотонів на виході.

У 1993 році лабораторія компанії British Telecom продемонструвала одну з перших реалізацій практичної схеми квантового каналу на базі волокна довжиною 10 км, яка базувалася на принципі фазової модуляції [6] [7]. Було досягнуто ефективну швидкість передачі в 60 кбіт/с.

У 1990-ті роки були спроби створення ВОЛЗ з використанням як носії сигналів оптичних солітонів.. Солітони мають властивість збереження форми огинаючої імпульсу при поширенні по волокну. Солітони пружно стикаються один з одним, не втрачаючи енергії, іншими словами вони можуть бути схожими на інші солітони, не помічаючи їх. Якщо енергія солітонного імпульсу поменшає деякого порогового значення, він «розвалюється». Таким чином, якщо через бічну поверхню волокна виводиться енергія (здійснюється несанкціонований доступ), то приймач на одному з кінців волокна може виявити порушення конфіденційності інформації, що передається зі зміни форми оптичних імпульсів або їх повної відсутності. Однак солітонні лінії передачі інформації не знайшли широкого застосування через обмеження на швидкість передачі інформації та розробку більш швидких ВОЛП.

Методи несанкціонованого доступу

Моди циліндричного хвилеводу

Волокна можна розділити на два види: одномодові та багатомодові. В одномодовому волокні може поширюватися лише одна мода (HE_{11}), завдяки чому відсутня міжмодова взаємодія, що покращує дисперсійні характеристики, необхідні передачі сигналу великі відстані.

Втрати на вигині волокна

Якісний розгляд питання говорить про те, що якщо кут падіння світла на поверхню розділу серцевини та оболонки волокна буде зменшений і стане меншим за критичний кут, то світло почне виходити з ядра і випромінюватись на місці вигину. Більш правильне пояснення полягає в тому, що неоднорідності в геометрії волокна, викликають зв'язування нерадіаційних (напрямних і радіаційних (випромінювальних) мод. Внаслідок чого ведена мода втрачає енергію і сигнал слабшає. Далі випромінюваний сигнал можна детектувати. Одна з можливостей здійснення цього методу – це вигин волокна

Параметричний канал витоку інформації

Внаслідок впливу акустичного поля змінюється тиск на всі елементи високочастотних генераторів технічних засобів прийому інформації (ТЗПІ) та допоміжних технічних засобів й систем (ДТЗС). При цьому змінюється взаємне розташування елементів схем, проводів у котушках індуктивності, дроселів тощо, що може призвести до змін параметрів високочастотного сигналу, наприклад, його модуляції інформаційним сигналом. Тому цей канал витоку інформації називається параметричним. Найчастіше спостерігається паразитна модуляція інформаційним сигналом випромінювань гетеродинів радіоприймальних і телевізійних пристроїв, що у приміщеннях, де ведуться конфіденційні розмови.

Параметричний канал витоку інформації може бути реалізований шляхом високочастотного (ВЧ) опромінення приміщення, де встановлені закладні пристрої (ЗП), що мають елементи, параметри яких (наприклад, добротність і резонансна частота об'ємного резонатора) змінюються під дією акустичного (мовного) сигналу.

При опроміненні приміщення потужним ВЧ сигналом, у такому ЗП при взаємодії опромінюючого електромагнітного поля зі спеціальними елементами закладки (наприклад, чвертьхвильовим вібратором) відбувається утворення вторинних радіохвиль, тобто перевипромінювання електромагнітного поля. А спеціальний пристрій закладки (наприклад об'ємний резонатор) забезпечує амплітудну, фазову або частотну модуляцію перевідбитого сигналу за законом зміни мовного сигналу.

Для реалізації такого каналу необхідні спеціальний передавач із спрямованим випромінюванням та приймач.

20.2. Методи та засоби технічного захисту інформації

Пасивні та активні методи і засоби захисту інформації від витоку технічними каналами

Усі заходи захисту інформації від витоку акустичним, віброакустичним та оптоелектронним каналами зводяться до зниження рівня акустичних/віброакустичних сигналів (озвучення інформації) до певного співвідношення сигнал/завада. Ступень захисту інформації визначається відповідними нормами.

Необхідного співвідношення сигнал/завада можна досягнути пасивними або активними заходами:

– **Пасивні заходи захисту інформації** спрямовані на підвищення звукоізоляції огороджувальних конструкції (далі – ОК) (встановлення металопластикових вікон, ущільнювачів дверей, створення «плаваючої підлоги», встановлення акустичних фільтрів у повітроводи тощо).

– **Активні заходи захисту інформації** спрямовані зниження співвідношення сигнал/завада до норми шляхом створення акустичної\віброакустичної завади на межі огороджувальних конструкцій.

Класифікація технічних засобів захисту

Технічними називаються такі засоби захисту інформації, у яких основна захисна функція реалізується технічним пристроєм (комплексом або системою).

*Безсумнівними **перевагами** технічних засобів захисту інформації (ТЗЗІ) є*:

- досить висока надійність;
- досить широке коло завдань;
- можливість створення комплексних систем ЗІ (КСЗІ);
- гнучке реагування на спроби несанкціонованого впливу;
- традиційність використовуваних методів здійснення захисних функцій.

*Основні **недоліки** ТЗЗІ полягають у наступному:*

– висока вартість багатьох засобів;

– необхідність регулярного проведення регламентних робіт і контролю;

– можливість видачі фіктивних тривог.

Системну класифікацію ТЗЗІ зручно провести по наступній сукупності критеріїв:

– здійсненна функція захисту;

– ступінь складності пристрою;

– спряженість із засобами обчислювальної техніки (ОТ).

Наведені значення критеріїв інтерпретуються в такий спосіб.

Спряженість із засобами ОТ.

– *Автономні* – засоби, що виконують свої захисні функції незалежно від функціонування засобів ОТ, тобто повністю автономно.

– *Сполучені* – засоби, виконані у вигляді самостійних пристроїв, але виконуючі захисні функції в сполученні (спільно) з основними засобами ОТ.

– *Вбудовані* – засоби, які конструктивно включені до складу апаратури ОТ.

Виконувана функція захисту.

– *Зовнішній захист* – захист від впливу дестабілізуючих факторів, що проявляються за межами зони ресурсів.

– *Упізнавання* – специфічна група засобів, призначених для впізнавання людей по різних індивідуальних характеристиках.

– *Внутрішній захист* – захист від впливу дестабілізуючих факторів, що проявляються безпосередньо в засобах обробки інформації.

Ступінь складності пристрою.

– *Прості пристрої* – нескладні прилади й пристосування, що виконують окремі процедури захисту.

– *Складні пристрої* – комбіновані агрегати, що складаються з деякої кількості простих пристроїв, здатні до здійснення складних процедур захисту.

– *Системи* – закінчені технічні об'єкти, здатні здійснювати деяку комбіновану процедуру захисту, що має самостійне значення.

Якщо кожний елемент класифікаційної структури представити як група ТЗЗІ, то повний арсенал цих засобів буде включати 27 самостійних груп.

Відповідно до класифікації у функціональному відношенні, що *очолює значення має класифікація по виконуваній функції*. Класифікація ж за критеріями спряженості й ступеня складності відбиває, головним чином, лише особливості конструктивної й організаційної реалізації ТЗЗІ.

Як уже було сказано, виділяють три макрофункції захисту, виконуваних ТЗЗІ: зовнішній захист, упізнавання й внутрішній захист. Подальша деталізація функціональної класифікації ТЗЗІ приводить до виділення 11-і груп (рисунок 21.2). ТЗЗІ, що входять у ці групи, можуть бути різної складності й різного виконання. До теперішнього часу розроблена велика кількість різних ТЗЗІ, багато які з них випускаються серійно.



Рисунок 21.2 – Класифікація ТЗЗІ по функціональному призначенню

Технічні засоби захисту території й об'єктів

Для керування доступом у приміщення широке поширення одержали замки з кодовим набором. Крім того, для захисту приміщень широко використовуються датчики, які можуть бути розділені на три групи:

- датчики для виявлення *спроб проникнення* на територію об'єкта або в контрольоване приміщення;
- датчики для виявлення *присутності людини* в приміщенні;
- датчики для виявлення *переміщення* охоронюваного предмета.

Відповідно до вимог по технічному захисту на кожному охоронюваному об'єкті встановлюються наступні типи пожежно-захисних систем:

- зовнішні системи сигналізації проникнення;
- внутрішні системи сигналізації проникнення;
- системи сигналізації пожежної охорони.

Внутрішні системи сигналізації проникнення діляться на однорубіжні, дворубіжні й багатозоні.

Структурна схема однорубіжної охоронної системи сигналізації припускає побудову шлейфа сигналізації з сповіщувачами, що дають інформацію на пульт центрального спостереження (ПЦС) про порушення шлейфа або його обриві, а також можливість управляти виносними світловими й звуковими сигналізаторами.

Дворубіжна охоронна система сигналізації припускає організацію двох рубежів охорони об'єкта.

Для першого рубежу доцільно використовувати сповіщувачи, що забезпечують розмикання контактів, а для другого – охоронні сповіщувачи об'ємної дії. Перевага другого варіанта полягає в уточненій селекції сигналів охоронних сповіщувачей, які спрацьовують на другому рубежі охорони.

Структурна схема організації багатозоної системи захисту дозволяє здійснювати охорону до шістнадцяти зон усередині об'єкта. Використовується дворубіжна охоронна система сигналізації з можливістю вимикання деяких зон, причому охорона інших утримується в робочому стані.

Зовнішні системи сигналізації проникнення служать для надійної сигналізації про проникнення через зони, що захищаються, постачені огорожами (на особливих об'єктах таких огорож може бути дві).

Для захисту приміщень широко застосовуються також лазерні й оптичні системи, датчики яких спрацьовують при перетинанні порушником світлового променя.

Пристрої й системи впізнавання застосовуються, в основному, у системах керування доступом у приміщення, що захищаються. Це завдання вирішується з використанням не тільки фізичних, але й апаратних і програмних засобів.

Акустичні засоби захисту

Для визначення норм захисту приміщень по акустичному каналі використовується наступна розрахункова формула:

$$\mathbf{D = L_C - Q - L_П}\ [\text{дБ}],$$

де **D** – співвідношення сигнал/шум; $\mathbf{L_C}$ – рівень мовного сигналу; $\mathbf{L_П}$ – рівень перешкод; **Q** – звукоізолюючі характеристики конструкцій, що обгороджують.

Рівень перешкод у приміщенні становить 15 дб, поза приміщенням – 5 дб.

Якщо необхідно робити захист приміщення по акустичному каналі, варто впливати на середовище поширення. Для цієї мети використовуються ***акустичні генератори шуму***. Крім того, генератори шуму широко використовуються для оцінки акустичних властивостей приміщень.

Технічні засоби ***ультразвукового захисту*** приміщень з'явилися порівняно недавно, але зарекомендували себе, як надійні засоби ТЗ акустичної інформації. Відмінною рисою цих засобів є вплив на мікрофонний пристрій і його підсилювач досить потужним ультразвуковим сигналом, що викликає блокування підсилювача або виникнення значних нелінійних перекручувань, що приводять, в остаточному підсумку, до порушення працездатності мікрофонного пристрою.

Особливості захисту від радіозакладок

При розробці вимог до апаратури придушення радіовипромініючих пристроїв, що підслухують, використовується такий показник, як коефіцієнт розбірливості мови **(**W_C). На практиці використовуються нормативні значення $\mathbf{W_C}$, при яких:

- виключається відновлення мовних повідомлень ($W_C \leq 0{,}2$);
- забезпечується відновлення мовних повідомлень ($W_C \geq 0{,}8$).

Апаратура придушення являє собою генератор (передавач) шумових перешкод, що встановлюється в зашумляємому приміщенні. При цьому відстань від радіовипромініючих закладок до прийомних пристроїв перехоплення їхніх випромінювань буде практично таке ж, як від передавача шумових перешкод до цих прийомних пристроїв, що придушуються. При такому тактичному застосуванні передавача перешкод повністю знімається невизначеність щодо розміщення прийомних пристроїв перехоплення випромінювань радіозакладок, забезпечується простота використання апаратури придушення, висока надійність і ефективність протидії.

Захист від убудованих і вузьконаправлених мікрофонів

Для захисту від вузьконаправлених мікрофонів рекомендуються наступні міри:

– при проведенні нарад варто обов'язково закривати вікна й двері (найкраще, щоб кімната для нарад являла собою ізольоване приміщення);

– для проведення переговорів потрібно вибирати приміщення, стіни яких не є зовнішніми стінами будинку;

– необхідно забезпечити контроль приміщень, що перебувають на одному поверсі з кімнатою для нарад, а також приміщень, що перебувають на суміжних поверхах.

Із застосовуваних зараз ТЗЗІ можна виділити наступні основні групи:

– генератори акустичного шуму;

– генератори шуму в радіодіапазоні;

– сканери – спеціальні приймачі для виявлення радіовипромінювань;

– нелінійні локатори;

– нелінійні локатори провідних ліній;

– детектори працюючих магнітофонів;

– скремблери (системи захисту телефонних переговорів);

– аналізатори спектра;

– частотоміри;

– детектори мережі 220 В 50 Гц;

– детектори підключень до телефонної лінії;

– комплекси, що забезпечують виконання декількох функцій по “очищенню приміщень”;

– програмні засоби захисту комп'ютерів і мереж;

– системи й засоби захисту від несанкціонованого доступу, у тому числі, системи біометричного доступу.

Класифікація пристроїв пошуку технічних засобів розвідки може бути наступною.

1. Пристрої пошуку активного типу:

– нелінійні локатори (досліджують відгук на вплив електромагнітним полем);

– рентгенметри (просвічують за допомогою рентгенівської апаратури);

– магніто-резонансні локатори (використовують явище орієнтації молекул у магнітному полі).

2. Пристрої пошуку пасивного типу:

– металошукачі;

– тепловізори;

– пристрої й системи пошуку по електромагнітному випромінюванню;

– пристрої пошуку за зміноюі параметрів телефонної лінії (напруги, індуктивності, ємності, добротності);

– пристрої пошуку за зміною магнітного поля (детектори записуючої апаратури).

Для захисту приміщень широко використовуються ***пристрої постановки перешкод***. Постановники перешкод різного виду й діапазону є ефективними засобами для захисту переговорів від прослуховування, а також для глушіння радіомікрофонов і зашумлення провідних ліній.

Сигнали перешкоди радіодіапазону прийнято ділити на ***загороджувальні*** й ***прицільні***. Загороджувальна перешкода ставиться на весь діапазон частот, у якому передбачається робота радіопередавача, а прицільна – точно на частоті цього радіопередаючого пристрою.

Захист ліній проводового зв'язку

Для захисту ліній зв'язку від наведень необхідно розмістити лінію в що екранує оплітку або фольгу, заземлену в одному місці, щоб уникнути протікання по екрані струмів, викликаних нееквіпотенціальністю точок заземлення. Для захисту ліній зв'язку від наведень необхідно мінімізувати площу контуру, утвореного прямим і зворотним проведенням лінії. Якщо лінія являє собою одиночне проведення, а зворотний струм тече по деякій заземлюючій поверхні, то необхідно максимально наблизити проведення до поверхні. Якщо лінія утворена двома проводами, має більшу довжину, то її необхідно скрутити, утворивши біфіляри (кручену пару). Лінії, виконані з екранованого проведення або коаксіального кабелю, по оплітці якого протікає зворотний струм, також повинні відповідати вимогам мінімізації площі контуру лінії.

Методи й засоби захисту проводових телефонних ліній

Всі системи захисту проводових телефонних ліній діляться на пасивні й активні.

Пасивний захист

До засобів пасивного захисту відносяться фільтри й інші пристосування, призначені для зриву деяких видів прослуховування приміщень за допомогою телефонних ліній, що перебувають у режимі відбою. Ці засоби можуть установлюватися в розрив телефонної лінії або вбудовуватися безпосередньо в ланцюзі телефонного апарата.

Крім зазначених, широко застосовуються різні ***індикаторні прилади***. Принцип дії індикаторних пристроїв заснований на вимірі й аналізі параметрів телефонних ліній.

Прилади для постановки активної загороджувальної перешкоди

Ці прилади призначені для захисту телефонних ліній практично від всіх видів пристроїв, що прослуховують. Досягається це шляхом подачі в лінію додаткових сигналів (загороджувальної перешкоди) і зміни стандартних параметрів телефонної лінії (звичайно в розумних межах змінюється постійна складова напруги в лінії й струм у ній) у всіх режимах роботи.

Захист факсимільних і телефонних апаратів, концентраторів

Для того щоб повністю придушити всі види випромінювань, створюваних ТА, необхідно відфільтрувати випромінювання в лінійних проводах, що

відходять від апарата, і проводах мікротелефону, а також забезпечити достатню екранування внутрішньої схеми ТА. Екранування й фільтрація всіх проводів, що відходять від апарата, можливі тільки при значній переробці конструкції ТА й зміні його електричних параметрів. Із усього сказаного треба вивід – щоб захистити ТА, необхідно виконати наступні заходи:

- захистити ланцюг мікротелефону;
- захистити ланцюг дзвінка;
- захистити двопроводну лінію телефонної мережі.

Екранування приміщень

Для повного усунення наведень від технічних засобів передачі інформації (ТЗПІ) у приміщеннях, лінії яких виходять за межі контрольованої зони, необхідно не тільки придушити їх у проводах, що відходять від джерела, але й обмежити сферу дії електромагнітного поля, створюваного в безпосередній близькості від джерела системою його внутрішньої електропроводки. Це завдання вирішується шляхом застосування екранування. Екранування підрозділяється на:

- електростатичне;
- магнитостатичне;
- електромагнітне.

Захист від навмисного силового впливу (НСВ)

Під ***навмисним силовим впливом*** (НСВ) розуміється навмисне створення різкого сплеску напруги в мережі живлення з такими амплітудою, тривалістю й енергією сплеску, які здатні привести до збоїв у роботі встаткування або до його деградації. Для НСВ використовуються спеціальні технічні засоби (ТЗ), які підключаються до мережі безпосередньо за допомогою гальванічного зв'язку, через конденсатор або трансформатор.

Захист від НСВ по ланцюгах живлення

ПЕОМ або інше електронне устаткування автоматизованих систем (АС) має два шляхи значимих для проникнення енергії НСВ по мережі живлення: *кондуктивний шлях* через джерело вторинного електроживлення й *наведення* через паразитні ємнісні й індуктивні зв'язки, як внутрішні, так і між спільно прокладеними кабелями й інформаційними лініями зв'язку. Основними принципами захисту від НСВ по ланцюгах живлення є наступні.

1. Із залученням кваліфікованих фахівців-електриків необхідно проаналізувати схему електропостачання об'єкта для виявлення можливих каналів для нападу на об'єкт по ланцюгах живлення.

2. Схема електропостачання об'єкта повинна бути розділена на зони, у яких можна організувати ті або інші заходи щодо захисту.

3. На всі фідери, які виходять за межі зон, повинні бути встановлені групові пристрої захисту від НСВ.

4. При монтажі на об'єкті виділеної мережі живлення для АС необхідно розетки, щитки живлення та інше встаткування розміщати в приміщеннях з устаткуванням АС і в приміщеннях, що перебувають під контролем.

5. Після завершення монтажу електропостачання знімається своєрідний “портет” мережі за допомогою аналізатора неоднорідності лінії.

6. Доступ до щитів живлення й інших елементів електроустаткування будинку повинен бути обмежений відповідними документами й інструкціями, а також технічними заходами.

7. Все електроустаткування (у тому числі й побутовому призначенні) повинне ретельно перевірятися.

8. Бажано організувати на об'єкті цілодобовий моніторинг мережі електроживлення за допомогою відповідних приладів, що реєструють, і одночасну реєстрацію в журналі всіх збоїв і ушкоджень устаткування з обов'язковою фіксацією часу виникнення збоїв і характеру дефектів.

9. ТЗ НСВ із ємнісним накопичувачем мають демаскуючі акустичні ознаки – при розрядці конденсатори генерують акустичний імпульс. Це обставина можна використовувати для пошуку ТЗ НСВ такого типу.

10. При закупівлях устаткування АС необхідно звертати увагу на ступінь його захисту від імпульсних перешкод.

Захист від НСВ по комунікаційних каналах

Найбільший збиток при нападі із застосуванням ТЗ НСВ наносяться об'єктам, у яких АС із безперервним процесом обробки потоків інформації є ядром системи (до таких об'єктів відносяться системи зв'язку, особливо цифрові, системи обробки банківських даних, керування повітряним рухом і т.п.). Досить ефективний напад із застосуванням ТЗ НСВ на системи, що забезпечують безпеку об'єкта: вивід з ладу встаткування системи безпеки може представити зловмисникам тимчасове вікно тривалістю до декількох доби (на період заміни або ремонту встаткування) для здійснення злочинних дій.

Для забезпечення захисту АС від НСВ по комунікаційних каналах (головним чином мова йде про провідні лінії зв'язку) необхідне проведення певних заходів організаційного й технічного характеру. Їхня деталізація вимагає прив'язки до конкретного об'єкта.

1. Необхідно перевірити із залученням кваліфікованих фахівців схему внутрішніх і зовнішніх комунікаційних каналів об'єкта для виявлення можливих шляхів для нападу на об'єкт по провідних лініях зв'язку.

2. Схема внутрішніх і зовнішніх комунікаційних каналів об'єкта повинна бути розділена на зони, у яких можна реалізувати ті або інші заходи щодо захисту.

3. На всі провідні лінії зв'язку, які виходять за межі зон, підконтрольних службі безпеки об'єкта, повинні бути встановлені пристрої захисту від НСВ для кожного провідника ліній зв'язку.

4. Після завершення монтажу кабельних комунікацій і ВУС знімається “портрет” комунікаційної мережі за допомогою аналізатора неоднорідностей лінії зв'язку.

5. Доступ до міні-АТС, крос-панелей і інших елементів комунікаційних каналів зв'язку повинен бути обмежений відповідними документами й технічними заходами, а поточне обслуговування встаткування й ремонтних робіт необхідно робити під контролем співробітників режимної служби.

6. При проектуванні схем розміщення й монтажі комунікаційного встаткування АС необхідно усувати потенційні можливості для атаки на об'єкт за допомогою ТЗ НСВ. При закупівлях комунікаційного встаткування для АС необхідно звертати увагу на ступінь його захисту від імпульсних перешкод.

7. При побудові схеми захисту об'єкта доцільно виділити три рубежі:

– рубіж I – захист по периметрі об'єкта всіх комунікаційних каналів для запобігання зовнішньої погрози нападу з використанням ТЗ НСВ;

– рубіж II – поетапний захист для локалізації ТЗ НСВ, стаціонарно встановлених усередині охоронюваного об'єкта або пронесених усередину його для організації однократної атаки;

– рубіж III – індивідуальний захист найбільш відповідальних елементів АС.

Для невеликих об'єктів рубіж I може відсутній, а рубіж II – скоротитися.

8. Для *першого рубежу*, як мінімум, необхідно встановити захист всіх провідних ліній зв'язку від перенапруги за допомогою повітряних розрядників і варисторів (аналогічні схеми застосовуються для захисту від індукованих розрядів блискавки).

Для *другого рубежу* захисту найбільше доцільно використовувати комбіновані низькопорогові перешкодозахищені схеми.

9. Для *третього рубежу* необхідно застосовувати схеми захисту, максимально наближені до обладнання, яке захищається.

10. Після монтажу системи захисту від НСВ по комунікаційних каналах цю систему й АС у цілому необхідно випробувати на реальні впливи.

Захист від прослуховування мобільного зв’язку

Для того, щоб мінімізувати ризик злому телефону, експерти з кібербезпеки наполягають на дотриманні таких правил:

1. Вчасно оновлювати операційну систему смартфона, що включає і автоматичне оновлення патчів безпеки.

– Увімкнути PIN-код на SIM-картку, а не лише на гаджет. Це дасть додатковий захист від злому телефону та встановлення шпигунської програми.

2. Встановити двокрокову перевірку в месенджерах.

– Не завантажувати програми з неперевірених джерел лише з Google Play Market або App Store.

– Видалити зі смартфона ті програми, якими ви давно не користуєтесь. Адже вони, як і раніше, передають дані з вашого смартфона на сторонні сервери.

– Перевірити, доступ до якої інформації вже мають встановлені програми: до камери, мікрофону, галереї. Заблокуйте непотрібні функції.

– Не встановлювати на телефон програми віддаленого керування типу Team Viewer.

Експерти не радять не використовувати однакові номери у месенджерах, соціальних мережах та пошті. На їх думку, **Telegram, WhatsApp чи Viber краще активувати на іноземні номери.** При цьому раз на півроку не забувати поповнювати мобільний рахунок і робити дзвінки за ними за кордоном.

Програми, які допоможуть захистити телефон від прослуховування

Існують наступні програми в Google Play Market та App Store, які позиціонують себе як захист телефону від злому та прослуховування.

EAGLE Security FREE 2.0

– захищає від прослуховування через хибні базові станції;

– контролює, які із встановлених додатків мають доступ до камери та мікрофону;

– блокує доступ небажаного ПЗ до камери та мікрофону.

Детектор шпигунського ПЗ (антишпигунський сканер)

– блокує шпигунські програми.

Anti Spy – Сканер програм-шпигунів

– бореться зі шпигунськими програмами за допомогою штучного інтелекту.

Paranoia Access – анти шпигун

– глушить диктофон від прослуховування.

Система контролю та управління доступом (СКУД)

Система контролю та управління доступом, **СКУД** (англ. *Physical Access Control System, PACS*) – сукупність програмно-апаратних технічних засобів контролю та засобів управління, що мають на меті обмеження та реєстрацію входу-виходу об'єктів (людей, транспорту) на заданій території через «точки проходу»: Двері, ворота, КПП.

Основне завдання – управління доступом на задану територію (кого пускати, в який час і яку територію), включаючи:

– обмеження доступу на задану територію;

– ідентифікацію особи, яка має доступ на задану територію.

Додаткові завдання:

– облік робочого часу;

– розрахунок заробітної плати (при інтеграції із системами бухгалтерського обліку);

– ведення бази персоналу/відвідувачів;

– інтеграція із системою безпеки, наприклад:

- із системою відеоспостереження для поєднання архівів подій систем, передачі системі відеоспостереження сповіщень про необхідність стартувати запис, повернути камеру для запису наслідків зафіксованої підозрілої події;
- з системою охоронної сигналізації (СОС), наприклад, для обмеження доступу до приміщень, що стоять на охороні, або для автоматичного зняття та постановки приміщень на охорону.
- з системою пожежної сигналізації (СПС) для отримання інформації про стан пожежних сповіщувачів, автоматичне розблокування евакуаційних виходів та закриття протипожежних дверей у разі пожежної тривоги.

На особливо відповідальних об'єктах мережа пристроїв СКУД виконується фізично не пов'язаною з іншими інформаційними мережами.

Запобіжні пристрої

Встановлюються на двері:

– Електрозасувки – їх зазвичай встановлюють на внутрішні двері (внутрішньоофісні і т. п.) Електрозащілки, як і інші типи замків, бувають напругою, що відкриваються (тобто двері відкриваються при подачі напруги живлення на замок), і напругою, що закриваються (відчиняються, як тільки з них знімається напруга живлення, тому рекомендовано для використання пожежною інспекцією).

– Електромагнітні замки – практично всі замикаються напругою, тобто придатні для встановлення на шляхах евакуації під час пожежі.

– Електромеханічні замки – досить стійкі до злому (якщо міцний замок механічно), багато хто має механічний перевзвод (це означає, що якщо на замок подали відкриваючий імпульс, він буде розблокований до тих пір, поки двері не відчинять).

Встановлюються на проходах/проїздах:

Турнікет-трипод поясний із зчитувачем системи контролю доступу

– Турнікети використовуються на прохідних підприємствах, суспільно значущих об'єктах (стадіони, вокзали, метро, еякі держустанови) скрізь, де потрібно організувати контрольований прохід великої кількості людей. Турнікети поділяються на два основні типи: поясні та повноростові. Якщо поряд з турнікетом немає вільного проходу, що швидко відкривається (на випадок пожежі), поясний турнікет повинен бути обладнаний т.з. планками «антипаніка» – планками, що зламуються зусиллям нормальної людини (вимога пожежної інспекції).

– Шлюзові кабіни – використовуються в банках, на режимних об'єктах (на підприємствах із підвищеними вимогами до безпеки).

– Ворота та шлагбауми – переважно встановлюються на в'їздах на територію підприємства, на автомобільних парковках та автостоянках, на в'їздах на прибудинкову територію, у двори житлових будівель. Основна вимога – стійкість до кліматичних умов та можливість автоматизованого керування (за допомогою системи контролю доступу). Коли йдеться про організацію контролю доступу до проїзду, до системи пред'являються додаткові вимоги – підвищена дальність зчитування міток, розпізнавання автомобільних номерів (у разі інтеграції із системою відеоспостереження).

– Автоматичні дорожні бар'єри – використовуються для гарантованого запобігання несанкціонованому проїзду автотранспорту на територію, що захищається. Є заходами антитерористичного захисту, оскільки проїзд через піднятий бар'єр призводить до руйнування підвіски автомобіля.

Ідентифікатор

Основні типи виконання – картка, брелок, мітка. Є базовим елементом системи контролю доступу, оскільки зберігає код, який служить визначення прав («ідентифікації») власника. Це може бути Touch memory, безконтактна карта (наприклад, RFID-мітка), або застаріваючий тип карток з магнітною смугою. Як ідентифікатор можуть виступати також коди, що вводяться на клавіатурі, або окремі біометричні ознаки людини – відбиток пальця, малюнок сітківки або райдужної оболонки ока, тривимірне зображення обличчя.

Надійність (стійкість до злому) системи контролю доступу значною мірою визначається типом ідентифікатора, що використовується: наприклад, найбільш поширені безконтактні карти proximity можуть підроблятися в майстернях з виготовлення ключів на устаткуванні, наявному у вільному продажу. Тому для об'єктів, які потребують вищого рівня захисту, такі ідентифікатори не підходять. Принципово вищий рівень захищеності забезпечують RFID-мітки, у яких код карти зберігається у захищеній області й шифрується.

Крім безпосереднього використання в системах контролю доступу, RFID-мітки широко застосовуються і в інших областях. Наприклад, у локальних розрахункових системах (оплата обідів у їдальні та інших послуг), системах лояльності тощо.

Контролер

Автономний контролер – це «мозок» системи: саме контролер визначає, чи пропустити власника ідентифікатора у двері, оскільки зберігає коди ідентифікаторів зі списком прав доступу кожного з них у власній енергонезалежній пам'яті. Коли людина пред'являє (підносить до пристрою, що зчитує) ідентифікатор, лічений з нього код порівнюється з зберігається в базі, на підставі чого приймається рішення про відкриття дверей.

Мережевий контролер об'єднується в єдину систему з іншими контролерами та комп'ютером для можливості централізованого контролю та управління. У такому разі рішення про надання доступу може прийматись як контролером, так і програмним забезпеченням головного комп'ютера. Найчастіше об'єднання контролерів мережу здійснюється за допомогою промислового інтерфейсу RS-485 або локальної мережі Ethernet.

У випадках, коли необхідно забезпечити роботу контролера при аваріях електромережі, блок контролера забезпечується власним акумулятором або зовнішнім блоком резервного живлення. Час роботи від акумулятора може становити від кількох годин до кількох діб.

Зчитувач

Це пристрій, який отримує («зчитує») код ідентифікатора та передає його в контролер. Варіанти виконання зчитувача залежать від типу ідентифікатора: для «таблетки» – це два електричні контакти (у вигляді «лузи»), для proximity-карти – це електронна плата з антеною в корпусі, а для зчитування, наприклад, малюнку райдужної оболонки ока до складу зчитувача має входити камера. Якщо зчитувач встановлюється на вулиці (ворота, зовнішні двері будівлі, проїзд на територію автостоянки), то він повинен витримувати кліматичні навантаження – перепади температур, опади – особливо якщо йдеться про об'єкти в районах із суворими кліматичними умовами. А якщо існує загроза вандалізму, потрібна ще й механічна міцність (сталевий корпус). Окремо можна виділити зчитувачі для дальньої ідентифікації об'єктів (з відстанню ідентифікації до 50 м). Такі системи зручні на автомобільних проїздах, парковках, на в'їздах на платні дороги тощо. Ідентифікатори для таких зчитувачів, як правило, активні (містять вбудовану батарейку).

Конвертери середовища

Служать для підключення апаратних модулів СКУД один до одного та до ПК. Наприклад, є популярними конвертори RS-485 ↔ RS-232 та RS-485 ↔ Ethernet. Деякі контролери СКУД вже мають інтегрований інтерфейс Ethernet, що дозволяє без використання будь-яких додаткових пристроїв підключатися до ПК і зв'язуватися один з одним.

Допоміжне обладнання

Блоки безперебійного живлення, дверні доводчики, датчики відчинення дверей, кнопки, дроти, відеоспостереження і т.д.

Програмне забезпечення

Не є обов'язковим елементом системи контролю доступу, використовується у разі, коли потрібна обробка інформації про проходи, побудова звітів, або коли для початкового програмування, управління та збору інформації в процесі роботи системи необхідне мережне програмне забезпечення, яке встановлюється на один або кілька ПК, з'єднаних у мережа.

Усі СКУД можна віднести до двох великих класів або категорій: мережеві системи та автономні системи.

Популярні компанії виробники програмного забезпечення систем контролю та управління доступу: ITV Group, ZkTeco, PERCo, ControlGate, Hikvision, Bosh, Parsec, Bolid, RusGuard, HID Global, IronLogic, OVISION.

Мережеві системи

У мережі всі контролери з'єднані з комп'ютером, що дає безліч переваг для великих підприємств, але зовсім не потрібно для «однодверної» СКУД. Мережеві системи зручні для великих об'єктів (офіси, виробничі підприємства), оскільки керувати навіть десятком дверей, на яких встановлені автономні системи, стає надзвичайно важко. Незамінні мережеві системи у таких випадках:

– якщо необхідно реалізувати складні алгоритми допуску груп співробітників з різними привілеями до різних зон підприємства та мати можливість оперативно їх змінювати;

– якщо необхідно вибірково видаляти або створювати перепустки (мітки) для великої кількості точок проходу або для великої кількості співробітників (велика текучка та втрати пропусків);

– якщо необхідна інформація про події (архів подій), що відбулися раніше, або потрібен додатковий контроль у реальному часі. Наприклад, у мережній системі існує функція фотоверифікації: на прохідній при піднесенні вхідною людиною ідентифікатора до зчитувача, службовець (вахтер, охоронець) може на екрані монітора бачити фотографію людини, якій у базі даних присвоєно даний ідентифікатор, і порівняти із зовнішністю проходить, що під передачі карток іншим;

– якщо необхідно організувати облік робочого дня та контроль трудової дисципліни;

– якщо необхідно забезпечити взаємодію (інтеграцію) з іншими підсистемами безпеки, наприклад, відеоспостереженням або пожежною сигналізацією).

У мережній системі з одного місця можна не тільки контролювати події на всій території, що охороняється, але і централізовано управляти правами користувачів, вести базу даних. Мережеві системи дозволяють організувати кілька робочих місць, розділивши функції управління між різними співробітниками та службами підприємства.

У мережевих системах контролю доступу можуть застосовуватися бездротові технології, звані радіоканали. Використання бездротових мереж часто визначається конкретними ситуаціями: складно чи неможливо прокласти провідні комунікації між об'єктами, скорочення фінансових витрат на монтаж точки проходу тощо. Існує велика кількість варіантів радіоканалів, однак у СКУД використовуються лише деякі з них.

– Bluetooth. Даний вид бездротового пристрою передачі даних є аналогом Ethernet. Його особливість полягає в тому, що відпадає необхідність прокладати паралельні комунікації для об'єднання компонентів під час використання інтерфейсу RS-485.

– Wi-Fi. Основна перевага даного радіоканалу полягає у великій дальності зв'язку, здатного досягати кількох сотень метрів. Це особливо необхідно для з'єднання між собою об'єктів на великих відстанях (?). При цьому скорочуються як тимчасові, і фінансові витрати на прокладання вуличних комунікацій.

– ZigBee. Спочатку сферою застосування даного радіоканалу була система охоронної та пожежної сигналізації. Технології не стоять на місці та активно розвиваються, тому ZigBee може використовуватись і в системах контролю доступу. Ця бездротова технологія працює в діапазоні 2,45 ГГц, що не ліцензується.

– GSM. Перевага використання бездротового каналу зв'язку – практично суцільне покриття. До основних методів передачі інформації в мережі, що розглядається, відносяться GPRS, SMS і голосовий канал.

Непоодинокі ситуації, коли встановлення повноцінної системи безпеки може виявитися невиправдано дорогою для вирішення поставленого завдання. У таких ситуаціях оптимальним рішенням буде встановлення автономного контролера на кожну точку проходу, які необхідно обладнати доступом.

Автономні системи

Автономні системи дешевші, простіше в експлуатації, не вимагають прокладання сотень метрів кабелю, використання пристроїв сполучення з комп'ютером, самого комп'ютера. При цьому до мінусів таких систем відноситься неможливість створювати звіти, вести облік робочого часу, передавати та узагальнювати інформацію про події, керуватися дистанційно. При виборі автономної системи з високими вимогами безпеки рекомендується звернути увагу на наступне:

– Зчитувач повинен бути відокремлений від контролера, щоб дроти, якими можливе відкривання замка, були недоступні зовні.

– Контролер повинен мати резервне джерело живлення у разі відключення електроживлення.

– Переважно використовувати зчитувач у вандалозахищеному корпусі.

У складі автономної системи контролю доступу використовуються також електронні замки, що передають інформацію бездротовими каналами зв'язку: у двері встановлюється механічний замок з електронним управлінням і вбудованим зчитувачем. Замок по радіоканалу пов'язаний з хабом, який вже по дротах обмінюється інформацією з робочою станцією, де встановлено програмне забезпечення.

Для автономної системи можна використовувати «зворотний метод», коли на контрольних точках встановлюються ідентифікатори, а співробітники відзначаються зчитувачем-контролером, згодом дані передаються при першій нагоді – поява зв'язку у зчитувача. Цей метод зручно використовувати, наприклад, у місцях, де відсутня зв'язок, можливість прокладання електроживлення або інших комунікацій. Також «зворотний метод» може використовуватися для контролю патрулювання великих периметрів: після обходу території або після закінчення зміни охоронець здає на перевірку контролер, в якому записані всі контрольні точки, що пройшли, із зазначенням послідовності проходу і часу проходу кожної точки.

Додаткові можливості

– GSM модуль, який дозволяє надсилати SMS з інформацією про прохід (використовується, наприклад, у школах).

– для мережевий СКУД (також деякі автономні системи) – можливість віддаленого управління мережею Інтернет (наприклад, управління системою контролю доступу з центрального офісу, якщо підприємство має безліч філій).

– комплекс для персоналізації пластикових карток (принтер для друку на пластиковій картці даних власника, у тому числі фотографії).

– режим «антипасбек» – якщо людина вже пройшла на територію, що охороняється, то повторне пред'явлення її ідентифікатора на вхід буде заборонено (поки карта не буде пред'явлена на вихід), що виключить можливість проходу по одній карті двох і більше осіб. При цьому мережний СКУД дозволяє організувати такий режим на всіх точках проходу, об'єднаних у мережу, що забезпечує повнофункціональний захист по всьому периметру контрольованої території.

Застосування СКУД

Сфери застосування СКУД різноманітні:

– офіси компаній; бізнес-центри;
– банки;
– заклади освіти (школи, технікуми, виші);
– промислове підприємство;
– охоронювані території;
– автостоянки, паркування;
– місця проїзду автотранспорту;
– приватні будинки, житлові комплекси, котеджі;
– готелі;
– громадські установи (спорткомплекси, музеї, метрополітен та ін.).

Основні типи компаній на ринку

– Виробники.
– Дистриб'ютори.
– Проектувальники.
– Інтегратори.
– Торгові будинки.
– Монтажні організації.
– Кінцеві замовники.
– Великі кінцеві замовники (мають власну службу безпеки).

Системи відеоспостереження

Відеоспостереження – процес, який здійснюється із застосуванням оптико-електронних пристроїв, призначених для візуального контролю або автоматичного аналізу зображень (автоматичне розпізнавання осіб, державних номерів). У англомовному середовищі використовується термін англ. *Closed Circuit Television, CCTV* – система телебачення замкнутого контуру.

Технічні засоби

Відеокамери

На даний момент найбільшого застосування отримали відеокамери на основі ПЗЗ-матриць. У більшості випадків використовуються короткофокусні об'єктиви типу фікс-фокус, що не потребують фокусування, та автоматичне керування експозицією. Основні виробники матриць – Sony, Sharp, Panasonic, Samsung, LG, Hynix. Їх використання дозволило створити помірні за ціною та досить високоякісні вироби широкого застосування. Зазвичай різниця між камерами, заснованими на матрицях різних виробників, проявляється у складних умовах освітлення. У лінійці кожного виробника присутні як дешеві та стандартні за параметрами матриці, так і матриці підвищеної роздільної здатності та/або підвищеної чутливості.

За конструктивними особливостями камери можна поділити на такі типи:

– **Модульна відеокамера** – безкорпусний пристрій у вигляді одношарової друкованої плати, найбільш поширений розмір 32×32 мм, призначений для установки в термокожухи, напівсфери тощо.

– **Мінівідеокамера** – відеокамери в квадратних або циліндричних корпусах, які зазвичай застосовуються як готовий виріб для установки всередині приміщень.

– **Корпусна відеокамера** – найпоширеніший форм-фактор пристроїв, який також називають **камерою стандартного дизайну** або **Box camera**. Переважна кількість пристроїв даного типу поставляється без об'єктиву і кронштейна кріплення, залишаючи споживачеві можливість найбільш гнучкого конфігурування кінцевого пристрою, при використанні термокожухом можливе використання пристрою поза приміщенням.

– **Купольна відеокамера**, також відома як **Dome camera** – корпус є напівсферою або кулею, прикріпленою до основи. Може бути виконана як із пластику, так і з металу.

– **Керовані (поворотні або швидкісні відеокамери)** – комбінований пристрій, що складається з камери, трансфокатора та поворотного пристрою. Найбільшого поширення набули звані інтегровані камери, виконані як купола.

– **Гіростабілізовані відеокамери** – відеокамери, які використовуються на рухомих об'єктах для отримання стабілізованого зображення.

За типом вихідного сигналу відеокамери поділяють на **аналогові** та **цифрові**. Більшість цифрових камер передають сигнал стандартної комп'ютерної мережі типу Ethernet – так звані IP-камери.

За способом передачі даних відеокамери поділяються на **дротові** та **бездротові**. Останні мають у своєму складі передавальний пристрій та антену. Бездротовими в тому числі є цифрові IP-камери, що передають зображення мережним кабелем або радіоканалу мережі Wi-Fi – так звані Wi-Fi-відеокамери.

Об'єктиви

Об'єктив – це пристрій, призначений для фокусування світлового потоку на матриці відеокамери.

Об'єктиви поділяються на:

- **монофокальні** – об'єктиви з постійною фокусною відстанню;
- **варіофокальні** (трансфокатори) – об'єктиви зі змінною фокусною відстанню, що змінюється вручну або дистанційно.

За способом керування діафрагмою об'єктиви діляться на об'єктиви з фіксованою діафрагмою, з керуванням діафрагмою Direct Drive та з керуванням діафрагмою Video Drive.

Корпуси

Для різних умов експлуатації модульні відеокамери поміщаються в корпуси різних типів, наприклад, купольний корпус (традиційний для камер, що встановлюються всередині приміщень), термокожух (корпус, захищений від впливу опадів та низьких температур; призначений для камер, що встановлюються на вулиці), антивандальний корпус (для вуличної та внутрішньої установки) та ін.

Засоби виведення зображення

Послідовний відеокомутатор (Switcher) – пристрій для послідовного виведення зображення камер на 1 монітор. (Застаріли з появою цифрових пристроїв запису.)

Квадратор – пристрій для одночасного відтворення зображення від камер (зазвичай 4 або 8) на 1 монітор. (Застаріли з появою цифрових пристроїв запису.)

Мультиплексор – пристрій для одночасного виведення зображення від камер (зазвичай 4/8 або 16) на 1 монітор та формування послідовності зображення від усіх камер для запису аналоговий магнітофон. (Застаріли з появою цифрових пристроїв запису.)

Матричний відеокомутатор (Matrix switcher) – пристрій для одночасного виведення зображення від будь-якої камери в системі на будь-який монітор в системі. Набагато складніший і ефективніший пристрій, ніж звичайний відеокомутатор.

Пристрої запису зображення

Цифрові реєстратори – сучасні пристрої запису на жорсткий диск (HDD). Поділяються на *відеосервери* (засновані або на звичайному ПК під керуванням Windows або Linux (зі спеціалізованою платою відеозахоплення у разі застосування аналогових камер) та програмним забезпеченням запису та обробки відео, або на спеціально зібраному спеціалізованому комп'ютері, що є ядром великої системи безпеки) та автономні *відеореєстратори* (DVR, non-PC чи Stand-alone).

Інші спеціалізовані реєстратори – різні типи пристроїв застосовуються для вирішення окремих завдань відеоспостереження. Наприклад, для запису та зберігання інформації від камер системи відеоспостереження, встановлених у вагонах метрополітену, крім інших пристроїв застосовується вибухозахищена пам'ять типу флеш.

Також багато IP-камер мають слот для карт пам'яті, на яку вони можуть робити запис. Це робить камеру самодостатнім засобом відеофіксації, а також використовується для резервування запису – наприклад, у разі виходу з ладу основного пристрою запису зображення.

Відео- та аудіодомофони

Пристрої для організації контролю доступу до приміщень з функцією відеофіксації та/або аудіофіксації.

Допоміжні пристрої

– Тепловізори – пристрій для спостереження за розподілом температури досліджуваної поверхні, наприклад, для виявлення людини в темний час доби з її теплового випромінювання.

– Автоматичні фотокамери – використовуються для розширення можливостей систем відеоспостереження.

– Мікрофони – використовуються для синхронного отримання відео та звуку. У ряді випадків використовується різна кількість відеокамер та мікрофонів – асинхронні системи відеоспостереження та аудіоконтролю.

Додаткове обладнання

Для організації відеоспостереження використовують широкий спектр додаткового обладнання: ІЧ-прожектори, модулятори, підсилювачі тощо.

Система відеоспостереження

Система відеоспостереження – це програмно-апаратний комплекс (відеокамери, об'єктиви, монітори, реєстратори та ін. обладнання), призначений для організації відеоконтролю як на локальних, так і на територіально-розподілених об'єктах. До функцій відеоспостереження належить не тільки захист від злочинців, а й спостереження за працівниками, відвідувачами в офісі, на складі або магазині, контроль діяльності в будь-якому приміщенні.

Таким чином, система відеоспостереження забезпечує:

– візуальний контроль ситуації на об'єкті, що охороняється – надання інформації на пост спостереження в режимі реального часу;

– запис відеоінформації на цифровий відеореєстратор, що дозволяє документувати події, що відбуваються на об'єкті;

– виконання функцій охоронної сигналізації через детектори руху відеокамер або зовнішніх охоронних датчиків та поінформованість оператора системи про виникнення тривоги у контрольованій зоні.

Камери відеоспостереження можуть бути різних форм та типів.

Охоронне телебачення

Відеоспостереження на транспорті

- **Відеоспостереження в автобусах та маршрутних таксі**

Основні завдання:

– фіксування злочинів у салонах;

– контроль дій та робочого часу водія.

Рішення реалізується з допомогою організації відеозапису кожному транспортному засобі. Після прибуття транспортного засобу до парку інформація з локальних пристроїв відеозапису передається на архівні відеосервери парку.

- **Відеоспостереження в електропоїздах**

Основні завдання:

– фіксування злочинів у вагонах;

– контроль дій машиніста

Рішення реалізується за допомогою організації відеозапису у кожному вагоні. У деяких випадках відеотрансляція з камер в режимі реального часу здійснюється кабіну машиніста. Після прибуття електропоїзда до депо інформація з локальних пристроїв відеозапису передається на архівні відеосервери залізничного депо.

- **Відеоспостереження у вагонах метрополітену** (може бути аналогічним до відеоспостереження в електропоїздах)

Основні завдання:

– фіксування злочинів у вагонах;

– контроль дій машиніста;

– можливість оперативної реакцію події як реального часу.

Рішення реалізується за допомогою організації відеозапису у кожному вагоні. Після прибуття електропоїзда метро в депо, інформація з локальних пристроїв відеозапису передається на архівні відеосервери метрополітену. Вирішення окремого завдання передачі даних з вагонів, що рухаються в режимі реального часу, дало можливість оператору Ситуаційного центру в будь-який момент підключитися до будь-якої з камер, які встановлені у вагонах.

- **Відеоспостереження на промисловому залізничному транспорті**

Системами відеоспостереження оснащуються також вантажні та магістральні тепловози та електровози, що знаходяться у власності промислових підприємств (наприклад, видобувна промисловість), що забезпечує:

– підвищення безпеки руху (при знаходженні працівників, сторонніх людей та предметів на залізничних коліях, для безпечного перетину залізничних переїздів тощо);

– контроль збереження вантажу та несанкціонованих зливів палива;

– оцінку роботи локомотивних бригад (дотримання регламентів, грамотність дій);

– доказову базу під час розслідування аварійних ситуацій.

Рішення реалізується за допомогою установки:

– камер зовні та всередині локомотива;

– відеореєстратора у вібростійкому та антивандальному виконанні;

– мікрофона для запису переговорів локомотивної бригади;

– монітора для відображення відео з камер у кабіні машиніста.

– **Відеоспостереження в особистому автомобілі**

З 2007 року почалося широке зростання використання автомобільних відеореєстраторів у власних автомобілях. Цифровий автомобільний відеореєстратор разом із відеокамерою здійснює безперервний запис дорожньої ситуації. Запис відеореєстратора приймається як доказ у суді і допомагає довести невинність або знайти винуватця ДТП, що сховався.

Розважальні та торговельні об'єкти

Основне завдання відеоспостереження у казино – забезпечення збереження майна компанії. До обов'язків оператора входить також відстеження несумлінного персоналу, шахраїв, моніторинг випадків крадіжки. В ідеалі оператор знає всі правила казино, основні стратегії та системи рахунку, стежить за зовнішнім виглядом та діями персоналу, поведінкою гравців, спираючись на мову тіла.

На великих торгових об'єктах відеоспостереження використовується з такими цілями:

– протидія розкраданням із боку відвідувачів. Шляхом взаємодії оператора CCTV з магазинними детективами (співробітниками служби безпеки, що перебувають у торговому залі під виглядом покупців) та групою фізичної охорони (співробітниками охоронних компаній) здійснюється негласний постійний візуальний супровід підозрілих осіб по магазину.

– контроль за персоналом магазину Без системи контролю доступу за магнітними ключами відеоспостереження допомагає контролювати трудову дисципліну (час приходів і доглядів співробітників). Також розміщені у складських та службових приміщеннях відеокамери допомагають у роботі служби безпеки при аналізі бізнес-втрат, що виникають у логістичному відділі:

- розслідування проведення безтоварних документів (коли товару фактично не привезли, а відповідальна особа його фіктивно прийняла)
- розслідування фактів пересортиці товару, що приймається і відвантажується
- розслідування фактів псування товару при переміщенні по складах (невмілість чи недбалість персоналу)

– забезпечення спільної безпеки. Оскільки оператор відеоспостереження при грамотно підібраному розміщенні і типі камер контролює практично весь зал, він може по радіостанції скоординувати прибуття співробітників охорони на

місце виникнення пожежі, скоєння протиправних дій, для надання першої допомоги відвідувачу, який погано почував себе. Перегляд архівів допомагає розслідувати нещасні випадки з персоналом (склади, як правило, механізовані підйомно-навантажувальною технікою, травми та подібні НП там не рідкість)

– оскільки великі торгові комплекси є місцем скоєння злочинів не тільки щодо самого підприємства, а й відвідувачів, наявність мережі відеоспостереження з архівуванням даних допомагає розслідувати і в ряді випадків запобігати викраданням автомашин з парковок, діяльності злодіїв-кишенькових злодіїв і борсетників. Найчастіше правоохоронці звертаються до РБ магазинів з проханням надати архівні відео, коли подібні злочини відбуваються в полі огляду CCTV.

Офіси

На даний момент системи відеоспостереження в Україні встановлені в половині офісів країни. Фіксація подій в офісі служить для забезпечення безпеки співробітників, запобігання дрібному крадіжці, виявлення несумлінних працівників, а також обмеження можливості «відпливу» службової інформації.

Законність відеоспостереження

Законність відеоспостереження визначається та регулюється відповідними законами та підзаконними актами країни, на території якої встановлюватиметься неприховане та приховане відеоспостереження. Майже завжди діє наступний принцип: законність відеоспостереження залежить від того, чи не порушує воно права людини і чи є у вас дозвіл на здійснення цієї діяльності від людей, яких вона безпосередньо торкнеться. Туалетні кімнати та зони відпочинку входять до місць, де установка відеоспостереження неприпустима. Місця, де встановлені камери, повинні бути обладнані спеціальними попереджувальними знаками, наприклад, «Ведеться відеоспостереження». Відповідні зміни також мають знайти відображення і у трудовому договорі співробітника, де мають бути прописані такі пункти:

– переглядати відеоархів має право обмежене коло осіб, переважно керівник та співробітники служби безпеки;

– вищезазначені працівники повинні бути повідомлені про відповідальність за розголошення та використання персональних даних працівників;

– записи з камер відеоспостереження не можна використовуватиме стимулювання поведінки співробітників, і навіть у виховних цілях.

Домашній сектор

Типова система відеоспостереження, призначена для домашнього користування, включає відеокамеру, що підключається кабельним або бездротовим каналом до домашньої локальної мережі. У комплект також входить програмне забезпечення для віддаленого спостереження, відеозапису, а також для керування записаним контентом. Мережа будується на базі однієї або кількох IP-камер. Передача відео через мережу вимагає суттєвої ширини каналу передачі, тому в системах відеоспостереження використовується кодування інформації з метою стиснення. Раніше для побудови мережі застосовувалися

спеціалізовані пристрої для кодування даних. В даний час кодери вбудовуються безпосередньо в IP-камери.

Висотне телебачення

Відеоспостереження за місцями масового скупчення людей, місцями проведення культурних та спортивних заходів, спеціальними операціями та наземними об'єктами – це завдання замкнутих систем висотного телебачення. Часто інформація, отримана з відеокамер, є ключовою для оперативного реагування у позаштатних ситуаціях. Висотне телебачення використовується також для рятувальних та пошукових операцій.

Характеристики та одиниці виміру, що використовуються в системах відеоспостереження

Чутливість відеокамери характеризується мінімальним отвором діафрагми (максимальним F-числом), що дає відеосигнал розмаху 1 В на тестовій таблиці, освітленість якої 2000 лк, з колірною температурою 3200° К. Чутливість відеокамери, чітко визначена в її зазвичай плутають із мінімальною освітленістю.

Мінімальна освітленість (у характеристиках відеокамер цей параметр часто вказують як чутливість) – це найменша освітленість на об'єкті, при якій відеокамера дає сигнал, що розпізнається, виражається в **люксах** на об'єкті. Ряд виробників використовує термін розпізнаваний сигнал у сенсі і вказують рівень сигналу на виході відеокамери. Цей рівень може становити навіть 10%, що при включеному автоматичному регулюванні посилення (АРП) здаватиметься значно більше.

Таблиця 21.1 – Мінімальна освітленість

Типові рівні освітленості	Безхмарна ніч	Ясна безмісячна ніч	Повний місяць	Вуличне освітлення	Офісне освітлення	Ясний день
Рівень освітленості, лк	0,0001	0,001	0,01-0,1	1-10	100-1000	до 100 000

Динамічний діапазон ПЗЗ-матриці відеокамери визначається як максимальний сигнал по відношенню до середньоквадратичного значення фону експозиції, тобто відношення темних та яскравих об'єктів у межах однієї сцени. Чим вище це ставлення, тим більше темні елементи помітні на яскравому тлі кадру.

Роздільна здатність відеокамери – це максимальна кількість ліній, що містяться в одному кадрі монітора (**ТВЛ** – телевізійні лінії, від англ. Television Lines, TVL). Зазвичай вказується роздільна здатність по горизонталі, роздільна здатність по вертикалі становить 3/4 від горизонтальної.

Роздільна здатність пристроїв обробки та відображення відеоінформації вимірюється, як правило, у **пікселях**. Це здатність приладу окремо спостерігати, фіксувати та (або) відображати поруч розташовані точки графічного образу об'єкта. Вимірюється числом точок, що окремо відображаються, що припадають

на дюйм поверхні кадру. Перше число – кількість точок по горизонталі, друге – по вертикалі. Іноді її вимірюють у CIF.

Відношення сигнал/шум – це перевищення рівня сигналу над рівнем шуму при мінімальному освітленні, вимірюється в дБ та залежить від якості ПЗЗ матриці відеокамери. На екрані зашумлене зображення виглядає як зернистість чи сніг, а кольоровому зображенні з'являються короткі кольорові смужки чи спалахи. Формула за напругою має вигляд $S/N=20lg\ (U_c/U_ш)$ *Формула* за потужністю сигналу має вигляд $S / N= 10lg\ (P_c / P_ш)$

Швидкість запису (відтворення або відтворення) – **Кадрова частота** – кількість кадрів, яку відеосистема записує (відтворює або передає) за одну секунду. Вимірюється в *кадрах на секунду* (англ. *frames per second,* ***fps***). Іноді виробниками використовується ***pps*** – кількість напівполів, що відображаються відеосистемою за секунду. 1 fps = 2 pps.

Режими запису

- Безперервний запис – це постійний цілодобовий запис відео.
- Запис за розкладом – запис у певний час доби.
- Запис за тривогою – запис починається при надходженні певного сигналу.
- Запис за детектором руху – запис здійснюється лише під час зміни зображення.
- Екстрений запис або запис у ручному режимі – запис починається за командою оператора (при натисканні кнопки).

Двопоточність – властивість IP-відеокамер та пристроїв кодування відео надавати два відеопотоку різної якості для кожного каналу відео. Потік високої роздільної здатності використовується для збереження в архів і відображення в повноекранному режимі. Потік низької роздільної здатності використовується для відображення в режимі мультиекрану. Загалом можливе надання більше двох потоків.

Інтегровані системи безпеки

В даний час системи відеоспостереження стали надавати не лише стандартні можливості відтворення та запис відеопотоку з камери. Вони дозволяють в автоматичному режимі вирішувати безліч завдань без участі людини, починаючи від простого детектування руху в області спостереження, закінчуючи високоточним підрахунком машин, що проїхали або минулих людей (система підрахунку відвідувачів).

Інтегровані системи безпеки включають комплекс організаційних і технічних заходів щодо захисту об'єктів від будь-якого несанкціонованого проникнення на об'єкт, від несанкціонованого збору конфіденційної інформації, від розкрадань, фактів вандалізму або саботажу. Вони знижують комерційні ризики та ймовірність безперервності бізнесу. Інтегровані системи можуть і повинні бути використані у випадках настання подій інформаційної безпеки – використання у судовому діловодстві, корпоративних розслідуваннях, зміні менеджменту системи інформаційної безпеки компанії.

Взаємопов'язані елементи систем інтегрованої безпеки включають:

– системи відеоспостереження, дистанційні системи відеоспостереження, бездротові, розподілені та централізовані системи відеоспостереження;

– аудіоконтроль, включаючи віддалений аудіоконтроль;

– системи контролю доступу (СКД), системи віддаленого контролю та управління доступу (СКУД), у тому числі інтегровані із системою розпізнавання осіб, системи контролю робочого часу, дозоване отримання інформації про перебування співробітників на об'єкті;

– системи розпізнавання номерів на парковках;

– захист технічними засобами приміщень та об'єктів від несанкціонованого прослуховування, перегляду та збору інформації (захист від прослуховування за допомогою радіозасобів, радіозакладок, радіосканерів, за допомогою ІЧ сканерів, акустичних та віброакустичних засобів прослуховування, контроль телефонних ліній, ліній кабельного телебачення, електромереж та електромереж).;

– обладнання для захисту від прослуховування під час переговорів поза приміщеннями;

– захист від радіопідривників (радіокерованих вибухових пристроїв);

– контроль радіаційної безпеки з метою захисту від радіаційного терору;

– різні системи всеосяжної охоронної сигналізації та пожежної сигналізації (ОПС, ОС, ПС);

– установку шлагбаумів, турнікетів, шлюзових камер тощо;

– комплекс засобів захисту від насильницького вторгнення чи нападу бандитських угруповань.

Інтегровані системи безпеки можуть бути побудовані на різних віддалених об'єктах із загальним центром управління.

Пожежна сигналізація

Пожежна сигналізація – сукупність технічних засобів для виявлення загоряння, повідомлення про місце виникнення та обробки сигналу, також процес отримання, обробки, передачі та подання інформації про пожежу в заданому вигляді за допомогою даних технічних засобів.

Пожежна сигналізація є різновидом вимірювальних інформаційних систем, включає вимірювальні пристрої та засоби обробки інформації. На відміну більшості вимірювальних систем, установки пожежної сигналізації визначають не кількісне значення контрольованого параметра, лише його відхилення убік більш допустимої. Обробка результатів зводиться в основному для отримання даних про місце виникнення пожежонебезпечної ситуації. Вимоги до швидкодії систем є вкрай жорсткими поряд із майже повною відсутністю вимог до накопичення інформації.

Технічні засоби пожежної сигналізації

У пожежній сигналізації використовуються кабелі для сигналізації та блокування.

Склад:

– Сповіщувачі пожежні автоматичні (димові, теплові, полум'я, газові або комбіновані).

– Сповіщувачі пожежні ручні.

– Прилад приймально-контрольний (ППК).

– Релейний блок – за потребою.

– Джерело безперебійного електроживлення.

– Допоміжні елементи пожежних шлейфів.

– Допоміжні пристрої каналу передачі повідомлень (повторювачі, перетворювачі та ін.).

Пожежна та охоронна сигналізації на об'єкті можуть бути об'єднані в охоронно-пожежну систему (ОПС) з використанням загального ППК, каналу зв'язку та деяких інших елементів.

Додаток А. Тексти Законів та стандартів України щодо забезпечення кібербезпеки

А.1. Закон України «Про інформацію».

А.2. Закон України «Про науково-технічну інформацію».

А.3. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».

А.4. Закон України «Про основні засади забезпечення кібербезпеки України».

А.5. Закон України «Про державну таємницю».

А.6. Закон України «Про захист персональних даних».

А.7. Постанова КМУ від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури.

А.8. ДСТУ 3396.0,1,2-97.

А.9. ДСТУ ISO/IEC 15408-1:2017.

А.10. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу».

А.11. НД ТЗІ 2.5-004-99. «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу».

А.12. Закон України «Про доступ до публічної інформації».

А.1. Закон України «Про інформацію»

Цей Закон регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації, та складається з наступних розділів і статей.

Розділ I. ЗАГАЛЬНІ ПОЛОЖЕННЯ
Стаття 1. Визначення термінів
Стаття 2. Основні принципи інформаційних відносин
Стаття 3. Державна інформаційна політика
Стаття 4. Суб'єкти і об'єкт інформаційних відносин
Стаття 5. Право на інформацію
Стаття 6. Гарантії права на інформацію
Стаття 7. Охорона права на інформацію
Стаття 8. Мова інформації
Стаття 9. Основні види інформаційної діяльності
Розділ II. ВИДИ ІНФОРМАЦІЇ
Стаття 10. Види інформації за змістом
Стаття 11. Інформація про фізичну особу
Стаття 12. Інформація довідково-енциклопедичного характеру
Стаття 13. Інформація про стан довкілля (екологічна інформація)
Стаття 14. Інформація про товар (роботу, послугу)
Стаття 15. Науково-технічна інформація
Стаття 16. Податкова інформація
Стаття 17. Правова інформація
Стаття 18. Статистична інформація
Стаття 19. Соціологічна інформація
Стаття 19. Критична технологічна інформація
Стаття 20. Доступ до інформації
Стаття 21. Інформація з обмеженим доступом
Розділ III. ДІЯЛЬНІСТЬ ЖУРНАЛІСТІВ, ЗАСОБІВ МАСОВОЇ ІНФОРМАЦІЇ, ЇХ ПРАЦІВНИКІВ
Стаття 22. Масова інформація та її засоби
Стаття 23. Інформаційна продукція та інформаційна послуга
Стаття 24. Заборона цензури та заборона втручання в професійну діяльність журналістів і засобів масової інформації
Стаття 25. Гарантії діяльності засобів масової інформації та журналістів
Стаття 26. Акредитація журналістів, працівників засобів масової інформації
Розділ IV. ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА ПРО ІНФОРМАЦІЮ
Стаття 27. Відповідальність за порушення законодавства про інформацію
Стаття 28. Неприпустимість зловживання правом на інформацію
Стаття 29. Поширення суспільно необхідної інформації
Стаття 30. Звільнення від відповідальності
Стаття 31. Відшкодування матеріальної та моральної шкоди

Розділ І. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення термінів

1. У цьому Законі наведені нижче терміни вживаються в такому значенні:

– документ – матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі;

– захист інформації – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї;

– інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;

– суб'єкт владних повноважень – орган державної влади, орган місцевого самоврядування, інший суб'єкт, що здійснює владні управлінські функції відповідно до законодавства, у тому числі на виконання делегованих повноважень.

Стаття 2. Основні принципи інформаційних відносин

1. Основними принципами інформаційних відносин є:

– гарантованість права на інформацію;

– відкритість, доступність інформації, свобода обміну інформацією;

– достовірність і повнота інформації;

– свобода вираження поглядів і переконань;

– правомірність одержання, використання, поширення, зберігання та захисту інформації;

– захищеність особи від втручання в її особисте та сімейне життя.

Стаття 3. Державна інформаційна політика

1. Основними напрямами державної інформаційної політики є:

– забезпечення доступу кожного до інформації;

– забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації;

– створення умов для формування в Україні інформаційного суспільства;

– забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень;

– створення інформаційних систем і мереж інформації, розвиток електронного урядування;

– постійне оновлення, збагачення та зберігання національних інформаційних ресурсів;

– забезпечення інформаційної безпеки України;

– сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору.

Стаття 4. Суб'єкти і об'єкт інформаційних відносин

1. Суб'єктами інформаційних відносин є:

– фізичні особи;

– юридичні особи;

– об'єднання громадян;

– суб'єкти владних повноважень.

2. Об'єктом інформаційних відносин є інформація.

Стаття 5. Право на інформацію

1. Кожен має право на інформацію, що передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів.

Реалізація права на інформацію не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб.

Стаття 6. Гарантії права на інформацію

1. Право на інформацію забезпечується:

– створенням механізму реалізації права на інформацію;

– створенням можливостей для вільного доступу до статистичних даних, архівних, бібліотечних і музейних фондів, інших інформаційних банків, баз даних, інформаційних ресурсів;

– обов'язком суб'єктів владних повноважень інформувати громадськість та засоби масової інформації про свою діяльність і прийняті рішення;

– обов'язком суб'єктів владних повноважень визначити спеціальні підрозділи або відповідальних осіб для забезпечення доступу запитувачів до інформації;

– здійсненням державного і громадського контролю за додержанням законодавства про інформацію;

– встановленням відповідальності за порушення законодавства про інформацію.

2. Право на інформацію може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку, з метою запобігання заворушенням чи кримінальним правопорушенням, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.

Стаття 7. Охорона права на інформацію

1. Право на інформацію охороняється законом. Держава гарантує всім суб'єктам інформаційних відносин рівні права і можливості доступу до інформації.

2. Ніхто не може обмежувати права особи у виборі форм і джерел одержання інформації, за винятком випадків, передбачених законом.

Суб'єкт інформаційних відносин може вимагати усунення будь-яких порушень його права на інформацію.

3. Забороняється вилучення і знищення друкованих видань, експонатів, інформаційних банків, документів з архівних, бібліотечних, музейних фондів, крім встановлених законом випадків або на підставі рішення суду.

4. Право на інформацію, створену в процесі діяльності фізичної чи юридичної особи, суб'єкта владних повноважень або за рахунок фізичної чи юридичної особи, Державного бюджету України, місцевого бюджету, охороняється в порядку, визначеному законом.

Стаття 8. Мова інформації

1. Мову інформації визначають Закон України "Про забезпечення функціонування української мови як державної", інші закони України та міжнародні договори, згода на обов'язковість яких надана Верховною Радою України.

Стаття 9. Основні види інформаційної діяльності

1. Основними видами інформаційної діяльності є створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації.

Розділ ІІ. ВИДИ ІНФОРМАЦІЇ

Стаття 10. Види інформації за змістом

За змістом інформація поділяється на такі види:

– інформація про фізичну особу;

– інформація довідково-енциклопедичного характеру;

– інформація про стан довкілля (екологічна інформація);

– інформація про товар (роботу, послугу);

– науково-технічна інформація;

– податкова інформація;

– правова інформація;

– статистична інформація;

– соціологічна інформація;

– критична технологічна інформація;

– інші види інформації.

Стаття 11. Інформація про фізичну особу

1. Інформація про фізичну особу (персональні дані) – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

2. Не допускаються збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини. До конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження.

Кожному забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законом.

Центральний орган виконавчої влади, що забезпечує формування та реалізує державну фінансову та бюджетну політику, під час здійснення повноважень щодо верифікації та моніторингу державних виплат не потребує згоди фізичних осіб на отримання та обробку персональних даних.

Стаття 12. Інформація довідково-енциклопедичного характеру

1. Інформація довідково-енциклопедичного характеру – систематизовані, документовані, публічно оголошені або іншим чином поширені відомості про суспільне, державне життя та навколишнє природне середовище.

2. Основними джерелами інформації довідково-енциклопедичного характеру є: енциклопедії, словники, довідники, рекламні повідомлення та оголошення, путівники, картографічні матеріали, електронні бази та банки

даних, архіви різноманітних довідкових інформаційних служб, мереж та систем, а також довідки, що видаються уповноваженими на те органами державної влади та органами місцевого самоврядування, об'єднаннями громадян, організаціями, їх працівниками та автоматизованими інформаційно-комунікаційними системами.

3. Правовий режим інформації довідково-енциклопедичного характеру визначається законодавством та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

Стаття 13. Інформація про стан довкілля (екологічна інформація)

1. Інформація про стан довкілля (екологічна інформація) – відомості та/або дані про:

– стан складових довкілля та його компоненти, включаючи генетично модифіковані організми, та взаємодію між цими складовими;

– фактори, що впливають або можуть впливати на складові довкілля (речовини, енергія, шум і випромінювання, а також діяльність або заходи, включаючи адміністративні, угоди в галузі навколишнього природного середовища, політику, законодавство, плани і програми);

– стан здоров'я та безпеки людей, умови життя людей, стан об'єктів культури і споруд тією мірою, якою на них впливає або може вплинути стан складових довкілля;

– інші відомості та/або дані.

2. Правовий режим інформації про стан довкілля (екологічної інформації) визначається законами України та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

3. Інформація про стан довкілля, крім інформації про місце розташування військових об'єктів, не може бути віднесена до інформації з обмеженим доступом.

Стаття 14. Інформація про товар (роботу, послугу)

1. Інформація про товар (роботу, послугу) – відомості та/або дані, які розкривають кількісні, якісні та інші характеристики товару (роботи, послуги).

2. Інформація про вплив товару (роботи, послуги) на життя та здоров'я людини не може бути віднесена до інформації з обмеженим доступом.

3. Правовий режим інформації про товар (роботу, послугу) визначається законами України про захист прав споживачів, про рекламу, іншими законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

Стаття 15. Науково-технічна інформація

1. Науково-технічна інформація – будь-які відомості та/або дані про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, одержані в ході науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

2. Правовий режим науково-технічної інформації визначається Законом України "Про науково-технічну інформацію", іншими законами та

міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

3. Науково-технічна інформація є відкритою за режимом доступу, якщо інше не встановлено законами України.

Стаття 16. Податкова інформація

1. Податкова інформація – сукупність відомостей і даних, що створені або отримані суб'єктами інформаційних відносин у процесі поточної діяльності і необхідні для реалізації покладених на контролюючі органи завдань і функцій у порядку, встановленому Податковим кодексом України.

2. Правовий режим податкової інформації визначається Податковим кодексом України та іншими законами.

Стаття 17. Правова інформація

1. Правова інформація – будь-які відомості про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо.

2. Джерелами правової інформації є Конституція України, інші законодавчі і підзаконні нормативно-правові акти, міжнародні договори та угоди, норми і принципи міжнародного права, а також ненормативні правові акти, повідомлення засобів масової інформації, публічні виступи, інші джерела інформації з правових питань.

3. З метою забезпечення доступу до законодавчих та інших нормативних актів фізичним та юридичним особам держава забезпечує офіційне видання цих актів масовими тиражами у найкоротші строки після їх прийняття.

Стаття 18. Статистична інформація

1. Статистична інформація – документована інформація, що дає кількісну характеристику масових явищ та процесів, які відбуваються в економічній, соціальній, культурній та інших сферах життя суспільства.

2. Офіційна державна статистична інформація підлягає систематичному оприлюдненню.

3. Держава гарантує суб'єктам інформаційних відносин відкритий доступ до офіційної державної статистичної інформації, за винятком інформації, доступ до якої обмежений згідно із законом.

4. Правовий режим державної статистичної інформації визначається Законом України "Про державну статистику", іншими законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

Стаття 19. Соціологічна інформація

1. Соціологічна інформація – будь-які документовані відомості про ставлення до окремих осіб, подій, явищ, процесів, фактів тощо.

2. Правовий режим соціологічної інформації визначається законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

Стаття 19. Критична технологічна інформація

1. Критична технологічна інформація – дані, що обробляються (приймаються, передаються, зберігаються) в системах управління технологічними процесами об’єктів критичної інфраструктури.

2. Правовий режим критичної технологічної інформації визначається законами України та міжнародними договорами України, згода на обов’язковість яких надана Верховною Радою України.

3. Критична технологічна інформація за режимом доступу належить до інформації з обмеженим доступом та підлягає захисту згідно із законом.

Стаття 20. Доступ до інформації

1. За порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом.

2. Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом.

Стаття 21. Інформація з обмеженим доступом

1. Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація.

2. Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом.

Відносини, пов'язані з правовим режимом конфіденційної інформації, регулюються законом.

3. Порядок віднесення інформації до таємної або службової, а також порядок доступу до неї регулюються законами.

4. До інформації з обмеженим доступом не можуть бути віднесені такі відомості:

1) про стан довкілля, якість харчових продуктів і предметів побуту;

2) про аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей;

3) про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;

4) про факти порушення прав і свобод людини, включаючи інформацію, що міститься в архівних документах колишніх радянських органів державної безпеки, пов’язаних з політичними репресіями, Голодомором 1932-1933 років в Україні та іншими злочинами, вчиненими представниками комуністичного та/або націонал-соціалістичного (нацистського) тоталітарних режимів;

5) про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб;

5^{-1}) щодо діяльності державних та комунальних унітарних підприємств, господарських товариств, у статутному капіталі яких більше 50 відсотків акцій (часток) належать державі або територіальній громаді, а також

господарських товариств, 50 і більше відсотків акцій (часток) яких належать господарському товариству, частка держави або територіальної громади в якому становить 100 відсотків, що підлягають обов’язковому оприлюдненню відповідно до закону;

6) інші відомості, доступ до яких не може бути обмежено відповідно до законів та міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України.

Розділ ІІІ. ДІЯЛЬНІСТЬ ЖУРНАЛІСТІВ, ЗАСОБІВ МАСОВОЇ ІНФОРМАЦІЇ, ЇХ ПРАЦІВНИКІВ

Стаття 22. Масова інформація та її засоби

1. Масова інформація – інформація, що поширюється з метою її доведення до необмеженого кола осіб.

2. Засоби масової інформації – засоби, призначені для публічного поширення друкованої або аудіовізуальної інформації.

Стаття 23. Інформаційна продукція та інформаційна послуга

1. Інформаційна продукція – матеріалізований результат інформаційної діяльності, призначений для задоволення потреб суб'єктів інформаційних відносин. Інформаційною послугою є діяльність з надання інформаційної продукції споживачам з метою задоволення їхніх потреб.

2. Інформаційна продукція та інформаційні послуги є об'єктами цивільно-правових відносин, що регулюються цивільним законодавством України.

Стаття 24. Заборона цензури та заборона втручання в професійну діяльність журналістів і засобів масової інформації

1. Забороняється цензура – будь-яка вимога, спрямована, зокрема, до журналіста, засобу масової інформації, його засновника (співзасновника), видавця, керівника, розповсюджувача, узгоджувати інформацію до її поширення або накладення заборони чи перешкоджання в будь-якій іншій формі тиражуванню або поширенню інформації.

Ця заборона не поширюється на випадки, коли попереднє узгодження інформації здійснюється на підставі закону, а також у разі накладення судом заборони на поширення інформації.

2. Забороняються втручання у професійну діяльність журналістів, контроль за змістом поширюваної інформації, зокрема з метою поширення чи непоширення певної інформації, замовчування суспільно необхідної інформації, накладення заборони на висвітлення окремих тем, показ окремих осіб або поширення інформації про них, заборони критикувати суб'єкти владних повноважень, крім випадків, встановлених законом, договором між засновником (власником) і трудовим колективом, редакційним статутом.

3. Умисне перешкоджання законній професійній діяльності журналістів та/або переслідування журналіста за виконання професійних обов'язків, за критику тягне за собою відповідальність згідно із законами України.

Стаття 25. Гарантії діяльності засобів масової інформації та журналістів

1. Під час виконання професійних обов'язків журналіст має право здійснювати письмові, аудіота відеозаписи із застосуванням необхідних технічних засобів, за винятком випадків, передбачених законом.

2. Журналіст має право безперешкодно відвідувати приміщення суб'єктів владних повноважень, відкриті заходи, які ними проводяться, та бути особисто прийнятим у розумні строки їх посадовими і службовими особами, крім випадків, визначених законодавством.

3. Журналіст має право не розкривати джерело інформації або інформацію, яка дозволяє встановити джерела інформації, крім випадків, коли його зобов'язано до цього рішенням суду на основі закону.

4. Після пред'явлення документа, що засвідчує його професійну належність, працівник засобу масової інформації має право збирати інформацію в районах стихійного лиха, катастроф, у місцях аварій, масових безпорядків, воєнних дій та на територіях, де оголошено надзвичайний стан, надзвичайну ситуацію або вжиті адміністративні та медико-санітарні заходи (карантин), крім випадків, передбачених законом.

5. Журналіст має право поширювати підготовлені ним матеріали (фонограми, відеозаписи, письмові тексти тощо) за власним підписом (авторством) або під умовним ім'ям (псевдонімом).

6. Журналіст засобу масової інформації має право відмовитися від авторства (підпису) на матеріал, якщо його зміст після редакційної правки (редагування) суперечить його переконанням.

7. Права та обов'язки журналіста, працівника засобу масової інформації, визначені цим Законом, поширюються на зарубіжних журналістів, працівників зарубіжних засобів масової інформації, які працюють в Україні.

Стаття 26. Акредитація журналістів, працівників засобів масової інформації

1. З метою створення сприятливих умов для здійснення журналістами, працівниками засобів масової інформації професійної діяльності суб'єкт владних повноважень може здійснювати їх акредитацію.

Усі дії, пов'язані з акредитацією, мають ґрунтуватися на принципах відкритості, рівності, справедливості з метою забезпечення права громадськості на одержання інформації через засоби масової інформації. Відсутність акредитації не може бути підставою для відмови в допуску журналіста, працівника засобу масової інформації на відкриті заходи, що проводить суб'єкт владних повноважень.

2. Акредитація журналіста, працівника засобу масової інформації здійснюється безоплатно на підставі його заяви або подання засобу масової інформації.

У заяві, поданій журналістом, працівником засобу масової інформації, зазначаються його прізвище, ім'я та по батькові, адреса, номер засобу зв'язку, адреса електронної пошти (за наявності). До заяви додаються копії документів, що посвідчують особу та засвідчують її професійну належність.

У поданні засобу масової інформації зазначаються його повне найменування, дата і номер реєстрації, адреса, адреса електронної пошти (за наявності), номер засобу зв'язку, прізвище, ім'я та по батькові журналіста, працівника засобу масової інформації, щодо якого вноситься подання. До подання додаються копії документів, що посвідчують особу.

В акредитації не може бути відмовлено в разі подання усіх документів, передбачених цією частиною.

Суб'єкт владних повноважень може встановлювати спрощений порядок акредитації.

3. Порядок акредитації, визначений суб'єктом владних повноважень, підлягає оприлюдненню.

4. Суб'єкти владних повноважень, що здійснили акредитацію журналістів, працівників засобів масової інформації, зобов'язані сприяти провадженню ними професійної діяльності; завчасно сповіщати їх про місце і час проведення сесій, засідань, нарад, брифінгів та інших публічних заходів; надавати їм інформацію, призначену для засобів масової інформації; а також сприяти створенню умов для здійснення запису і передачі інформації, проведення інтерв'ю, отримання коментарів посадових осіб.

5. У разі якщо захід проводиться відповідно до міжнародних або інших спеціальних протоколів, можуть встановлюватися особливі умови допуску журналістів. Такі особливі умови оприлюднюються на офіційному веб-сайті відповідного суб'єкта владних повноважень до проведення заходу.

6. Журналіст, працівник засобу масової інформації зобов'язаний дотримуватися встановлених суб'єктом владних повноважень правил внутрішнього трудового розпорядку, не перешкоджати діяльності його службових та посадових осіб.

7. Суб'єкти владних повноважень, що акредитували журналіста, працівника засобу масової інформації, приймають рішення про припинення акредитації у разі:

– подання ним відповідної заяви;

– неодноразового грубого порушення ним обов'язків, визначених цією статтею;

– звернення засобу масової інформації, за поданням якого здійснена акредитація.

8. У рішенні про припинення акредитації зазначаються посадова особа чи службова особа (суб'єкт владних повноважень), яка прийняла відповідне рішення, дата прийняття рішення, підстава для прийняття рішення та порядок його оскарження. Письмове повідомлення про припинення акредитації видається або надсилається засобу масової інформації або журналістові, працівникові засобу масової інформації протягом п'яти робочих днів з дня прийняття відповідного рішення.

9. Рішення про припинення акредитації може бути оскаржено до суду в установленому порядку.

Розділ IV. ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА ПРО ІНФОРМАЦІЮ

Стаття 27. Відповідальність за порушення законодавства про інформацію

1. Порушення законодавства України про інформацію тягне за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність згідно із законами України.

Стаття 28. Неприпустимість зловживання правом на інформацію

1. Інформація не може бути використана для закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання міжетнічної, расової, релігійної ворожнечі, вчинення терористичних актів, посягання на права і свободи людини.

Стаття 29. Поширення суспільно необхідної інформації

1. Інформація з обмеженим доступом може бути поширена, якщо вона є суспільно необхідною, тобто є предметом суспільного інтересу, і право громадськості знати цю інформацію переважає потенційну шкоду від її поширення.

2. Предметом суспільного інтересу вважається інформація, яка свідчить про загрозу державному суверенітету, територіальній цілісності України; забезпечує реалізацію конституційних прав, свобод і обов'язків; свідчить про можливість порушення прав людини, введення громадськості в оману, шкідливі екологічні та інші негативні наслідки діяльності (бездіяльності) фізичних або юридичних осіб тощо.

Стаття 30. Звільнення від відповідальності

1. Ніхто не може бути притягнутий до відповідальності за висловлення оціночних суджень.

2. Оціночними судженнями, за винятком наклепу, є висловлювання, які не містять фактичних даних, критика, оцінка дій, а також висловлювання, що не можуть бути витлумачені як такі, що містять фактичні дані, зокрема з огляду на характер використання мовно-стилістичних засобів (вживання гіпербол, алегорій, сатири). Оціночні судження не підлягають спростуванню та доведенню їх правдивості.

Якщо особа вважає, що оціночні судження або думки принижують її гідність, честь чи ділову репутацію, а також інші особисті немайнові права, вона вправі скористатися наданим їй законодавством правом на відповідь, а також на власне тлумачення справи у тому самому засобі масової інформації з метою обґрунтування безпідставності поширених суджень, надавши їм іншу оцінку. Якщо суб'єктивну думку висловлено в брутальній, принизливій чи непристойній формі, що принижує гідність, честь чи ділову репутацію, на особу, яка таким чином та у такий спосіб висловила думку або оцінку, може бути покладено обов'язок відшкодувати завдану моральну шкоду.

3. Суб'єкти інформаційних відносин звільняються від відповідальності за розголошення інформації з обмеженим доступом, якщо суд встановить, що ця інформація є суспільно необхідною.

4. Додаткові підстави звільнення від відповідальності засобів масової інформації та журналістів встановлюються законами України "Про друковані засоби масової інформації (пресу) в Україні", "Про телебачення і радіомовлення", "Про інформаційні агентства" та іншими.

Стаття 31. Відшкодування матеріальної та моральної шкоди

1. У разі якщо порушенням права на свободу інформації особі завдано матеріальної чи моральної шкоди, вона має право на її відшкодування за рішенням суду.

2. Суб'єкти владних повноважень як позивачі у справах про захист честі, гідності та ділової репутації вправі вимагати в судовому порядку лише спростування недостовірної інформації про себе і не мають права вимагати відшкодування моральної (немайнової) шкоди. Це не позбавляє посадових і службових осіб права на захист честі, гідності та ділової репутації в суді.

А.2. Закон України «Про науково-технічну інформацію»

Цей Закон визначає основи державної політики в галузі науково-технічної інформації, порядок її формування і реалізації в інтересах науково-технічного, економічного і соціального прогресу країни та складається з наступних розділів і статей.

Розділ I. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення термінів

Стаття 2. Об’єкт відносин у сфері науково-технічної інформації

Стаття 3. Суб’єкти відносин у сфері науково-технічної інформації

Стаття 4. Законодавство України у сфері науково-технічної інформації

Розділ II. ПРАВОВИЙ РЕЖИМ НАУКОВО-ТЕХНІЧНОЇ ІНФОРМАЦІЇ

Стаття 5. Право на науково-технічну інформацію

Стаття 6. Права на науково-технічну інформацію

Стаття 7. Відносини між особами, яким належать права на науково-технічну інформацію, її споживачами і посередниками

Розділ III. НАЦІОНАЛЬНА СИСТЕМА НАУКОВО-ТЕХНІЧНОЇ ІНФОРМАЦІЇ

Стаття 8. Визначення та склад національної системи науково-технічної інформації

Стаття 9. Основні завдання національної системи науково-технічної інформації

Стаття 10. Інформаційні ресурси національної системи науково-технічної інформації

Стаття 11. Державна реєстрація, облік і використання результатів науково-технічної діяльності

Стаття 12. Організація надходження та використання зарубіжної науково-технічної інформації

Розділ IV. РИНОК НАУКОВО-ТЕХНІЧНОЇ ІНФОРМАЦІЇ

Стаття 13. Науково-технічна інформація як об’єкт товарних відносин

Стаття 14. Формування ринку науково-технічної інформації

Стаття 15. Умови надання інформаційної продукції та послуг

Стаття 16. Відносини виробників і споживачів науково-технічної інформації

Розділ V. ДЕРЖАВНА ПОЛІТИКА У СФЕРІ НАУКОВО-ТЕХНІЧНОЇ ІНФОРМАЦІЇ

Стаття 17. Державна підтримка науково-інформаційної діяльності

Стаття 18. Державне управління у сфері науково-технічної інформації

Стаття 19. Відповідальність за порушення законодавства України про науково-технічну інформацію

Розділ VI. МІЖНАРОДНЕ СПІВРОБІТНИЦТВО У СФЕРІ НАУКОВО-ТЕХНІЧНОЇ ІНФОРМАЦІЇ

Стаття 20. Міжнародна інформаційна діяльність

Стаття 21. Міждержавний обмін науково-технічною інформацією

Стаття 22. Діяльність іноземних фізичних та юридичних осіб в Україні у сфері науково-технічної інформації

Стаття 23. Забезпечення суверенітету України у сфері науково-технічної інформації

Метою Закону є створення в Україні правової бази для одержання та використання науково-технічної інформації.

Законом регулюються правові і економічні відносини громадян, юридичних осіб, держави, що виникають при створенні, одержанні, використанні та поширенні науково-технічної інформації, а також визначаються правові форми міжнародного співробітництва в цій галузі.

Дія Закону поширюється на підприємства, установи, організації незалежно від форм власності, а також громадян, які мають право на одержання, використання та поширення науково-технічної інформації. Дія Закону не поширюється на інформацію, що містить державну та іншу охоронювану законом таємницю.

Розділ І. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення термінів

У цьому Законі наведені нижче терміни вживаються в такому значенні:

– науково-технічна інформація – будь-які відомості та/або дані про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, одержані в ході науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;

– науково-інформаційна діяльність – це сукупність дій, спрямованих на задоволення потреб громадян, юридичних осіб і держави у науково-технічній інформації, що полягає в її збиранні, аналітично-синтетичній обробці, фіксації, зберіганні, пошуку і поширенні;

– інформаційні ресурси науково-технічної інформації – це систематизоване зібрання науково-технічної літератури і документації (книги, брошури, періодичні видання, патентна документація, нормативно-технічна документація, промислові каталоги, конструкторська документація, звітна науково-технічна документація з науково-дослідних і дослідно-конструкторських робіт, депоновані рукописи, переклади науково-технічної літератури і документації), зафіксовані на паперових чи інших носіях;

– довідково-інформаційний фонд – це сукупність упорядкованих первинних документів і довідково-пошукового апарату, призначених для задоволення інформаційних потреб;

– довідково-пошуковий апарат – це сукупність упорядкованих вторинних документів, створюваних для пошуку першоджерел;

– інформаційні ресурси спільного користування – це сукупність інформаційних ресурсів державних органів науково-технічної інформації, наукових, науково-технічних бібліотек, а також комерційних центрів, фірм, організацій, які займаються науково-технічною діяльністю і з власниками яких укладено договори про їх спільне використання;

– аналітично-синтетична обробка науково-технічної інформації – це процес обробки інформації шляхом аналізу і синтезу змісту документів з метою одержання необхідних відомостей, а також шляхом їх класифікації, оцінки, співставлення і узагальнення;

– інформаційний ринок – це система економічних, організаційних і правових відносин щодо продажу і купівлі інформаційних ресурсів, технологій, продукції та послуг.

Стаття 2. Об'єкт відносин у сфері науково-технічної інформації

Об'єктом відносин у сфері науково-технічної інформації є вітчизняна і зарубіжна науково-технічна інформація.

Науково-технічна інформація охоплює отримувані в процесі науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності результати, зафіксовані у формі, яка забезпечує їх відтворення, використання та поширення.

Науково-технічна інформація є суспільним надбанням, необхідною умовою продуктивної інтелектуальної діяльності, зокрема наукової і технічної творчості.

Науково-технічна інформація, що є продуктом інтелектуальної творчої праці, становить об'єкт права інтелектуальної власності, а відносини щодо її придбання, зберігання, переробки, використання і поширення регулюються чинним законодавством.

Стаття 3. Суб'єкти відносин у сфері науково-технічної інформації

1. Суб'єктами відносин, що регулюються цим Законом, є державні органи, органи місцевого і регіонального самоврядування, юридичні особи та громадяни України, міжнародні організації, іноземні юридичні особи і громадяни та особи без громадянства.

2. Фізичні та юридичні особи у сфері дії цього Закону виступають як творці і накопичувачі науково-технічної інформації, власники, виробники, зберігачі і споживачі інформаційної продукції та послуг, а також як посередники у сфері науково-інформаційної діяльності.

Стаття 4. Законодавство України у сфері науково-технічної інформації

Відповідно до Конституції законодавство України у сфері науково-технічної інформації складається з Закону України "Про інформацію", цього Закону та інших актів законодавства.

Розділ II. ПРАВОВИЙ РЕЖИМ НАУКОВО-ТЕХНІЧНОЇ ІНФОРМАЦІЇ

Стаття 5. Право на науково-технічну інформацію

1. Усі громадяни України, юридичні особи, державні органи, органи місцевого і регіонального самоврядування відповідно до Конституції України і цього Закону мають право на відкриту науково-технічну інформацію, яке передбачає можливість вільного її одержання, зберігання, використання і поширення під час здійснення наукової, науково-дослідної, виробничої, громадської та іншої діяльності, що не забороняється чинним законодавством.

2. Режим доступу до відкритої науково-технічної інформації та інформації з обмеженим доступом регулюється чинним законодавством.

Стаття 6. Права на науково-технічну інформацію

1. Права на науково-технічну інформацію охороняються відповідно до закону.

2. Підставою виникнення прав на науково-технічну інформацію є створення науково-технічної інформації своїми силами і за свій рахунок; виконання договору про створення науково-технічної інформації; виконання будь-якого договору, що містить умови переходу прав на інформацію до іншої особи.

3. Права на науково-технічну інформацію, створену кількома особами, визначаються договором, укладеним між творцями цієї інформації.

4. Права на науково-технічну інформацію, створену за рахунок коштів державного бюджету, визначаються державою шляхом прийняття загальних рішень і шляхом укладення договорів між державним органом, що здійснює фінансування, і виконавцем робіт із створення науково-технічної інформації.

Права на науково-технічну інформацію, що належали фізичним та юридичним особам, можуть переходити до держави в разі передачі її до відповідних державних банків даних, фондів або архівів на договірній основі.

Стаття 7. Відносини між особами, яким належать права на науково-технічну інформацію, її споживачами і посередниками

1. Споживач науково-технічної інформації несе відповідальність за дотримання прав особи, якій належать права на цю інформацію. Споживач науково-технічної інформації не має права передачі одержаної науково-технічної інформації третій особі, якщо це не обумовлено договором з особою, якій належать права на науково-технічну інформацію.

Якщо споживач науково-технічної інформації одержав від особи, якій належать права на цю інформацію, або через посередника інформацію, що не відповідає умовам договору між ними, він має право вимагати безоплатного усунення недоліків у погоджений строк.

У разі відмови особи, якій належать права на цю інформацію, або посередника добровільно задовольнити законні вимоги споживача спір вирішується в суді.

2. Особа, якій належать права на інформацію, здійснює свої права щодо науково-технічної інформації самостійно або через посередника. Відносини між особою, якій належать права на інформацію, і посередником регулюються договором.

Розділ ІІІ. НАЦІОНАЛЬНА СИСТЕМА НАУКОВО-ТЕХНІЧНОЇ ІНФОРМАЦІЇ

Стаття 8. Визначення та склад національної системи науково-технічної інформації

1. Основною метою національної системи науково-технічної інформації є задоволення потреб громадян, юридичних осіб і держави в науково-технічній інформації.

Національна система науково-технічної інформації – це організаційно-правова структура, за допомогою якої формується державна інформаційна політика, а також здійснюється координація робіт по створенню, користуванню,

зберіганню та поширенню національних ресурсів науково-технічної інформації з урахуванням інтересів національної безпеки.

2. Національна система науково-технічної інформації складається з:

– спеціалізованих державних підприємств, установ, організацій, державних органів науково-технічної інформації, наукових і науково-технічних бібліотек, об'єднаних загальносистемними зв'язками та обов'язками;

– підприємств будь-яких організаційно-правових форм, заснованих на приватній чи колективній власності, предметом діяльності яких є інформаційне забезпечення народного господарства і громадян України.

Діяльність складових частин національної системи науково-технічної інформації здійснюється на основі договірно-обумовленого поділу праці в її збиранні, накопичуванні, переробці, зберіганні, поширенні та використанні.

3. Структура національної системи науково-технічної інформації, завдання і функції її основних інформаційних ланок щодо виконання загальносистемних зобов'язань, їх права і обов'язки визначаються положеннями, що затверджуються спеціально уповноваженим центральним органом державної виконавчої влади, який здійснює управління у сфері науково-технічної інформації.

4. Відносини між національною системою науково-технічної інформації України та системами науково-технічної інформації інших держав будуються на основі угод і договорів.

Стаття 9. Основні завдання національної системи науково-технічної інформації

Основними завданнями національної системи науково-технічної інформації є:

– формування на основі вітчизняних і зарубіжних джерел довідково-інформаційних фондів, включаючи бази і банки даних, та інформаційне забезпечення юридичних та фізичних осіб;

– одержання, обробка, зберігання, поширення і використання інформації, одержаної в процесі науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності юридичних та фізичних осіб;

– організація надходження до України, обробка, зберігання і поширення зарубіжної науково-технічної інформації на основі вивчення світового інформаційного ринку;

– підготовка аналітичних матеріалів, необхідних для прийняття державними органами, органами місцевого і регіонального самоврядування рішень з питань науково-технічного, економічного і соціального розвитку країни;

– аналітично-синтетична обробка першоджерел, реферування опублікованих і не опублікованих на території України джерел науково-технічної та економічної інформації, створення на цій основі і поширення інформаційної продукції та послуг;

– розроблення і впровадження сучасних технологій в науково-інформаційну діяльність;

– організація пропаганди і сприяння широкому використанню досягнень науки і техніки, передового виробничого досвіду;

– створення загальнодоступної мережі бібліотек, інформаційних центрів громадського користування як бази для освіти, виробництва та наукових досліджень, системи реалізації прав громадян на культурний та фаховий розвиток.

Стаття 10. Інформаційні ресурси національної системи науково-технічної інформації

1. Інформаційні ресурси національної системи науково-технічної інформації становлять сукупність довідково-інформаційних фондів з необхідним довідково-пошуковим апаратом і відповідними технічними засобами зберігання, обробки і передачі, що є у володінні, розпорядженні, користуванні державних органів і служб науково-технічної інформації, наукових і науково-технічних бібліотек, комерційних центрів, підприємств, установ і організацій.

2. Інформаційні ресурси науково-технічної інформації, що є власністю держави, визнаються державними ресурсами науково-технічної інформації. Їх розподіл між різними державними органами, службами, установами та порядок обміну може регулюватися на рівні загальнодержавних та відомчих рішень через уповноважені на те структури.

3. У поповненні інформаційних ресурсів національної системи науково-технічної інформації беруть участь фізичні і юридичні особи України незалежно від форм власності. При цьому законодавством України можуть встановлюватись обов'язкові норми їх участі (крім тієї, що реалізується на договірних засадах). Використання органами і службами науково-технічної інформації переданих їм підприємствами і організаціями матеріалів і технічної документації провадиться на умовах, встановлюваних підприємствами і організаціями – власниками цих матеріалів, крім випадків, коли законодавством не передбачено інше. Органи і служби науково-технічної інформації, яким передається така інформація, гарантують захист прав інтелектуальної власності, додержання комерційної таємниці, захист законних інтересів юридичних та фізичних осіб – творців інформації про науково-технічні досягнення.

4. Використання в процесі створення ресурсів науково-технічної інформації творів літератури, мистецтва і науки допускається за умов додержання авторського права. Це положення поширюється також на програмне забезпечення обчислювальної техніки і автоматизованих інформаційних систем.

Стаття 11. Державна реєстрація, облік і використання результатів науково-технічної діяльності

1. Результати науково-дослідної, дослідно-конструкторської, проектно-технологічної та іншої науково-технічної діяльності, фінансування якої повністю або частково здійснюється за рахунок коштів державного бюджету, підлягають обов'язковій реєстрації та обліку.

Порядок реєстрації та обліку визначається спеціально уповноваженим центральним органом виконавчої влади, що здійснює управління в сфері науково-технічної інформації.

2. Права на результати науково-дослідних, дослідно-конструкторських, проектно-технологічних та інших робіт, що проводяться за рахунок власних коштів юридичних та фізичних осіб, належать цим особам і реєструються ними на добровільних засадах в державному органі науково-технічної інформації з наступним поширенням звітних матеріалів самостійно або через відповідні служби науково-технічної інформації на договірній основі.

3. Відомості про всі зареєстровані в Україні результати науково-технічної діяльності з зазначенням місцезнаходження звітної документації та умов їх передачі розповсюджуються за запитом заінтересованих осіб та організацій органами і службами науково-технічної інформації, відповідальними за реєстрацію цих результатів, крім випадків обмежень, пов'язаних із державною чи комерційною таємницею.

Стаття 12. Організація надходження та використання зарубіжної науково-технічної інформації

Придбання зарубіжної науково-технічної літератури і документації, баз і банків даних, необхідних для формування державних ресурсів науково-технічної інформації, здійснюється як за безвалютним обміном, так і за рахунок інвалютних коштів органів і служб науково-технічної інформації. Для створення ресурсів зарубіжної науково-технічної інформації державних органів і наукових організацій, що фінансуються з бюджету, валютні кошти щорічно передбачаються в державному бюджеті цільовим призначенням.

Розділ IV. РИНОК НАУКОВО-ТЕХНІЧНОЇ ІНФОРМАЦІЇ

Стаття 13. Науково-технічна інформація як об'єкт товарних відносин

Інформаційна продукція та послуги органів науково-технічної інформації, а також підприємств, установ, організацій, окремих громадян, які здійснюють науково-інформаційну діяльність, можуть бути об'єктами товарних відносин, що регулюються чинним законодавством.

Ціни на інформаційну продукцію та послуги встановлюються договорами, за винятком випадків, передбачених цим Законом.

Стаття 14. Формування ринку науково-технічної інформації

1. Органи науково-технічної інформації, підприємства, організації, громадяни, що здійснюють науково-інформаційну діяльність і вільно реалізують свою інформаційну продукцію та інформаційні послуги, є товаровиробниками, які беруть участь у створенні ринку на загальних підставах незалежно від форм власності.

2. Товаровиробник має право вчиняти будь-які дії стосовно реалізації своєї продукції, що не суперечать чинному законодавству.

3. Підприємства, установи і організації незалежно від форм власності, що здійснюють науково-інформаційну діяльність, є вільними у виборі постачальників інформації, форм відносин з ними, методів і видів інформування, а також номенклатури інформаційної продукції та послуг, крім випадків, коли власники цих підприємств, установ і організацій встановлюють певні вимоги щодо номенклатури продукції, сфери інформаційного обслуговування тощо.

Стаття 15. Умови надання інформаційної продукції та послуг

1. Державні органи та служби науково-технічної інформації, які організують використання державних ресурсів науково-технічної інформації, здійснюють її пошук і передачу на безприбуткових засадах. У наукових і науково-технічних бібліотеках, які фінансуються з бюджету, науково-технічна інформація, що не потребує спеціального тематичного пошуку або копіювання, надається безплатно.

2. Огляди, аналітичні і фактографічні довідки, інші види інформаційної продукції, що готуються на основі аналізу, оцінки та узагальнення науково-технічної інформації (за винятком державних замовлень), реалізуються на комерційних засадах.

Без отримання прибутку здійснюється репродукування друкованих творів у галузі науки і техніки з науковою, навчальною і освітньою метою відповідно до чинного законодавства.

3. Державні органи та служби науково-технічної інформації, інші інформаційні центри, фірми, підприємства, установи і організації, які формують ресурси науково-технічної інформації за рахунок власних коштів, надають інформаційну продукцію і послуги на комерційних засадах.

4. У ході здійснення купівлі-продажу інформаційної продукції повинні гарантуватись охорона прав інтелектуальної власності, державної та комерційної таємниці, законні права та інтереси власника і виробника інформаційної продукції і послуг.

Стаття 16. Відносини виробників і споживачів науково-технічної інформації

Відносини між державними органами і службами науково-технічної інформації, підприємствами, установами і організаціями будь-яких форм власності, які здійснюють науково-інформаційну діяльність, і споживачами інформації будуються на основі контрактів (договорів) та на інших формах угод, передбачених чинним законодавством. Контракт (договір) є основним документом, що регламентує відносини між виробником і споживачем інформації.

На контрактній (договірній) основі можуть також здійснюватись інформаційне забезпечення, наукові дослідження і розробки для органів державної влади, крім випадків, коли діючими законами передбачено безплатне надання інформації цим органам.

Розрахунки з зарубіжними партнерами здійснюються на договірних умовах і в порядку, встановленому законодавством.

Розділ V. ДЕРЖАВНА ПОЛІТИКА У СФЕРІ НАУКОВО-ТЕХНІЧНОЇ ІНФОРМАЦІЇ

Стаття 17. Державна підтримка науково-інформаційної діяльності

1. Держава з метою створення та розвитку національної системи науково-технічної інформації забезпечує:

– створення державних мереж первинного збирання, обробки та зберігання усіх видів науково-технічної інформації;

– проведення заходів для поширення і підвищення якісного рівня інформаційної продукції та послуг;

– фінансову, в тому числі валютну, підтримку надходження науково-технічної інформації до державних органів і служб науково-технічної інформації, наукових і науково-технічних бібліотек, створення їх мереж і відповідного технічного забезпечення;

– підготовку кадрів у сфері інформатики і науково-інформаційної діяльності через систему навчальних закладів вищої та середньої освіти, підвищення рівня інформаційної підготовки спеціалістів народного господарства;

– вільну конкуренцію між органами науково-технічної інформації, іншими підприємствами та організаціями усіх форм власності, які здійснюють науково-інформаційну діяльність;

– захист суб'єктів відносин в галузі науково-технічної інформації від прояву недобросовісної конкуренції та монополізму в будь-яких сферах науково-інформаційної діяльності.

2. Держава сприяє відкритості та загальнодоступності науково-технічної інформації.

Обмеження щодо доступу, поширення та використання інформації, яка є державною або іншою таємницею, що охороняється законом, визначаються законами України.

3. Держава підтримує міжнародне співробітництво у сфері науково-технічної інформації, створює для цього правові і економічні умови та сприяє здійсненню суб'єктами науково-інформаційної діяльності вільних і рівноправних відносин з міжнародними організаціями і установами, якщо це не суперечить чинному законодавству України.

4. Держава сприяє формуванню, зберіганню і ефективному використанню державних ресурсів науково-технічної інформації шляхом:

– створення реєстраційно-облікового механізму, який забезпечує збирання, обробку і поширення відомостей про виконані за рахунок коштів державного бюджету наукові дослідження і розробки, дисертації та інші види науково-технічних робіт, про нові види продукції, бази і банки даних;

– проведення пільгової податкової та фінансово-кредитної політики щодо послуг з надання науково-технічної інформації споживачеві та передачі інформації про науково-технічні досягнення державним органам і службам науково-технічної інформації;

– виділення коштів і матеріально-технічних засобів для роботи над створенням і розвитком державних ресурсів науково-технічної інформації та їх використанням, а також для міжгалузевого обміну інформацією про науково-технічні досягнення;

– створення механізму зберігання інформаційних ресурсів, баз і банків даних, сформованих в державних організаціях та органах управління, їх відповідної передачі іншим установам в разі ліквідації або реорганізації;

– впровадження економічних механізмів створення і підтримки підприємств, заснованих на приватній чи колективній власності, які здійснюють інформаційну діяльність, та їх інтеграції в національну систему науково-технічної інформації.

Стаття 18. Державне управління у сфері науково-технічної інформації

Кабінет Міністрів України визначає орган державного управління, який забезпечує організацію діяльності у сфері науково-технічної інформації, здійснює функціональне управління національною системою науково-технічної інформації, формує і реалізує політику в цій сфері.

Стаття 19. Відповідальність за порушення законодавства України про науково-технічну інформацію

Порушення законодавства України про науково-технічну інформацію тягне за собою відповідальність згідно з чинним законодавством.

Розділ VI. МІЖНАРОДНЕ СПІВРОБІТНИЦТВО У СФЕРІ НАУКОВО-ТЕХНІЧНОЇ ІНФОРМАЦІЇ

Стаття 20. Міжнародна інформаційна діяльність

Міжнародне співробітництво у сфері науково-технічної інформації та міжнародна інформаційна діяльність регулюються згідно з чинним законодавством.

Стаття 21. Міждержавний обмін науково-технічною інформацією

1. Міждержавний обмін науково-технічною інформацією здійснюється відповідно до угод, підписаних Україною.

2. Держава забезпечує відкритий і рівноправний доступ своїх громадян і громадян держав – партнерів за угодами до інформаційних ресурсів спільного користування.

3. Уряд України визначає національний інформаційний центр, який координує міждержавний обмін науково-технічною інформацією.

Стаття 22. Діяльність іноземних фізичних та юридичних осіб в Україні у сфері науково-технічної інформації

Іноземні юридичні та фізичні особи, а також особи без громадянства можуть інвестувати розвиток сфери науково-технічної інформації України відповідно до чинного законодавства.

Стаття 23. Забезпечення суверенітету України у сфері науково-технічної інформації

Суверенітет України у сфері науково-технічної інформації забезпечується:

– організацією та державною підтримкою власних інформаційних систем і наданням для них можливостей шукати, фіксувати, отримувати, оброблювати і поширювати в інтересах суспільства науково-технічну інформацію, вироблену в Україні або в інших країнах світу;

– встановленням власності держави на ресурси науково-технічної інформації, що формуються за рахунок коштів бюджету;

– створенням і розвитком національної системи науково-технічної інформації;

– організацією доступу інших держав до інформаційних ресурсів України на основі укладання угод та договорів про їх спільне використання, ліцензуванням і квотуванням науково-технічної інформації, яка може бути використана за межами України для виготовлення зброї, військової техніки, наукоємної продукції;

– організацією належної системи охорони та зберігання інформації.

А.3. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»

Цей Закон регулює відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах (далі – система) та складається з наступних статей.

Стаття 1. Визначення термінів

Стаття 2. Об'єкти захисту в системі

Стаття 3. Суб'єкти відносин

Стаття 4. Доступ до інформації в системі

Стаття 5. Відносини між володільцем інформації та власником системи

Стаття 6. Відносини між власником системи та користувачем

Стаття 7. Відносини між власниками систем

Стаття 8. Умови обробки інформації в системі

Стаття 9. Забезпечення захисту інформації в системі

Стаття 10. Повноваження державних органів у сфері захисту інформації в системах

Стаття 11. Відповідальність за порушення законодавства про захист інформації в системах

Стаття 12. Міжнародні договори

Стаття 1. Визначення термінів

У цьому Законі наведені нижче терміни вживаються в такому значенні:

– блокування інформації в системі – дії, внаслідок яких унеможливлюється доступ до інформації в системі;

– виток інформації – результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї;

– володілець інформації – фізична або юридична особа, якій належать права на інформацію;

– власник системи – фізична або юридична особа, якій належить право власності на систему;

– доступ до інформації в системі – отримання користувачем можливості обробляти інформацію в системі;

– захист інформації в системі – діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі;

– знищення інформації в системі – дії, внаслідок яких інформація в системі зникає;

– інформаційна (автоматизована) система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;

– інформаційно-комунікаційна система – сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле;

– комплексна система захисту інформації – взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації;

– користувач інформації в системі (далі – користувач) – фізична або юридична особа, яка в установленому законодавством порядку отримала право доступу до інформації в системі;

– криптографічний захист інформації – вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

– несанкціоновані дії щодо інформації в системі – дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства;

– обробка інформації в системі – виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів;

– порушення цілісності інформації в системі – несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст;

– порядок доступу до інформації в системі – умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації;

– електронна комунікаційна система – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання та/або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;

– технічний захист інформації – вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації;

– резервна копія державних інформаційних ресурсів – копія інформації, яка міститься в державних інформаційних ресурсах, що перебувають у володінні або розпорядженні органів державної влади, органів місцевого самоврядування, військових формувань, утворених відповідно до законів України, державних підприємств, установ та організацій, та є критичною для їх сталого функціонування, створюється, записується, обробляється або зберігається у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів з метою подальшого відновлення цієї інформації;

– резервування державних інформаційних ресурсів та систем – сукупність заходів, спрямованих на забезпечення створення резервної копії (резервних копій) та зберігання державних інформаційних ресурсів та систем з метою забезпечення безперервності їх роботи та подальшого відновлення інформації, що міститься в державних інформаційних ресурсах та системах, а також інсталяційних копій програмного забезпечення та операційних систем (та/або їх

образів), в яких здійснюється їх обробка. Перелік видів державних інформаційних ресурсів та систем, щодо яких може здійснюватися резервне копіювання, визначається Кабінетом Міністрів України.

Стаття 2. Об'єкти захисту в системі

Об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

Стаття 3. Суб'єкти відносин

Суб'єктами відносин, пов'язаних із захистом інформації в системах, є:

– володільці інформації;

– власники системи;

– користувачі;

– спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації і підпорядковані йому регіональні органи;

На підставі укладеного договору або за дорученням власник системи може надати право розпоряджатися системою іншій фізичній або юридичній особі – розпоряднику системи.

Стаття 4. Доступ до інформації в системі

Порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються володільцем інформації.

Порядок доступу до державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, перелік користувачів та їх повноваження стосовно цієї інформації визначаються законодавством.

У випадках, передбачених законом, доступ до інформації в системі може здійснюватися без дозволу її володільця в порядку, встановленому законом.

Стаття 5. Відносини між володільцем інформації та власником системи

Власник системи забезпечує захист інформації в системі в порядку та на умовах, визначених у договорі, який укладається ним із володільцем інформації, якщо інше не передбачено законом.

Власник системи на вимогу володільця інформації надає відомості щодо захисту інформації в системі.

Протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування володільці інформації – власники (держателі) державних інформаційних ресурсів можуть укладати договори про технічне адміністрування відповідних реєстрів з іноземними компаніями, організаціями – постачальниками послуг з надання хмарних ресурсів (надавачами хмарних послуг), утвореними відповідно до законодавства інших держав, та/або їх зареєстрованими (акредитованими або легалізованими) відповідно до законодавства України філіями, представництвами та іншими відокремленими підрозділами з місцезнаходженням на території України в порядку, встановленому Кабінетом Міністрів України.

Стаття 6. Відносини між власником системи та користувачем

Власник системи надає користувачеві відомості про правила і режим роботи системи та забезпечує йому доступ до інформації в системі відповідно до визначеного порядку доступу.

Стаття 7. Відносини між власниками систем

Власник системи, яка використовується для обробки інформації з іншої системи, забезпечує захист такої інформації в порядку та на умовах, що визначаються договором, який укладається між власниками систем, якщо інше не встановлено законодавством.

Власник системи, яка використовується для обробки інформації з іншої системи, повідомляє власника зазначеної системи про виявлені факти несанкціонованих дій щодо інформації в системі.

Стаття 8. Умови обробки інформації в системі

Умови обробки інформації в системі визначаються власником системи відповідно до договору з володільцем інформації, якщо інше не передбачено законодавством.

Державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності комплексної системи захисту інформації здійснюється за результатами державної експертизи, яка проводиться з урахуванням галузевих вимог та норм інформаційної безпеки у порядку, встановленому законодавством.

Підтвердження відповідності та проведення державної експертизи засобів технічного і криптографічного захисту інформації здійснюються в порядку, встановленому законодавством. Для створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби криптографічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації, та засоби технічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері технічного захисту інформації або сертифікат відповідності, виданий органом з оцінки відповідності, який акредитовано:

– національним органом України з акредитації;

– чи національним органом з акредитації іншої держави, якщо і національний орган України з акредитації, і національний орган з акредитації такої держави є членами міжнародної або регіональної організації з акредитації та/або уклали з такою організацією угоду про взаємне визнання щодо оцінки відповідності.

Державні інформаційні ресурси та інформація з обмеженим доступом, крім державної таємниці, службової інформації та державних і єдиних реєстрів, створення та забезпечення функціонування яких визначено законами, можуть оброблятися в системі без застосування комплексної системи захисту інформації у разі виконання всіх таких умов:

– підтвердження відповідності системи управління інформаційною безпекою за результатами процедури з оцінки відповідності національним стандартам України щодо систем управління інформаційною безпекою, яка проведена органом з оцінки відповідності, акредитованим національним органом України з акредитації чи національним органом з акредитації іншої держави, якщо і національний орган України з акредитації, і національний орган з акредитації такої держави є членами міжнародної або регіональної організації з акредитації та/або уклали з такою організацією угоду про взаємне визнання щодо оцінки відповідності;

– використання для захисту інформації в системі засобів криптографічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації;

– жоден з елементів системи не може бути розташований, а власник такої системи або його офіційний представник не може бути юридичною особою (його представником), зареєстрованою на територіях України, на яких органи державної влади України тимчасово не здійснюють своїх повноважень, на територіях держав, визнаних Верховною Радою України державами-агресорами, на територіях держав, щодо яких застосовані санкції відповідно до Закону України "Про санкції", та на територіях держав, які входять до митних союзів з такими державами;

– власник системи або його представник, який надає послуги з використанням системи, елементи якої розміщуються поза межами України, має бути юридичною особою, зареєстрованою в Україні, або мати свого офіційного представника в Україні;

– виконання особливих вимог, встановлених Кабінетом Міністрів України до забезпечення захисту інформації в системах залежно від категорії державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, що обробляються.

Власники систем для забезпечення належного функціонування систем та захисту інформації, що обробляється в них:

– створюють резервні копії державних інформаційних ресурсів та систем із дотриманням встановлених для таких ресурсів та систем вимог щодо їх захисту, цілісності та конфіденційності;

– забезпечують створення резервних копій державних інформаційних ресурсів та систем на окремих фізичних носіях у зашифрованому вигляді та їх подальшу передачу (переміщення) для зберігання в установленому законодавством порядку, у тому числі за межами України (зокрема в закордонних дипломатичних установах України), протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування;

– забезпечують в установленому законодавством порядку передачу (переміщення) державних інформаційних ресурсів та їх резервних копій для розміщення на хмарних ресурсах та/або в центрах обробки даних, розташованих за межами України, протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування.

Порядок передачі, зберігання, функціонування та доступу до державних інформаційних ресурсів та їх резервних копій встановлюється Кабінетом Міністрів України.

Розміщення систем та зберігання резервних копій державних інформаційних ресурсів та систем на територіях України, на яких органи державної влади України тимчасово не здійснюють свої повноваження, територіях держав, визнаних Верховною Радою України державами-агресорами, територіях держав, щодо яких застосовані санкції відповідно до Закону України "Про санкції", та територіях держав, які входять до митних та воєнних союзів з такими державами, забороняється.

Стаття 9. Забезпечення захисту інформації в системі

Відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

Власник системи, в якій обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним.

Про спроби та/або факти несанкціонованих дій у системі щодо державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, власник системи повідомляє відповідно спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкований йому регіональний орган.

Стаття 10. Повноваження державних органів у сфері захисту інформації в системах

Вимоги до забезпечення захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, встановлюються Кабінетом Міністрів України.

Спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації:

– розробляє пропозиції щодо державної політики у сфері захисту інформації та забезпечує її реалізацію в межах своєї компетенції;

– визначає вимоги та порядок створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

– організовує проведення державної експертизи комплексних систем захисту інформації, експертизи та підтвердження відповідності засобів технічного і криптографічного захисту інформації;

– здійснює контроль за забезпеченням захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

– здійснює заходи щодо виявлення загрози державним інформаційним ресурсам від несанкціонованих дій в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах та дає рекомендації з питань запобігання такій загрозі.

Державні органи в межах своїх повноважень за погодженням відповідно із спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкованим йому регіональним органом встановлюють особливості захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.

Особливості захисту інформації в системах, які забезпечують банківську діяльність, встановлюються Національним банком України.

Стаття 11. Відповідальність за порушення законодавства про захист інформації в системах

Особи, винні в порушенні законодавства про захист інформації в системах, несуть відповідальність згідно із законом.

Стаття 12. Міжнародні договори

Якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, визначено інші правила, ніж ті, що передбачені цим Законом, застосовуються норми міжнародного договору.

А.4. Закон України «Про основні засади забезпечення кібербезпеки України»

Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки, та складається з наступних статей.

Стаття 1. Визначення термінів

Стаття 2. Принципи застосування Закону

Стаття 3. Правові основи забезпечення кібербезпеки України

Стаття 4. Об’єкти кібербезпеки та кіберзахисту

Стаття 5. Суб’єкти забезпечення кібербезпеки

Стаття 6. Об’єкти критичної інфраструктури

Стаття 7. Принципи забезпечення кібербезпеки

Стаття 8. Національна система кібербезпеки

Стаття 9. Урядова команда реагування на комп’ютерні надзвичайні події України CERT-UA

Стаття 10. Державно-приватна взаємодія у сфері кібербезпеки

Стаття 11. Сприяння суб’єктам забезпечення кібербезпеки України

Стаття 12. Відповідальність за порушення законодавства у сфері кібербезпеки

Стаття 13. Фінансове забезпечення заходів кібербезпеки

Стаття 14. Міжнародне співробітництво у сфері кібербезпеки

Стаття 15. Контроль за законністю заходів із забезпечення кібербезпеки України

Стаття 1. Визначення термінів

У цьому Законі наведені нижче терміни вживаються в такому значенні:

– індикатори кіберзагроз – показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози;

– інформація про інцидент кібербезпеки – відомості про обставини кіберінциденту, зокрема про те, які об’єкти кіберзахисту і за яких умов зазнали кібератаки, які з них успішно виявлені, нейтралізовані, яким запобігли за допомогою яких засобів кіберзахисту, у тому числі з використанням яких індикаторів кіберзагроз;

– інцидент кібербезпеки (далі – кіберінцидент) – подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування

роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів;

– кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту;

– кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі;

– кіберзагроза – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів;

– кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем;

– кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України;

– кіберзлочинність – сукупність кіберзлочинів;

– кібероборона – сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії;

– кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних;

– кіберрозвідка – діяльність, що здійснюється розвідувальними органами у кіберпросторі або з його використанням;

– кібертероризм – терористична діяльність, що здійснюється у кіберпросторі або з його використанням;

– кібершпигунство – шпигунство, що здійснюється у кіберпросторі або з його використанням;

– критична інформаційна інфраструктура – сукупність об’єктів критичної інформаційної інфраструктури;

– Національна телекомунікаційна мережа – сукупність спеціальних телекомунікаційних систем (мереж), систем спеціального зв’язку, інших комунікаційних систем, які використовуються в інтересах органів державної влади та органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону, призначена для обігу (передавання, приймання, створення, оброблення, зберігання) та захисту національних інформаційних ресурсів, забезпечення захищених електронних комунікацій, надання спектра сучасних захищених інформаційно-комунікаційних (мультисервісних) послуг в інтересах здійснення управління державою у мирний час, в умовах надзвичайного стану та в особливий період, та яка є мережею (системою) подвійного призначення з використанням частини її ресурсу для надання послуг, зокрема з кіберзахисту, іншим споживачам;

– національні електронні інформаційні ресурси (далі – національні інформаційні ресурси) – систематизовані електронні інформаційні ресурси, які містять інформацію незалежно від виду, змісту, форми, часу і місця її створення (включаючи публічну інформацію, державні інформаційні ресурси та іншу інформацію), призначену для задоволення життєво важливих суспільних потреб громадянина, особи, суспільства і держави. Під електронними інформаційними ресурсами розуміється будь-яка інформація, що створена, записана, оброблена або збережена у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів;

– Національний центр резервування державних інформаційних ресурсів – організована сукупність об’єктів, створених з метою забезпечення надійності та безперебійності роботи державних інформаційних ресурсів, кіберзахисту, зберігання національних електронних інформаційних ресурсів, резервного копіювання інформації та відомостей національних електронних інформаційних ресурсів державних органів, військових формувань, утворених відповідно до законів, підприємств, установ та організацій;

– об’єкт критичної інформаційної інфраструктури – комунікаційна або технологічна система об’єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об’єкта критичної інфраструктури;

– система управління технологічними процесами (далі – технологічна система) – автоматизована або автоматична система, яка є сукупністю обладнання, засобів, комплексів та систем обробки, передачі та приймання, призначена для організаційного управління та/або управління технологічними процесами (включаючи промислове, електронне, комунікаційне обладнання,

інші технічні та технологічні засоби) незалежно від наявності доступу системи до мережі Інтернет та/або інших глобальних мереж передачі даних;

– системи електронних комунікацій (далі – комунікаційні системи) – системи передавання, комутації або маршрутизації, обладнання та інші ресурси (включаючи пасивні мережеві елементи, які дають змогу передавати сигнали за допомогою проводових, радіо-, оптичних або інших електромагнітних засобів, мережі мобільного, супутникового зв'язку, електричні кабельні мережі в частині, в якій вони використовуються для цілей передачі сигналів), що забезпечують електронні комунікації (передачу електронних інформаційних ресурсів), у тому числі засоби і пристрої зв'язку, комп'ютери, інша комп'ютерна техніка, інформаційно-телекомунікаційні системи, які мають доступ до мережі Інтернет та/або інших глобальних мереж передачі даних;

– система активної протидії агресії у кіберпросторі – сукупність організаційних, правових, наукових та технічних заходів, спрямованих на підвищення рівня кіберзахисту держави шляхом здійснення впливу на інформаційні (автоматизовані), електронно-комунікаційні, інформаційно-комунікаційні системи держави-агресора, джерела походження кіберзагроз та кібератак;

– активна протидія агресії у кіберпросторі – дії, спрямовані на підвищення рівня кіберзахисту шляхом нейтралізації кібератак держави-агресора, його систем і мереж, а також джерел походження кіберзагроз та кібератак, які використовуються для завдання шкоди національній безпеці України.

Терміни "національна безпека", "національні інтереси", "загрози національній безпеці" вживаються в цьому Законі у значенні, визначеному Законом України "Про основи національної безпеки України". Термін "об'єкт критичної інфраструктури" вживається в цьому Законі у значенні, визначеному Законом України "Про критичну інфраструктуру".

Термін "платіжний ринок" вживається в цьому Законі у значенні, наведеному в Законі України "Про платіжні послуги".

Стаття 2. Принципи застосування Закону

1. Цей Закон не поширюється на:

– відносини та послуги, пов'язані із змістом інформації, що обробляється (передається, зберігається) в комунікаційних та/або в технологічних системах;

– діяльність, пов'язану із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення;

– соціальні мережі, приватні електронні інформаційні ресурси в мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси), якщо такі інформаційні ресурси не містять інформацію, необхідність захисту якої встановлена законом, відносини та послуги, пов'язані з функціонуванням таких мереж і ресурсів;

– комунікаційні системи, які не взаємодіють з публічними мережами електронних комунікацій (електронними мережами загального користування), не підключені до мережі Інтернет та/або інших глобальних мереж передачі даних (крім технологічних систем).

2. Застосування законодавства у сфері кібербезпеки та прийняття суб'єктами владних повноважень рішень на виконання норм цього Закону здійснюються з додержанням принципів:

– мінімально необхідного регулювання, згідно з яким рішення (заходи) суб'єктів владних повноважень повинні бути необхідними і мінімально достатніми для досягнення мети і завдань, визначених цим Законом;

– об'єктивності та правової визначеності, максимально можливого застосування національного та міжнародного права щодо повноважень і обов'язків державних органів, підприємств, установ, організацій, громадян у сфері кібербезпеки;

– забезпечення захисту прав користувачів комунікаційних систем та/або споживачів послуг електронних комунікацій, та/або послуг із захисту інформації, кіберзахисту, у тому числі прав щодо невтручання у приватне життя і захисту персональних даних;

– прозорості, згідно з яким рішення (заходи) суб'єктів владних повноважень мають бути належним чином обґрунтовані та повідомлені суб'єктам, яких вони стосуються, до набрання ними чинності (їх застосування);

– збалансованості вимог та відповідальності, згідно з яким має бути забезпечено баланс між встановленням відповідальності за невиконання вимог кібербезпеки та кіберзахисту, а також за запровадження надмірних вимог та обмежень;

– недискримінації, згідно з яким рішення, дії та бездіяльність суб'єктів владних повноважень не можуть призводити до юридичного або фактичного обсягу прав та обов'язків особи, який є:

– відмінним від обсягу прав та обов'язків інших осіб у подібних ситуаціях, якщо тільки така відмінність не є необхідною та мінімально достатньою для задоволення загальносуспільного інтересу;

– таким, як і обсяг прав та обов'язків інших осіб у неподібних ситуаціях, якщо така однаковість не є необхідною та мінімально достатньою для задоволення загальносуспільного інтересу;

– еквівалентності вимог до забезпечення кібербезпеки об'єктів критичної інфраструктури, згідно з яким застосування правових норм повинно бути якомога більш рівнозначним щодо кіберзахисту комунікаційних та технологічних систем об'єктів критичної інфраструктури, що належать до одного сектору економіки та/або які здійснюють аналогічні функції.

Зазначені принципи застосовуються без переваги будь-якого з них з урахуванням мети і завдань цього Закону.

Стаття 3. Правові основи забезпечення кібербезпеки України

1. Правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, цей та інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою

України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України.

2. Якщо міжнародним договором України, згоду на обов'язковість якого надано Верховною Радою України, передбачено інші правила, ніж встановлені цим Законом, застосовуються положення міжнародного договору України.

Стаття 4. Об'єкти кібербезпеки та кіберзахисту

1. Об'єктами кібербезпеки є:

– конституційні права і свободи людини і громадянина;

– суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;

– держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;

– національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;

– об'єкти критичної інфраструктури.

2. Об'єктами кіберзахисту є:

– комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;

– об'єкти критичної інформаційної інфраструктури;

3) комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

3. Порядок формування переліку об'єктів критичної інформаційної інфраструктури, перелік таких об'єктів та порядок їх внесення до державного реєстру об'єктів критичної інформаційної інфраструктури, а також порядок формування та забезпечення функціонування державного реєстру об'єктів критичної інформаційної інфраструктури затверджуються Кабінетом Міністрів України.

Повноваження щодо формування та забезпечення функціонування реєстру об'єктів критичної інформаційної інфраструктури у банківській системі України покладаються на Національний банк України.

Стаття 5. Суб'єкти забезпечення кібербезпеки

1. Координація діяльності у сфері кібербезпеки як складової національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України.

2. Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України.

3. Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і

громадянина, національних інтересів України у кіберпросторі, боротьбу з кіберзлочинністю; організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури (крім об'єктів критичної інфраструктури у банківській системі України).

4. Суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є:

– міністерства та інші центральні органи виконавчої влади;

– місцеві державні адміністрації;

– органи місцевого самоврядування;

– правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності;

– Збройні Сили України, інші військові формування, утворені відповідно до закону;

– Національний банк України;

– підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури;

– суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

5. Суб'єкти забезпечення кібербезпеки у межах своєї компетенції:

– здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях;

– здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;

– здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз;

– розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту;

– забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління;

– здійснюють інші заходи із забезпечення розвитку та безпеки кіберпростору.

Стаття 6. Об'єкти критичної інфраструктури

1. Віднесення об'єктів до об'єктів критичної інфраструктури та формування Реєстру об'єктів критичної інфраструктури здійснюються відповідно до Закону України "Про критичну інфраструктуру".

2. Критерії та порядок віднесення об'єктів до об'єктів критичної інфраструктури, перелік таких об'єктів, загальні вимоги до їх кіберзахисту, у тому числі щодо застосування індикаторів кіберзагроз, та вимоги до проведення незалежного аудиту інформаційної безпеки затверджуються Кабінетом

Міністрів України, а щодо банків, інших осіб, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг – Національним банком України.

3. Вимоги і порядок проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури встановлюються відповідними нормативно-правовими актами з аудиту інформаційної безпеки, що затверджуються Кабінетом Міністрів України.

Розроблення нормативно-правових актів з незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури здійснюється на основі міжнародних стандартів, стандартів Європейського Союзу та НАТО з обов'язковим залученням представників основних суб'єктів національної системи кібербезпеки, наукових установ, незалежних аудиторів та експертів у сфері кібербезпеки, громадських організацій.

4. Відповідальність за забезпечення кіберзахисту комунікаційних і технологічних систем об'єктів критичної інфраструктури, захисту технологічної інформації відповідно до вимог законодавства, за невідкладне інформування урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA про інциденти кібербезпеки, за організацію проведення незалежного аудиту інформаційної безпеки на таких об'єктах покладається на власників та/або керівників підприємств, установ та організацій, віднесених до об'єктів критичної інфраструктури.

5. Обмін інформацією про інциденти кібербезпеки, що містить персональні дані, здійснюється з дотриманням вимог Закону України "Про захист персональних даних".

Стаття 7. Принципи забезпечення кібербезпеки

1. Забезпечення кібербезпеки в Україні ґрунтується на принципах:

– верховенства права, законності, поваги до прав людини і основоположних свобод та їх захисту в порядку, визначеному законом;

– забезпечення національних інтересів України;

– відкритості, доступності, стабільності та захищеності кіберпростору, розвитку мережі Інтернет та відповідальних дій у кіберпросторі;

– державно-приватної взаємодії, широкої співпраці з громадянським суспільством у сфері кібербезпеки та кіберзахисту, зокрема шляхом обміну інформацією про інциденти кібербезпеки, реалізації спільних наукових та дослідницьких проектів, навчання та підвищення кваліфікації кадрів у цій сфері;

– пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам, реалізації невід'ємного права держави на самозахист відповідно до норм міжнародного права у разі вчинення агресивних дій у кіберпросторі;

– пріоритетності запобіжних заходів;

– невідворотності покарання за вчинення кіберзлочинів;

– пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу;

– міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в терористичних, воєнних, інших протиправних цілях;

– забезпечення демократичного цивільного контролю за утвореними відповідно до законів України військовими формуваннями та правоохоронними органами, що провадять діяльність у сфері кібербезпеки.

Стаття 8. Національна система кібербезпеки

1. Національна система кібербезпеки є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури.

2. Основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України, які відповідно до Конституції і законів України виконують в установленому порядку такі основні завдання:

– Державна служба спеціального зв'язку та захисту інформації України забезпечує формування та реалізацію державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, активної протидії агресії у кіберпросторі, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснює державний контроль у цих сферах; координує діяльність інших суб'єктів забезпечення кібербезпеки щодо кіберзахисту; забезпечує створення та функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту; здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків; інформує про кіберзагрози та відповідні методи захисту від них; забезпечує впровадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації (переатестації); координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість; забезпечує функціонування Державного центру кіберзахисту та Центру активної протидії агресії у кіберпросторі, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA;

– Національна поліція України забезпечує захист прав і свобод людини і громадянина, інтересів суспільства і держави від кримінально протиправних посягань у кіберпросторі; здійснює заходи із запобігання, виявлення,

припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі;

– Служба безпеки України здійснює запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласно перевіряє готовність об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки;

– Міністерство оборони України, Генеральний штаб Збройних Сил України відповідно до компетенції здійснюють заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); здійснюють військову співпрацю з НАТО та іншими суб'єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз; впроваджують заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану;

– розвідувальні органи України здійснюють розвідувальну діяльність щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки;

– Національний банк України визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки банками, іншими особами, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторами платіжних систем та/або учасниками платіжних систем, технологічними операторами платіжних послуг, здійснює контроль за їх виконанням; створює центр кіберзахисту Національного банку України, забезпечує функціонування системи кіберзахисту для банків, інших осіб, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг; забезпечує проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки на об'єктах критичної інфраструктури в банках, інших особах, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторах платіжних систем та/або учасниках платіжних систем, технологічних операторах платіжних послуг.

3. Функціонування національної системи кібербезпеки забезпечується шляхом:

– вироблення і оперативної адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягнення сумісності з відповідними стандартами Європейського Союзу та НАТО;

– створення нормативно-правової та термінологічної бази у сфері кібербезпеки, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної безпеки та кібербезпеки відповідно до міжнародних стандартів, зокрема стандартів Європейського Союзу та НАТО;

– встановлення обов'язкових вимог інформаційної безпеки об'єктів критичної інформаційної інфраструктури, у тому числі під час їх створення, введення в експлуатацію, експлуатації та модернізації з урахуванням міжнародних стандартів та специфіки галузі, до якої належать відповідні об'єкти критичної інформаційної інфраструктури;

– формування конкурентного середовища у сфері електронних комунікацій, надання послуг із захисту інформації та кіберзахисту;

– залучення експертного потенціалу наукових установ, професійних та громадських об'єднань до підготовки проектів концептуальних документів у сфері кібербезпеки;

– проведення навчань щодо дій у разі надзвичайних ситуацій та інцидентів у кіберпросторі;

– функціонування системи аудиту інформаційної безпеки, запровадження кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту;

– розвитку мережі команд реагування на комп'ютерні надзвичайні події;

– розвитку та вдосконалення системи технічного і криптографічного захисту інформації;

– забезпечення дотримання вимог законодавства щодо захисту державних інформаційних ресурсів та інформації;

– створення та забезпечення функціонування Національної телекомунікаційної мережі;

– обміну інформацією про інциденти кібербезпеки між суб'єктами забезпечення кібербезпеки у порядку, визначеному законодавством;

– впровадження єдиної (універсальної) системи індикаторів кіберзагроз з урахуванням міжнародних стандартів з питань кібербезпеки та кіберзахисту;

– підготовки фахівців освітньо-кваліфікаційних рівнів бакалавра і магістра за державним замовленням в обсязі, необхідному для задоволення потреб державного сектору економіки, а також за небюджетні кошти, у тому числі для підвищення кваліфікації та проведення обов'язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об'єктів критичної інфраструктури, з урахуванням міжнародних стандартів;

– впровадження організаційно-технічної моделі національної системи кібербезпеки як комплексу заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію вразливості комунікаційних систем;

– встановлення вимог (правил, настанов) щодо безпечного використання мережі Інтернет та надання електронних послуг державними органами;

– державно-приватної взаємодії у запобіганні кіберзагрозам об’єктам критичної інфраструктури, реагуванні на кібератаки та кіберінциденти, усуненні їх наслідків, зокрема в умовах кризових ситуацій, надзвичайного і воєнного стану, в особливий період;

– періодичного проведення огляду національної системи кібербезпеки, розроблення індикаторів стану кібербезпеки;

– стратегічного планування та програмно-цільового забезпечення у сфері розвитку електронних комунікацій, інформаційних технологій, захисту інформації та кіберзахисту;

– розвитку міжнародного співробітництва у сфері кібербезпеки, підтримки міжнародних ініціатив у сфері кібербезпеки, що відповідають національним інтересам України, поглиблення співпраці України з Європейським Союзом та НАТО з метою посилення спроможності України у сфері кібербезпеки, участі у заходах із зміцнення довіри при використанні кіберпростору, що проводяться під егідою Організації з безпеки і співробітництва в Європі;

– здійснення оперативно-розшукових, розвідувальних, контррозвідувальних та інших заходів, спрямованих на запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти миру і безпеки людства, які вчиняються з використанням кіберпростору, розслідування, переслідування, оперативного реагування та протидії кіберзлочинності, розвідувально-підривній, терористичній та іншій діяльності у кіберпросторі, що завдає шкоди інтересам України, використанню мережі Інтернет у воєнних цілях;

– здійснення воєнно-політичних, військово-технічних та інших заходів для розширення можливостей Воєнної організації держави, сектору безпеки і оборони з використанням кіберпростору, створення і розвитку сил, засобів та інструментів можливої відповіді на агресію у кіберпросторі, яка може застосовуватися як засіб стримування воєнних конфліктів та загроз з використанням кіберпростору;

– обмеження участі у заходах із забезпечення інформаційної безпеки та кібербезпеки будь-яких суб’єктів господарювання, які перебувають під контролем держави, визнаної Верховною Радою України державою-агресором, або держав та осіб, стосовно яких діють спеціальні економічні та інші обмежувальні заходи (санкції), прийняті на національному або міжнародному рівні внаслідок агресії щодо України, а також обмеження використання продукції, технологій та послуг таких суб’єктів для забезпечення технічного та криптографічного захисту державних інформаційних ресурсів, посилення державного контролю в цій сфері;

– розвитку системи контррозвідувального забезпечення кібербезпеки, призначеної для запобігання, своєчасного виявлення та протидії зовнішнім і внутрішнім загрозам безпеці України з використанням кіберпростору; усунення умов, що їм сприяють, та причин їх виникнення;

– проведення розвідувальних заходів із виявлення та протидії загрозам національній безпеці України у кіберпросторі, виявлення інших подій і обставин, що стосуються сфери кібербезпеки.

4. Порядок функціонування Національної телекомунікаційної мережі, критерії, правила та вимоги щодо надання послуг, їх тарифікації для користувачів бюджетної сфери, відшкодування витрат державного бюджету на утримання Національної телекомунікаційної мережі затверджуються Кабінетом Міністрів України.

5. Впровадження організаційно-технічної моделі кібербезпеки як складової національної системи кібербезпеки здійснюється Державним центром кіберзахисту, який забезпечує створення та функціонування основних складових системи захищеного доступу державних органів до мережі Інтернет, системи антивірусного захисту національних інформаційних ресурсів, аудиту інформаційної безпеки та стану кіберзахисту об'єктів критичної інформаційної інфраструктури, системи виявлення вразливостей і реагування на кіберінциденти та кібератаки щодо об'єктів кіберзахисту, системи взаємодії команд реагування на комп'ютерні надзвичайні події, а також у взаємодії з іншими суб'єктами забезпечення кібербезпеки розробляє сценарії реагування на кіберзагрози, заходи щодо протидії таким загрозам, програми та методики проведення кібернавчань.

6. Органи державної влади, військові формування, утворені відповідно до законів України, державні підприємства, установи та організації з метою усунення можливих наслідків кіберінцидентів та кібератак створюють резервні копії національних електронних інформаційних ресурсів, що перебувають у їх володінні або розпорядженні та є критичними для їх сталого функціонування, та передають їх на зберігання до Національного центру резервування державних інформаційних ресурсів, крім тих, передача яких обмежена законодавством. Порядок передачі, збереження і доступу до зазначених копій визначається Кабінетом Міністрів України.

Національний центр резервування державних інформаційних ресурсів забезпечує:

– безперервність роботи відповідного національного електронного інформаційного ресурсу, резервного копіювання інформації та відомостей національного електронного інформаційного ресурсу через єдині основний та резервний захищені центри обробки даних (дата-центри), призначені для обробки національних електронних інформаційних ресурсів, резервного копіювання національних електронних інформаційних ресурсів;

– надійне функціонування серверного обладнання, системи зберігання даних, активного мережевого обладнання, архітектурно-технічних рішень щодо резервного копіювання й дублювання інформаційних систем, постійно працюючої інженерної інфраструктури;

– здійснення обов'язкового контролю за статистичними даними роботи з фізичного захисту об'єктів, системи управління та моніторингу інформаційних систем, комплексу організаційних заходів;

– розроблення, створення (побудову), модернізацію, розвиток, впровадження та супроводження програмного забезпечення інформаційної системи (платформи) для побудови та ведення реєстрів;

– переміщення протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування резервних копій національних електронних інформаційних ресурсів до електронних комунікаційних мереж закордонних дипломатичних установ України в порядку, встановленому Кабінетом Міністрів України.

Стаття 9. Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA

1. Завданнями CERT-UA є:

– накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів;

– надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об'єктів;

– організація та проведення практичних семінарів з питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту;

– підготовка та розміщення на своєму офіційному веб-сайті рекомендацій щодо протидії сучасним видам кібератак та кіберзагроз;

– взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки;

– взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамках участі у Форумі команд реагування на інциденти безпеки FIRST із сплатою щорічних членських внесків;

– взаємодія з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору;

– опрацювання отриманої від громадян інформації про кіберінциденти щодо об'єктів кіберзахисту;

– сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам.

2. Забезпечення функціонування CERT-UA здійснює Державна служба спеціального зв'язку та захисту інформації України у межах штатної чисельності та виділених обсягів фінансування.

Стаття 10. Державно-приватна взаємодія у сфері кібербезпеки

1. Державно-приватна взаємодія у сфері кібербезпеки здійснюється шляхом:

– створення системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій;

– підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і вмінь, необхідних для підтримки цілей кібербезпеки, реалізації державних і громадських проектів з підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту;

– обміну інформацією між державними органами, приватним сектором і громадянами щодо кіберзагроз об’єктам критичної інфраструктури, інших кіберзагроз, кібератак та кіберінцидентів;

– партнерства та координації команд реагування на комп’ютерні надзвичайні події;

– залучення експертного потенціалу, наукових установ, професійних об’єднань та громадських організацій до підготовки ключових галузевих проектів та нормативних документів у сфері кібербезпеки;

– надання консультативної та практичної допомоги з питань реагування на кібератаки;

– формування ініціатив та створення авторитетних консультаційних пунктів для громадян, представників промисловості та бізнесу з метою забезпечення безпеки в мережі Інтернет;

– запровадження механізму громадського контролю ефективності заходів із забезпечення кібербезпеки;

– періодичного проведення національного саміту з професійними постачальниками бізнес-послуг, включаючи страховиків, аудиторів, юристів, визначення їхньої ролі у сприянні кращому управлінню ризиками у сфері кібербезпеки;

– створення системи підготовки кадрів та підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки;

– тісної взаємодії з фізичними особами, громадськими та волонтерськими організаціями, ІТ-компаніями з метою виконання заходів кібероборони в кіберпросторі.

2. Державно-приватна взаємодія у сфері кібербезпеки застосовується з урахуванням встановлених законодавством особливостей правового режиму щодо окремих об’єктів та окремих видів діяльності.

Стаття 11. Сприяння суб’єктам забезпечення кібербезпеки України

Державні органи та органи місцевого самоврядування, їх посадові особи, підприємства, установи та організації незалежно від форми власності, особи, громадяни та об’єднання громадян зобов’язані сприяти суб’єктам забезпечення кібербезпеки, повідомляти відомі їм дані щодо загроз національній безпеці з використанням кіберпростору або будь-яких інших кіберзагроз об’єктам кібербезпеки, кібератак та/або обставин, інформація про які може сприяти запобіганню, виявленню і припиненню таких загроз, протидії кіберзлочинам, кібератакам та мінімізації їх наслідків.

Стаття 12. Відповідальність за порушення законодавства у сфері кібербезпеки

Особи, винні у порушенні законодавства у сферах національної безпеки, електронних комунікацій та захисту інформації, якщо кіберпростір є місцем та/або способом здійснення кримінального правопорушення, іншого винного діяння, відповідальність за яке передбачена цивільним, адміністративним, кримінальним законодавством, несуть відповідальність згідно із законом.

Стаття 13. Фінансове забезпечення заходів кібербезпеки

Джерелами фінансування робіт і заходів із забезпечення кібербезпеки та кіберзахисту є кошти державного і місцевих бюджетів, власні кошти суб'єктів господарювання, кредити банків, кошти міжнародної технічної допомоги та інші джерела, не заборонені законодавством.

Стаття 14. Міжнародне співробітництво у сфері кібербезпеки

1. Україна відповідно до укладених нею міжнародних договорів здійснює співробітництво у сфері кібербезпеки з іноземними державами, їх правоохоронними органами і спеціальними службами, а також з міжнародними організаціями, які здійснюють боротьбу з міжнародною кіберзлочинністю.

2. Україна відповідно до міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, може брати участь у спільних заходах із забезпечення кібербезпеки, зокрема у проведенні спільних навчань суб'єктів сектору безпеки і оборони в рамках заходів колективної оборони з дотриманням вимог законів України "Про порядок направлення підрозділів Збройних Сил України до інших держав" та "Про порядок допуску та умови перебування підрозділів збройних сил інших держав на території України".

3. Відповідно до законодавства України у сфері зовнішніх зносин суб'єкти забезпечення кібербезпеки у межах своїх повноважень можуть здійснювати міжнародну співпрацю у сфері кібербезпеки безпосередньо на двосторонній або багатосторонній основі.

4. Інформацію з питань, пов'язаних із боротьбою з міжнародною кіберзлочинністю, Україна надає іноземній державі на підставі запиту, додержуючись вимог законодавства України та її міжнародно-правових зобов'язань. Така інформація може бути надана без попереднього запиту іноземної держави, якщо це не перешкоджає проведенню досудового розслідування чи судового розгляду справи і може сприяти компетентним органам іноземної держави у припиненні кібератаки, своєчасному виявленні і припиненні кримінального правопорушення з використанням кіберпростору.

Стаття 15. Контроль за законністю заходів із забезпечення кібербезпеки України

1. Контроль за дотриманням законодавства при здійсненні заходів із забезпечення кібербезпеки здійснюється Верховною Радою України в порядку, визначеному Конституцією України.

Парламентський контроль за дотриманням законодавства про захист персональних даних та доступ до публічної інформації у сфері кібербезпеки здійснюється Уповноваженим Верховної Ради України з прав людини.

2. Контроль за діяльністю із забезпечення кібербезпеки суб'єктів сектору безпеки і оборони, інших державних органів здійснюється Президентом України та Кабінетом Міністрів України в порядку, визначеному Конституцією і законами України.

3. Незалежний аудит діяльності основних суб'єктів національної кібербезпеки, визначених частиною другою статті 8 цього Закону, щодо ефективності системи забезпечення кібербезпеки держави проводиться щороку згідно з міжнародними стандартами аудиту.

Звіти про результати проведення незалежного аудиту діяльності основних суб'єктів національної кібербезпеки, визначених частиною другою статті 8 цього Закону, щодо ефективності системи забезпечення кібербезпеки держави за попередній рік подаються Президентові України, Верховній Раді України та Кабінету Міністрів України у сорокап'ятиденний строк після закінчення календарного року.

Комітет Верховної Ради України, до предмета відання якого належать питання національної безпеки і оборони, та Комітет Верховної Ради України, до предмета відання якого належать питання інформатизації та зв'язку, на своїх засіданнях розглядають звіти основних суб'єктів національної кібербезпеки, визначених частиною другою статті 8 цього Закону, про результати незалежного аудиту їхньої діяльності щодо ефективності системи забезпечення кібербезпеки держави.

Основні суб'єкти національної кібербезпеки, визначені частиною другою статті 8 цього Закону, подають один раз на рік звіти про стан виконання ними заходів з питань забезпечення кібербезпеки держави, віднесених до їх компетенції, які мають містити, зокрема, інформацію про результати проведення незалежного аудиту їхньої діяльності.

За результатами розгляду звітів основних суб'єктів національної кібербезпеки Комітет Верховної Ради України, до предмета відання якого належать питання інформатизації та зв'язку, може порушити питання про розгляд цих питань Верховною Радою України.

А.5. Закон України «Про державну таємницю»

Цей Закон регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України, та складається з наступних розділів і статей.

Розділ I. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення термінів

Стаття 2. Законодавство України про державну таємницю

Стаття 3. Сфера дії Закону

Стаття 4. Державна політика щодо державної таємниці

Стаття 5. Компетенція державних органів, органів місцевого самоврядування та їх посадових осіб у сфері охорони державної таємниці

Стаття 6. Реалізація прав на секретну інформацію та її матеріальні носії

Стаття 7. Фінансування витрат на здійснення діяльності, пов'язаної з державною таємницею

Розділ II. ВІДНЕСЕННЯ ІНФОРМАЦІЇ ДО ДЕРЖАВНОЇ ТАЄМНИЦІ

Стаття 8. Інформація, що може бути віднесена до державної таємниці

Стаття 9. Державні експерти з питань таємниць

Стаття 10. Порядок віднесення інформації до державної таємниці

Стаття 11. Рішення державного експерта з питань таємниць

Стаття 12. Звід відомостей, що становлять державну таємницю

Стаття 13. Строк дії рішення про віднесення інформації до державної таємниці

Стаття 14. Зміна ступеня секретності інформації та скасування рішення про віднесення її до державної таємниці

Розділ III. ЗАСЕКРЕЧУВАННЯ ТА РОЗСЕКРЕЧУВАННЯ МАТЕРІАЛЬНИХ НОСІЇВ ІНФОРМАЦІЇ

Стаття 15. Засекречування та розсекречування матеріальних носіїв інформації

Стаття 16. Строк засекречування матеріальних носіїв інформації

Стаття 17. Оскарження рішення щодо засекречування матеріальних носіїв інформації

Розділ IV. ОХОРОНА ДЕРЖАВНОЇ ТАЄМНИЦІ

Стаття 18. Основні організаційно-правові заходи щодо охорони державної таємниці

Стаття 19. Єдині вимоги до матеріальних носіїв секретної інформації

Стаття 20. Дозвільний порядок провадження діяльності, пов'язаної з державною таємницею, та режим секретності

Стаття 21. Режимно-секретні органи

Стаття 22. Допуск громадян до державної таємниці

Стаття 23. Відмова у наданні допуску до державної таємниці

Стаття 24. Перевірка громадян у зв'язку з допуском їх до державної таємниці

Стаття 25. Оскарження громадянином відмови у наданні допуску до державної таємниці
Стаття 26. Переоформлення допуску до державної таємниці, підвищення або зниження його форми та скасування
Стаття 27. Доступ громадян до державної таємниці
Стаття 28. Обов'язки громадянина щодо збереження державної таємниці
Стаття 29. Обмеження прав у зв'язку з допуском та доступом до державної таємниці
Стаття 30. Компенсація громадянам у зв'язку з виконанням робіт, які передбачають доступ до державної таємниці
Стаття 30. Компенсація громадянам у зв'язку з виконанням робіт, які передбачають доступ до державної таємниці
Стаття 32. Обмеження щодо передачі державної таємниці іноземній державі чи міжнародній організації
Стаття 33. Обмеження, пов'язані з державною таємницею, щодо перебування і діяльності в Україні іноземців, осіб без громадянства та іноземних юридичних осіб, а також розташування та переміщення об'єктів і технічних засобів, що їм належать
Стаття 34. Особливості здійснення державними органами їх функцій щодо державних органів, органів місцевого самоврядування, підприємств, установ і організацій, що провадять діяльність, пов'язану з державною таємницею
Стаття 35. Технічний та криптографічний захисти секретної інформації
Стаття 36. Оперативно-розшукові заходи щодо охорони державної таємниці
Розділ V. КОНТРОЛЬ ЗА ЗАБЕЗПЕЧЕННЯМ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ТА НАГЛЯД ЗА ДОДЕРЖАННЯМ ЗАКОНОДАВСТВА ПРО ДЕРЖАВНУ ТАЄМНИЦЮ
Стаття 37. Контроль за забезпеченням охорони державної таємниці
Стаття 38. Нагляд за додержанням законодавства про державну таємницю
Розділ VI. ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА ПРО ДЕРЖАВНУ ТАЄМНИЦЮ
Стаття 39. Відповідальність за порушення законодавства про державну таємницю

Розділ I. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення термінів

У цьому Законі терміни вживаються у такому значенні:

– державна таємниця (далі також – секретна інформація) – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою;

– віднесення інформації до державної таємниці – процедура прийняття (державним експертом з питань таємниць) рішення про віднесення категорії відомостей або окремих відомостей до державної таємниці з установленням ступеня їх секретності шляхом обгрунтування та визначення можливої шкоди національній безпеці України у разі розголошення цих відомостей, включенням цієї інформації до Зводу відомостей, що становлять державну таємницю, та з опублікуванням цього Зводу, змін до нього;

– гриф секретності – реквізит матеріального носія секретної інформації, що засвідчує ступінь секретності даної інформації;

– державний експерт з питань таємниць – посадова особа, уповноважена здійснювати відповідно до вимог цього Закону віднесення інформації до державної таємниці у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, зміни ступеня секретності цієї інформації та її розсекречування;

– допуск до державної таємниці – оформлення права громадянина на доступ до секретної інформації;

– доступ до державної таємниці – надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, або ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, цією посадовою особою відповідно до її службових повноважень;

– засекречування матеріальних носіїв інформації – введення у встановленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом надання відповідного грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації;

– Звід відомостей, що становлять державну таємницю, – акт, в якому зведено переліки відомостей, що згідно з рішеннями державних експертів з питань таємниць становлять державну таємницю у визначених цим Законом сферах;

– категорія режиму секретності – категорія, яка характеризує важливість та обсяги відомостей, що становлять державну таємницю, які зосереджені в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях;

– криптографічний захист секретної інформації – вид захисту, що реалізується шляхом перетворення інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

– матеріальні носії секретної інформації – матеріальні об'єкти, в тому числі фізичні поля, в яких відомості, що становлять державну таємницю, відображені у вигляді текстів, знаків, символів, образів, сигналів, технічних рішень, процесів тощо;

– охорона державної таємниці – комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів,

спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв;

– режим секретності – встановлений згідно з вимогами цього Закону та інших виданих відповідно до нього нормативно-правових актів єдиний порядок забезпечення охорони державної таємниці;

– розсекречування матеріальних носіїв секретної інформації – зняття в установленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом скасування раніше наданого грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації;

– спеціальна експертиза щодо наявності умов для провадження діяльності, пов'язаної з державною таємницею, – експертиза, що проводиться з метою визначення в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях наявності умов, передбачених цим Законом, для провадження діяльності, пов'язаної з державною таємницею;

– ступінь секретності ("особливої важливості", "цілком таємно", "таємно") – категорія, яка характеризує важливість секретної інформації, ступінь обмеження доступу до неї та рівень її охорони державою;

– технічний захист секретної інформації – вид захисту, спрямований на забезпечення інженерно-технічними заходами конфіденційності, цілісності та унеможливлення блокування інформації.

Стаття 2. Законодавство України про державну таємницю

Відносини у сфері охорони державної таємниці регулюються Конституцією України, законами України "Про інформацію" та "Про доступ до публічної інформації", цим Законом, міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України та іншими нормативно-правовими актами.

Стаття 3. Сфера дії Закону

Дія цього Закону поширюється на органи законодавчої, виконавчої та судової влади, органи прокуратури України, інші державні органи, в тому числі територіальні органи центрального органу виконавчої влади, що реалізує державну митну політику, та центрального органу виконавчої влади, що реалізує державну податкову політику, утворені як відокремлені підрозділи центрального органу виконавчої влади без статусу юридичної особи, Верховну Раду Автономної Республіки Крим, Раду міністрів Автономної Республіки Крим, органи місцевого самоврядування, підприємства, установи та організації усіх форм власності, об'єднання громадян (далі – державні органи, органи місцевого самоврядування, підприємства, установи та організації), що провадять діяльність, пов'язану з державною таємницею, громадян України, іноземців та осіб без громадянства, яким у встановленому порядку наданий доступ до державної таємниці.

Передані Україні відомості, що становлять таємницю іноземної держави чи міжнародної організації, охороняються в порядку, передбаченому цим Законом. У разі, якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, установлено інші, ніж передбачені цим

Законом, правила охорони таємниці іноземної держави чи міжнародної організації, то застосовуються правила міжнародного договору України.

Стаття 4. Державна політика щодо державної таємниці

Державну політику щодо державної таємниці як складову засад внутрішньої та зовнішньої політики визначає Верховна Рада України.

Стаття 5. Компетенція державних органів, органів місцевого самоврядування та їх посадових осіб у сфері охорони державної таємниці

Президент України, забезпечуючи національну безпеку, видає укази та розпорядження з питань охорони державної таємниці, віднесених цим Законом та іншими законами до його повноважень.

Рада національної безпеки і оборони України координує та контролює діяльність органів виконавчої влади у сфері охорони державної таємниці.

Кабінет Міністрів України спрямовує та координує роботу міністерств, інших органів виконавчої влади щодо забезпечення здійснення державної політики у сфері охорони державної таємниці.

Центральні та місцеві органи виконавчої влади, Рада міністрів Автономної Республіки Крим та органи місцевого самоврядування здійснюють державну політику у сфері охорони державної таємниці в межах своїх повноважень, передбачених законом.

Спеціально уповноваженим державним органом у сфері забезпечення охорони державної таємниці є Служба безпеки України.

Забезпечення охорони державної таємниці відповідно до вимог режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, діяльність яких пов'язана з державною таємницею, покладається на керівників зазначених органів, підприємств, установ і організацій.

Стаття 6. Реалізація прав на секретну інформацію та її матеріальні носії

Володілець секретної інформації або власник матеріальних носіїв такої інформації реалізує свої права з урахуванням обмежень, установлених в інтересах національної безпеки України відповідно до цього Закону.

Якщо внаслідок обмеження прав на секретну інформацію або її матеріальні носії заподіюється шкода особі, якій належать такі права, відшкодування здійснюється за рахунок держави в порядку та розмірах, що визначаються в договорі між такою особою і державним органом (органами), якому (яким) державним експертом з питань таємниць надається право приймати рішення щодо суб’єктів, які мають доступ до цієї інформації та її матеріальних носіїв. Зазначеним договором також визначаються порядок та умови охорони державної таємниці, зокрема режим секретності під час користування і розпорядження секретною інформацією та її матеріальними носіями, обумовлюється згода особи на реалізацію прав щодо інформації або її матеріальних носіїв з урахуванням обмежень, установлених відповідно до цього Закону, взяття особою на себе зобов’язання щодо збереження державної таємниці та ознайомлення її з мірою відповідальності за порушення законодавства про державну таємницю.

Якщо особа, якій належать права на секретну інформацію або її матеріальні носії, відмовляється від укладення договору чи порушує його, за рішенням суду ця інформація або її матеріальні носії можуть бути вилучені за умови попереднього і повного відшкодування їх вартості особі, якій належали відповідні права.

Стаття 7. Фінансування витрат на здійснення діяльності, пов'язаної з державною таємницею

Фінансування витрат на здійснення діяльності, пов'язаної з державною таємницею, в бюджетних установах і організаціях здійснюється за рахунок Державного бюджету України, бюджету Автономної Республіки Крим та місцевих бюджетів. Кошти на зазначені витрати передбачаються у відповідних бюджетах окремим рядком. Зазначені витрати інших установ і організацій, а також підприємств відносяться до валових витрат виробника продукції, виготовлення якої пов'язано з державною таємницею.

Витрати на здійснення заходів щодо віднесення інформації до державної таємниці, засекречування, розсекречування та охорони матеріальних носіїв такої інформації, її криптографічного та технічного захисту, інші витрати, пов'язані з державною таємницею, на недержавних підприємствах, в установах, організаціях фінансуються на підставі договору з замовником робіт, пов'язаних з державною таємницею.

Підприємствам, установам і організаціям, які провадять діяльність, пов'язану з державною таємницею, можуть надаватися податкові та інші пільги в порядку, встановленому законом.

Розділ II. ВІДНЕСЕННЯ ІНФОРМАЦІЇ ДО ДЕРЖАВНОЇ ТАЄМНИЦІ

Стаття 8. Інформація, що може бути віднесена до державної таємниці

До державної таємниці у порядку, встановленому цим Законом, відноситься інформація:

1) у сфері оборони:

– про зміст стратегічних і оперативних планів та інших документів бойового управління, підготовку та проведення військових операцій, стратегічне та мобілізаційне розгортання військ, а також про інші найважливіші показники, які характеризують організацію, чисельність, дислокацію, бойову і мобілізаційну готовність, бойову та іншу військову підготовку, озброєння та матеріально-технічне забезпечення Збройних Сил України та інших військових формувань;

– про дислокацію, характеристики пунктів управління, зміст заходів загальнодержавного та регіонального, у разі необхідності міського і районного рівня, щодо приведення у готовність єдиної державної системи цивільного захисту населення і територій до виконання завдань в особливий період та про організацію системи зв'язку (оповіщення) в особливий період, можливості населених пунктів, регіонів і окремих об'єктів щодо евакуації, розосередження населення і забезпечення його життєдіяльності; забезпечення виробничої діяльності об'єктів національної економіки у воєнний час;

– про геодезичні, гравіметричні, картографічні та гідрометеорологічні дані і характеристики, які мають значення для оборони країни;

– про застосування систем озброєння, підготовку та проведення військових операцій;

– про винаходи, дослідження і розробку нових зразків озброєння в інтересах забезпечення національної безпеки і оборони та про результати таких досліджень і розробок;

– про заходи та показники розвитку Збройних Сил України та їх спроможностей;

– про склад, завдання та матеріально-технічне забезпечення розвідувального органу Міністерства оборони України та зібрану і створену ним інформацію в результаті його діяльності;

– про особовий склад Сил спеціальних операцій Збройних Сил України, а також осіб, які співпрацюють або раніше співпрацювали на конфіденційній основі із Силами спеціальних операцій Збройних Сил України, фінансування та матеріально-технічне забезпечення руху опору, засоби, зміст, плани, організацію, завдання, форми, методи і результати ведення руху опору, оперативний резерв та мережу осередків руху опору;

2) у сфері економіки, науки і техніки:

– про зміст мобілізаційних планів державних органів та органів місцевого самоврядування, мобілізаційні потужності, заходи мобілізаційної підготовки і мобілізації та обсяги їх фінансування, запаси та обсяги постачання стратегічних видів сировини і матеріалів, а також зведені відомості про номенклатуру та рівні накопичення, загальні обсяги поставок, відпуску, закладення, освіження, розміщення і фактичні запаси державного матеріального резерву;

– про використання транспорту, зв'язку, потужностей інших галузей та об'єктів інфраструктури держави в інтересах забезпечення її безпеки;

– про плани, обсяги та інші найважливіші характеристики добування, виробництва та реалізації окремих стратегічних видів сировини і продукції;

– про державні запаси дорогоцінних металів монетарної групи, коштовного каміння, валюти та інших цінностей, операції, пов'язані з виготовленням грошових знаків і цінних паперів, їх зберіганням, охороною і захистом від підроблення, обігом, обміном або вилученням з обігу, а також про інші особливі заходи фінансової діяльності держави;

– про наукові, науково-дослідні, дослідно-конструкторські та проектні роботи, предметом яких є створення новітніх складних зразків озброєння, військової або спеціальної техніки та інші роботи, що мають важливе оборонне чи економічне значення або суттєво впливають на зовнішньоекономічну діяльність та національну безпеку України;

– про найменування, загальну кількість, вартість озброєння, військової техніки, боєприпасів, запасних частин та матеріалів до них, що закуповуються для потреб військових формувань (правоохоронних органів);

– про кількість, строки поставок військовим формуванням чи правоохоронним органам, спеціальним формуванням Міністерства внутрішніх справ України для забезпечення їх боєздатності основних видів пального (мастильних матеріалів), речового майна та продовольства;

– про факт та предмет закупівлі товарів, робіт і послуг оборонного призначення для забезпечення Збройних Сил України та інших військових формувань та правоохоронних органів (крім випадків, якщо окрема інформація про закупівлю таких товарів, робіт і послуг оборонного призначення, що закуповуються відповідно до Закону України "Про оборонні закупівлі", становить державну таємницю. У такому разі окрема інформація розміщується у додатку до тендерної документації).

– Інформація не може бути повторно віднесена до державної таємниці після розсекречення та оприлюднення;

3) у сфері зовнішніх відносин:

– про директиви, плани, вказівки делегаціям і посадовим особам з питань зовнішньополітичної і зовнішньоекономічної діяльності України, спрямовані на забезпечення її національних інтересів і безпеки;

– про військове, науково-технічне та інше співробітництво України з іноземними державами, якщо розголошення відомостей про це завдаватиме шкоди національній безпеці України;

– про експорт та імпорт озброєння, військової і спеціальної техніки, окремих стратегічних видів сировини і продукції;

– про зміст секретної інформації, що отримується від іноземної держави чи міжнародної організації;

4) у сфері державної безпеки та охорони правопорядку:

– про особовий склад органів, що здійснюють оперативно-розшукову діяльність або розвідувальну чи контррозвідувальну;

– про засоби, зміст, плани, організацію, фінансування та матеріально-технічне забезпечення, форми, методи і результати оперативно-розшукової, розвідувальної і контррозвідувальної діяльності; про осіб, які співпрацюють або раніше співпрацювали на конфіденційній основі з органами, що проводять таку діяльність; про склад і конкретних осіб, що є негласними штатними працівниками органів, які здійснюють оперативно-розшукову, розвідувальну і контррозвідувальну діяльність;

– про організацію та порядок здійснення охорони адміністративних будинків та інших державних об'єктів, посадових та інших осіб, охорона яких здійснюється відповідно до Закону України "Про державну охорону органів державної влади України та посадових осіб";

– про систему урядового та спеціального зв'язку;

– про організацію, зміст, стан і плани розвитку криптографічного захисту секретної інформації, зміст і результати наукових досліджень у сфері криптографії;

– про системи та засоби криптографічного захисту секретної інформації, їх розроблення, виробництво, технологію виготовлення та використання;

– про державні шифри, їх розроблення, виробництво, технологію виготовлення та використання;

– про організацію режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, державні програми, плани та інші заходи у сфері охорони державної таємниці;

– про організацію, зміст, стан і плани розвитку технічного захисту секретної інформації;

– про результати перевірок, здійснюваних згідно з законом прокурором у порядку відповідного нагляду за додержанням законів, та про зміст матеріалів оперативно-розшукової діяльності, досудового розслідування та судочинства з питань, зазначених у цій статті сфер;

– про інші засоби, форми і методи охорони державної таємниці.

Конкретні відомості можуть бути віднесені до державної таємниці за ступенями секретності "особливої важливості", "цілком таємно" та "таємно" лише за умови, що вони належать до категорій, зазначених у частині першій цієї статті, і їх розголошення завдаватиме шкоди інтересам національної безпеки України та з дотриманням вимог статті 6 Закону України "Про доступ до публічної інформації".

Забороняється віднесення до державної таємниці будь-яких відомостей, якщо цим будуть звужуватися зміст і обсяг конституційних прав та свобод людини і громадянина, завдаватиметься шкода здоров'ю та безпеці населення.

Не відноситься до державної таємниці інформація:

– про стан довкілля, про якість харчових продуктів і предметів побуту, про вплив товару (роботи, послуги) на життя та здоров’я людини;

– про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, які сталися або можуть статися і загрожують безпеці громадян;

– про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;

– про факти порушень прав і свобод людини і громадянина;

– про незаконні дії державних органів, органів місцевого самоврядування та їх посадових і службових осіб;

– інша інформація, доступ до якої відповідно до законів та міжнародних договорів, згода на обов’язковість яких надана Верховною Радою України, не може бути обмежено.

Стаття 9. Державні експерти з питань таємниць

Державний експерт з питань таємниць здійснює відповідно до вимог цього Закону віднесення інформації у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку до державної таємниці, зміни ступеня секретності цієї інформації та її розсекречування.

Виконання функцій державного експерта з питань таємниць на конкретних посадових осіб покладається:

– у Верховній Раді України – Головою Верховної Ради України;

– в інших державних органах, Національній академії наук України, на підприємствах, в установах і організаціях – Президентом України за поданням Служби безпеки України на підставі пропозицій керівників відповідних державних органів, Національної академії наук України, підприємств, установ і організацій.

Втручання в діяльність державного експерта з питань таємниць особи, якій за посадою його підпорядковано, не допускається.

Державний експерт з питань таємниць відповідно до покладених на нього завдань:

1) визначає:

– підстави, за якими інформацію має бути віднесено до державної таємниці;

– підстави та доцільність віднесення до державної таємниці інформації про винаходи (корисні моделі), призначені для використання у сферах, зазначених у частині першій статті 8 цього Закону;

– доцільність віднесення до державної таємниці інформації про винаходи (корисні моделі), що мають подвійне застосування, на підставі порівняльного аналізу ефективності цільового використання та за згодою автора (власника патенту);

– ступінь секретності інформації, віднесеної до державної таємниці;

– державний орган (органи), якому надається право приймати рішення щодо кола суб'єктів, які матимуть доступ до секретної інформації;

2) готує висновок щодо завданої національній безпеці України шкоди у разі розголошення секретної інформації чи втрати матеріальних носіїв такої інформації;

3) установлює та продовжує строк дії рішення про віднесення інформації до державної таємниці із зазначенням дати її розсекречення;

4) дає Службі безпеки України рішення про зміну ступеня секретності інформації та скасування рішення про віднесення її до державної таємниці у разі, якщо підстави, на яких цю інформацію було віднесено до державної таємниці, перестали існувати;

5) затверджує за погодженням із Службою безпеки України розгорнуті переліки відомостей, що становлять державну таємницю, зміни до них, контролює відповідність змісту цих переліків Зводу відомостей, що становлять державну таємницю;

6) розглядає пропозиції державних органів, органів місцевого самоврядування, підприємств, установ, організацій, об'єднань громадян та окремих громадян щодо віднесення інформації до державної таємниці та її розсекречування;

7) затверджує висновки щодо обізнаності з державною таємницею громадян, які мають чи мали допуск до державної таємниці;

8) контролює обгрунтованість і правильність надання документам, виробам та іншим матеріальним носіям інформації, які містять відомості, включені до Зводу відомостей чи розгорнутих переліків відомостей, що становлять державну таємницю, відповідного грифа секретності, своєчасність зміни такого грифа та розсекречування цих носіїв із наданням їм реквізиту "розсекречено";

9) бере участь у розробленні критеріїв визначення шкоди, яку може бути завдано національній безпеці України у разі розголошення секретної інформації чи втрати матеріальних носіїв такої інформації.

Державний експерт з питань таємниць під час виконання покладених на нього функцій зобов'язаний:

1) погоджувати за посередництвом Служби безпеки України свої висновки про скасування рішень щодо віднесення інформації до міждержавних таємниць з відповідними посадовими особами держав – учасниць міжнародних договорів України про взаємне забезпечення збереження міждержавних таємниць та повідомляти їх про прийняті рішення щодо віднесення інформації до державної таємниці, на яку поширено чинність цих договорів;

2) подавати Службі безпеки України не пізніш як через десять днів з моменту підписання рішення про віднесення відомостей до державної таємниці або про скасування цих рішень, а розгорнуті переліки відомостей, що становлять державну таємницю, – у той же строк з моменту їх затвердження;

3) розглядати протягом одного місяця пропозиції Служби безпеки України про віднесення інформації до державної таємниці, скасування чи продовження терміну дії раніше прийнятого рішення про віднесення інформації до державної таємниці;

4) надавати відповідний гриф секретності рішенням про віднесення інформації до державної таємниці та про скасування цих рішень залежно від важливості їх змісту;

5) брати участь у засіданнях державних експертів з питань таємниць;

6) ініціювати питання щодо притягнення до відповідальності посадових осіб, які порушують законодавство України про державну таємницю.

Державний експерт з питань таємниць має право:

1) безперешкодно проводити перевірку виконання державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями, що перебувають у сфері його діяльності, рішень про віднесення інформації до державної таємниці, скасування цих рішень, додержання порядку засекречення інформації та у разі виявлення порушень давати обов'язкові для виконання приписи про їх усунення;

2) створювати експертні комісії з фахівців і науковців, які мають допуск до державної таємниці, для підготовки проектів рішень про віднесення інформації до державної таємниці, зниження ступеня її секретності та скасування зазначених рішень, висновків щодо обізнаності з державною таємницею громадян, які мають чи мали допуск до державної таємниці, а також для підготовки відповідних висновків у разі розголошення секретної інформації чи втрати матеріальних носіїв такої інформації;

3) скасовувати безпідставні рішення про надання носію інформації грифа секретності, зміну або скасування цього грифа;

4) клопотати про притягнення до відповідальності посадових осіб, які порушують законодавство України про державну таємницю;

5) одержувати в установленому порядку від державних органів, органів місцевого самоврядування, підприємств, установ та організацій відомості, необхідні для виконання своїх функцій.

Державним експертам з питань таємниць, а також фахівцям, які залучаються до підготовки рішень та висновків державних експертів з питань

таємниць, встановлюються додаткові виплати у порядку і розмірах, що визначаються Кабінетом Міністрів України.

Державний експерт з питань таємниць несе персональну відповідальність за законність і обґрунтованість свого рішення про віднесення інформації до державної таємниці або про зниження ступеня секретності такої інформації чи скасування рішення про віднесення її до державної таємниці, а також за умисне неприйняття рішення про віднесення до державної таємниці інформації, розголошення якої може завдати шкоди інтересам національної безпеки України.

Стаття 10. Порядок віднесення інформації до державної таємниці

Віднесення інформації до державної таємниці здійснюється мотивованим рішенням державного експерта з питань таємниць за його власною ініціативою, за зверненням керівників відповідних державних органів, органів місцевого самоврядування, підприємств, установ, організацій чи громадян.

Державний експерт з питань таємниць відносить інформацію до державної таємниці з питань, прийняття рішень з яких належить до його компетенції згідно з посадою. У разі, якщо прийняття рішення про віднесення інформації до державної таємниці належить до компетенції кількох державних експертів з питань таємниць, воно за ініціативою державних експертів або за пропозицією Служби безпеки України приймається колегіально та ухвалюється простою більшістю голосів. При цьому кожен експерт має право викласти свою думку.

Інформація вважається державною таємницею з часу опублікування Зводу відомостей, що становлять державну таємницю, до якого включена ця інформація, чи зміни до нього у порядку, встановленому цим Законом.

Інформація відноситься до державної таємниці з урахуванням таких принципів:

– дотримання балансу інтересів національної безпеки, демократичних принципів відкритості та прозорості;

– вільного обігу інформації;

– презумпції публічності інформації до її віднесення в установленому законодавством порядку до державної таємниці.

У разі невідповідності інформації вимогам, встановленим цим Законом, забороняється віднесення її до державної таємниці. Засекречуванню підлягає інформація, а не документ. Якщо документ містить державну таємницю, для ознайомлення надається інформація, доступ до якої не обмежений.

Стаття 11. Рішення державного експерта з питань таємниць

У рішенні державного експерта з питань таємниць про віднесення інформації до державної таємниці зазначаються:

– інформація, яка має становити державну таємницю, та її відповідність категоріям і вимогам, передбаченим статтею 8 цього Закону та статтею 6 Закону України "Про доступ до публічної інформації";

– підстави для віднесення інформації до державної таємниці;

– критерії віднесення інформації до державної таємниці, зокрема:

– визначення рівня та опис загрози та шкоди національній безпеці (національним інтересам) у разі невіднесення інформації до державної таємниці;

– визначення дати або події розсекречування інформації;

– ступінь секретності зазначеної інформації;

– обсяг фінансування заходів, необхідних для охорони такої інформації;

– державний орган, орган місцевого самоврядування, підприємство, установа, організація чи громадянин, який вніс пропозицію про віднесення цієї інформації до державної таємниці, та державний орган (органи), якому надається право визначати коло суб'єктів, які матимуть доступ до цієї інформації;

– строк, протягом якого діє рішення про віднесення інформації до державної таємниці.

Рішення про віднесення інформації до державної таємниці, продовження строку дії раніше прийнятого рішення про віднесення інформації до державної таємниці, зміну ступеня секретності інформації, скасування раніше прийнятого рішення про віднесення інформації до державної таємниці приймаються державним експертом з питань таємниць протягом одного місяця з часу надходження звернення державного органу, органу місцевого самоврядування, підприємства, установи, організації чи громадянина. Такі рішення підлягають реєстрації Службою безпеки України та є підставою для формування Зводу відомостей, що становлять державну таємницю, і внесення змін до зазначеного Зводу, до галузевих або відомчих розгорнутих переліків відомостей, що становлять державну таємницю. Порядок реєстрації рішень державних експертів з питань таємниць визначається Кабінетом Міністрів України.

Стаття 12. Звід відомостей, що становлять державну таємницю

Звід відомостей, що становлять державну таємницю, формує Служба безпеки України на підставі рішень державних експертів з питань таємниць. Зазначений Звід та зміни до нього набирають чинності з моменту опублікування в офіційних виданнях України.

Зміни до Зводу відомостей, що становлять державну таємницю, вносяться не пізніше трьох місяців з дня одержання Службою безпеки України відповідного рішення державного експерта з питань таємниць.

Зразки форм рішень державних експертів з питань таємниць, порядок та механізм формування Зводу відомостей, що становлять державну таємницю, і його опублікування визначаються Кабінетом Міністрів України.

На підставі та в межах Зводу відомостей, що становлять державну таємницю, з метою конкретизації та систематизації даних про секретну інформацію державні органи створюють галузеві або відомчі розгорнуті переліки відомостей, що становлять державну таємницю, а також можуть створювати міжгалузеві або міжвідомчі розгорнуті переліки відомостей, що становлять державну таємницю. Підприємства, установи та організації незалежно від форм власності, що провадять діяльність, пов'язану із державною таємницею, за ініціативою та погодженням із замовником робіт, пов'язаних з державною таємницею, можуть створювати власні розгорнуті переліки відомостей, що становлять державну таємницю. Такі переліки погоджуються із Службою безпеки України, затверджуються державними експертами з питань таємниць та реєструються у Службі безпеки України.

Розгорнуті переліки відомостей, що становлять державну таємницю, не можуть суперечити Зводу відомостей, що становлять державну таємницю.

У разі включення до Зводу відомостей, що становлять державну таємницю, або до розгорнутих переліків цих відомостей інформації, яка не відповідає категоріям і вимогам, передбаченим статтею 8 цього Закону, або порушення встановленого порядку віднесення інформації до державної таємниці заінтересовані громадяни та юридичні особи мають право оскаржити відповідні рішення до суду. З метою недопущення розголошення державної таємниці судовий розгляд скарг може проводитися в закритих засіданнях відповідно до закону.

Стаття 13. Строк дії рішення про віднесення інформації до державної таємниці

Строк, протягом якого діє рішення про віднесення інформації до державної таємниці, встановлюється державним експертом з питань таємниць з урахуванням ступеня секретності інформації, критерії визначення якого встановлюються Службою безпеки України, та інших обставин. Він не може перевищувати для інформації із ступенем секретності "особливої важливості" – 30 років, для інформації "цілком таємно" – 10 років, для інформації "таємно" – 5 років.

Після закінчення передбаченого частиною першою цієї статті строку дії рішення про віднесення інформації до державної таємниці державний експерт з питань таємниць приймає рішення про скасування рішення про віднесення її до державної таємниці або приймає рішення про продовження строку дії зазначеного рішення в межах строків, встановлених частиною першою цієї статті.

Президент України з власної ініціативи або на підставі пропозицій державних експертів з питань таємниць чи за зверненням державних органів, органів місцевого самоврядування, підприємств, установ, організацій чи громадян може встановлювати більш тривалі строки дії рішень про віднесення інформації до державної таємниці, ніж строки, передбачені частиною першою цієї статті.

Установлення строку дії рішення про віднесення інформації до державної таємниці, прийняття рішення про його продовження здійснюються з дотриманням вимог статті 6 Закону України "Про доступ до публічної інформації".

Стаття 14. Зміна ступеня секретності інформації та скасування рішення про віднесення її до державної таємниці

Підвищення або зниження ступеня секретності інформації та скасування рішення про віднесення її до державної таємниці здійснюються на підставі рішення державного експерта з питань таємниць або на підставі рішення суду у випадках, передбачених статтею 12 цього Закону, та оформляються Службою безпеки України шляхом внесення відповідних змін до Зводу відомостей, що становлять державну таємницю.

Інформація вважається державною таємницею з більш високим чи нижчим ступенем секретності або такою, що не становить державної таємниці, з часу

опублікування відповідних змін до Зводу відомостей, що становлять державну таємницю.

Розділ ІІІ. ЗАСЕКРЕЧУВАННЯ ТА РОЗСЕКРЕЧУВАННЯ МАТЕРІАЛЬНИХ НОСІЇВ ІНФОРМАЦІЇ

Стаття 15. Засекречування та розсекречування матеріальних носіїв інформації

Засекречування матеріальних носіїв інформації здійснюється шляхом надання на підставі Зводу відомостей, що становлять державну таємницю (розгорнутих переліків відомостей, що становлять державну таємницю), відповідному документу, виробу або іншому матеріальному носію інформації грифа секретності посадовою особою, яка готує або створює документ, виріб або інший матеріальний носій інформації. Засекречування документів здійснюється лише в частині відомостей, що становлять державну таємницю. У разі подання запиту на документ, частина якого засекречена, доступ до такого документа забезпечується в частині, що не засекречена.

Гриф секретності кожного матеріального носія секретної інформації повинен відповідати ступеню секретності інформації, яка у ньому міститься, згідно із Зводом відомостей, що становлять державну таємницю, – "особливої важливості", "цілком таємно" або "таємно". Реквізити кожного матеріального носія секретної інформації складаються із:

– грифа секретності;

– номера примірника;

– статті Зводу відомостей, що становлять державну таємницю, на підставі якої здійснюється засекречення;

– найменування посади та підпису особи, яка надала гриф секретності.

Якщо реквізити, зазначені у частині другій цієї статті, неможливо нанести безпосередньо на матеріальний носій секретної інформації, вони мають бути зазначені у супровідних документах.

Забороняється надавати грифи секретності, передбачені цим Законом, матеріальним носіям іншої таємної інформації, яка не становить державної таємниці, або конфіденційної інформації.

Перелік посад, перебування на яких дає посадовим особам право надавати матеріальним носіям секретної інформації грифи секретності, затверджується керівником державного органу, органу місцевого самоврядування, підприємства, установи, організації, що провадить діяльність, пов'язану з державною таємницею.

Ступені секретності науково-дослідних, дослідно-конструкторських і проектних робіт та інших секретних товарів, робіт і послуг, щодо яких здійснюється закупівля та які виконуються в інтересах забезпечення національної безпеки та оборони держави, встановлюються шляхом винесення відповідного висновку державним експертом з питань таємниць, який виконує свої функції у сфері діяльності замовника, разом з підрядником.

Після закінчення встановлених строків засекречування матеріальних носіїв інформації та у разі підвищення чи зниження визначеного державним експертом з питань таємниць ступеня секретності такої інформації або

скасування рішення про віднесення її до державної таємниці керівники державних органів, органів місцевого самоврядування, підприємств, установ, організацій, у яких здійснювалося засекречування матеріальних носіїв інформації, або керівники державних органів, органів місцевого самоврядування, підприємств, установ, організацій, які є їх правонаступниками, чи керівники вищого рівня зобов'язані протягом шести місяців забезпечити зміну грифа секретності або розсекречування цих матеріальних носіїв секретної інформації та письмово повідомити про це керівників державних органів, органів місцевого самоврядування, підприємств, установ, організацій, яким були передані такі матеріальні носії секретної інформації.

Стаття 16. Строк засекречування матеріальних носіїв інформації

Строк засекречування матеріальних носіїв інформації має відповідати строку дії рішення про віднесення інформації до державної таємниці, встановленого рішенням державного експерта з питань таємниць.

Перебіг строку засекречування матеріальних носіїв інформації починається з часу надання їм грифа секретності.

Стаття 17. Оскарження рішення щодо засекречування матеріальних носіїв інформації

Громадяни та юридичні особи мають право внести посадовим особам, які надали гриф секретності матеріальному носію секретної інформації, обов'язкову для розгляду мотивовану пропозицію про розсекречування цього носія інформації. Зазначені посадові особи повинні протягом одного місяця дати громадянину чи юридичній особі письмову відповідь з цього приводу.

Рішення про засекречування матеріального носія інформації може бути оскаржено громадянином чи юридичною особою в порядку підлеглості вищому органу або посадовій особі чи до суду. У разі незадоволення скарги, поданої в порядку підлеглості, громадянин або юридична особа мають право оскаржити рішення вищого органу або посадової особи до суду.

Розділ IV. ОХОРОНА ДЕРЖАВНОЇ ТАЄМНИЦІ

Стаття 18. Основні організаційно-правові заходи щодо охорони державної таємниці

З метою охорони державної таємниці впроваджуються:

– єдині вимоги до виготовлення, користування, збереження, передачі, транспортування та обліку матеріальних носіїв секретної інформації;

– дозвільний порядок провадження державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями діяльності, пов'язаної з державною таємницею;

– обмеження оприлюднення, передачі іншій державі або поширення іншим шляхом секретної інформації;

– обмеження щодо перебування та діяльності в Україні іноземців, осіб без громадянства та іноземних юридичних осіб, їх доступу до державної таємниці, а також розташування і переміщення об'єктів і технічних засобів, що їм належать;

– особливості здійснення державними органами їх функцій щодо державних органів, органів місцевого самоврядування, підприємств, установ і організацій, діяльність яких пов'язана з державною таємницею;

– режим секретності державних органів, органів місцевого самоврядування, підприємств, установ і організацій, що провадять діяльність, пов'язану з державною таємницею;

– спеціальний порядок допуску та доступу громадян до державної таємниці;

– технічний та криптографічний захисти секретної інформації.

Стаття 19. Єдині вимоги до матеріальних носіїв секретної інформації

Єдині вимоги до виготовлення, обліку, користування, зберігання, схоронності, передачі та транспортування матеріальних носіїв секретної інформації встановлюються Кабінетом Міністрів України.

Стаття 20. Дозвільний порядок провадження діяльності, пов'язаної з державною таємницею, та режим секретності

Державні органи, органи місцевого самоврядування, підприємства, установи, організації мають право провадити діяльність, пов'язану з державною таємницею, після надання їм Службою безпеки України спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею.

Надання дозволу здійснюється на підставі заявок державних органів, органів місцевого самоврядування, підприємств, установ і організацій та результатів спеціальної експертизи щодо наявності умов для провадження діяльності, пов'язаної з державною таємницею. З метою визначення наявності умов для провадження діяльності, пов'язаної з державною таємницею, Служба безпеки України може створювати спеціальні експертні комісії, до складу яких включати фахівців державних органів, органів місцевого самоврядування, підприємств, установ і організацій за погодженням з їх керівниками. Результати спеціальної експертизи щодо наявності умов для провадження діяльності, пов'язаної з державною таємницею, оформляються відповідним актом.

Дозвіл на провадження діяльності, пов'язаної з державною таємницею, надається державним органам, органам місцевого самоврядування, підприємствам, установам, організаціям за результатами спеціальної експертизи за умови, що вони:

– відповідно до компетенції, державних завдань, програм, замовлень, договорів (контрактів) беруть участь у діяльності, пов'язаній з державною таємницею;

– мають приміщення для проведення робіт, пов'язаних з державною таємницею, сховища для зберігання засекречених документів та інших матеріальних носіїв секретної інформації, що відповідають вимогам щодо забезпечення секретності зазначених робіт, виключають можливість доступу до них сторонніх осіб, гарантують збереження носіїв секретної інформації;

– додержуються передбачених законодавством вимог режиму секретності робіт та інших заходів, пов'язаних з використанням секретної інформації, порядку допуску осіб до державної таємниці, прийому іноземних громадян, а також порядку здійснення технічного та криптографічного захисту секретної інформації;

– мають режимно-секретний орган, якщо інше не передбачено цим Законом.

Керівники державних органів, органів місцевого самоврядування, підприємств, установ, організацій, що провадять діяльність, пов'язану з державною таємницею, мають бути обізнані з чинним законодавством про державну таємницю.

Термін дії дозволу на провадження діяльності, пов'язаної з державною таємницею, встановлюється Службою безпеки України і не може перевищувати 5 років. Його тривалість залежить від обсягу робіт (діяльності), що здійснюються державним органом, органом місцевого самоврядування, підприємством, установою, організацією, ступеня секретності та обсягу пов'язаних з цими роботами (діяльністю) відомостей, що становлять державну таємницю, а також категорії режиму секретності.

Дозвіл на провадження діяльності, пов'язаної з державною таємницею, не надається, якщо відсутні умови для провадження такої діяльності, передбачені цією статтею, а також якщо керівник підприємства, установи, організації не є громадянином України або не має допуску до державної таємниці.

Дозвіл на провадження діяльності, пов'язаної з державною таємницею, може бути скасований або його дія може бути зупинена Службою безпеки України на підставі акта проведеної нею перевірки, висновки якого містять дані про недодержання державним органом, органом місцевого самоврядування, підприємством, установою, організацією умов, передбачених цією статтею.

Державним органам, органам місцевого самоврядування, підприємствам, установам, організаціям, що провадять діяльність, пов'язану з державною таємницею, за результатами спеціальної експертизи надаються відповідні категорії режиму секретності (перша, друга або третя), що зазначаються Службою безпеки України у дозволах на провадження діяльності, пов'язаної з державною таємницею.

Державні органи, органи місцевого самоврядування, підприємства, установи і організації, яким надано зазначений у цій статті дозвіл, набувають права на доступ до конкретної секретної інформації згідно з рішенням державних органів, уповноважених державним експертом з питань таємниць приймати такі рішення. За погодженням з цими органами здійснюється передача секретної інформації або її матеріальних носіїв державним органам, органам місцевого самоврядування, підприємствам, установам і організаціям, які мають дозвіл на провадження діяльності, пов'язаної з державною таємницею.

Порядок надання, переоформлення, зупинення та поновлення дії або скасування дозволу на провадження діяльності, пов'язаної з державною таємницею, форма акта спеціальної експертизи щодо наявності умов для провадження діяльності, пов'язаної з державною таємницею, форма дозволу на провадження діяльності, пов'язаної з державною таємницею, та категорії режиму секретності встановлюються Кабінетом Міністрів України.

У разі виникнення кризової ситуації, що загрожує національній безпеці України, оголошення рішення про проведення мобілізації та (або) введення правового режиму воєнного стану надання спеціального дозволу на провадження діяльності, пов’язаної з державною таємницею, органам військового управління, військовим частинам, установам і організаціям Збройних Сил України, інших

військових формувань, правоохоронних органів спеціального призначення, Державної спеціальної служби транспорту, Державної служби спеціального зв'язку та захисту інформації України, що відмобілізовуються, доукомплектовуються, заново формуються, здійснюється у десятиденний термін.

Стаття 21. Режимно-секретні органи

В державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, що провадять діяльність, пов'язану з державною таємницею, з метою розроблення та здійснення заходів щодо забезпечення режиму секретності, постійного контролю за їх додержанням створюються на правах окремих структурних підрозділів режимно-секретні органи (далі – РСО), які підпорядковуються безпосередньо керівнику державного органу, органу місцевого самоврядування, підприємства, установи, організації.

Створення, реорганізація чи ліквідація РСО здійснюються за погодженням із Службою безпеки України. У своїй роботі РСО взаємодіють з органами Служби безпеки України.

До складу режимно-секретного органу входять підрозділи режиму, секретного діловодства та інші підрозділи, що безпосередньо забезпечують охорону державної таємниці, залежно від специфіки діяльності державного органу, органу місцевого самоврядування, підприємства, установи та організації.

В державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях із значним обсягом робіт, пов'язаних з державною таємницею, вводиться посада заступника керівника з питань режиму, на якого покладаються обов'язки та права керівника РСО.

В державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях з незначним обсягом робіт, пов'язаних з державною таємницею, де штатним розписом не передбачено створення РСО, облік і зберігання секретних документів, а також заходи щодо забезпечення режиму секретності здійснюються особисто їх керівниками або спеціально призначеним наказом керівника працівником після створення необхідних умов, що забезпечують режим секретності. На них поширюються обов'язки та права працівників РСО.

Призначення осіб на посади заступників керівників з питань режиму, начальників РСО та їх заступників, а також видання наказу про покладення на окремого працівника обов'язків щодо забезпечення режиму секретності здійснюється за погодженням з органами Служби безпеки України та РСО вищестоящих державних органів, органів місцевого самоврядування, підприємств, установ і організацій.

РСО комплектуються спеціалістами, яким надано допуск до державної таємниці із ступенем секретності "цілком таємно", якщо характер виконуваних робіт не вимагає допуску до державної таємниці із ступенем секретності "особливої важливості". Якщо державний орган, орган місцевого самоврядування, підприємство, установа або організація не провадить діяльність із секретною інформацією, що має ступені секретності "цілком таємно" та

"особливої важливості", РСО такого органу, підприємства, установи або організації комплектується спеціалістами, яким надано допуск до державної таємниці зі ступенем секретності "таємно".

Основними завданнями РСО є:

а) недопущення необгрунтованого допуску та доступу осіб до секретної інформації;

б) своєчасне розроблення та реалізація разом з іншими структурними підрозділами державних органів, органів місцевого самоврядування, підприємств, установ і організацій заходів, що забезпечують охорону державної таємниці;

в) запобігання розголошенню секретної інформації, випадкам втрат матеріальних носіїв цієї інформації, заволодінню секретною інформацією іноземними державами, іноземними юридичними особами, іноземцями, особами без громадянства та громадянами України, яким не надано допуску та доступу до неї;

г) виявлення та закриття каналів просочення секретної інформації в процесі діяльності державних органів, органів місцевого самоврядування, підприємства, установи, організації;

д) забезпечення запровадження заходів режиму секретності під час виконання всіх видів робіт, пов'язаних з державною таємницею, та під час здійснення зовнішніх відносин;

е) організація та ведення секретного діловодства;

є) здійснення контролю за станом режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях та на підпорядкованих їм об'єктах.

РСО мають право:

а) вимагати від усіх працівників державного органу, органу місцевого самоврядування, підприємства, установи та організації, а також відряджених неухильного виконання вимог законодавства щодо забезпечення охорони державної таємниці;

б) брати участь у розгляді проектів штатних розписів державного органу, органу місцевого самоврядування, підприємства, установи та організації та підвідомчих їм установ, підприємств у частині, що стосується РСО, вносити пропозиції щодо структури та чисельності працівників цих органів;

в) брати участь у проведенні атестації працівників, що виконують роботи, пов'язані з державною таємницею, а також у розгляді пропозицій щодо виплати в установленому нормативними актами порядку компенсації за роботу в умовах режимних обмежень;

г) залучати спеціалістів державного органу, органу місцевого самоврядування, підприємства, установи та організації до здійснення заходів щодо охорони державної таємниці;

д) здійснювати перевірки стану й організації роботи з питань захисту державної таємниці і забезпечення режиму секретності у підрозділах державного органу, органу місцевого самоврядування, підприємства, установи та організації,

а також у підвідомчих їм установах та підприємствах, давати відповідні рекомендації;

е) здійснювати перевірки додержання режиму секретності на робочих місцях працівників, що мають допуск до державної таємниці, вмісту спецсховищ (приміщень, сейфів, металевих шаф, спецчемоданів, спецпапок тощо), наявності документів, виробів та інших матеріальних носіїв секретної інформації;

є) порушувати перед керівником державного органу, органу місцевого самоврядування, підприємства, установи та організації питання про призначення службових розслідувань за фактами порушень режиму секретності та секретного діловодства, про притягнення осіб до відповідальності згідно з законом, а також давати рекомендації щодо обов'язкових для виконання вказівок керівникам підрозділів державного органу, органу місцевого самоврядування, підприємства, установи та організації та підвідомчих їм установ, підприємств з питань забезпечення режиму секретності;

ж) брати участь у службових розслідуваннях, у встановленому порядку вимагати від працівників державного органу, органу місцевого самоврядування, підприємства, установи та організації письмових пояснень щодо фактів розголошення ними секретних відомостей, втрати матеріальних носіїв секретної інформації, інших порушень режиму секретності;

з) вносити пропозиції керівникові державного органу, органу місцевого самоврядування, підприємства, установи та організації про припинення робіт, пов'язаних з державною таємницею, в структурних підрозділах, якщо умови для їх виконання не відповідають вимогам режиму секретності; опечатувати приміщення, де ведуться такі роботи або зберігаються матеріальні носії секретної інформації;

и) одержувати від громадян, яким оформляються документи на допуск до державної таємниці, анкетні дані;

і) використовувати засоби зв'язку та вести в установленому порядку поштово-телеграфне листування з іншими державними органами, органами місцевого самоврядування, підприємствами, установами і організаціями та їх РСО з питань забезпечення режиму секретності;

ї) мати печатку з найменуванням РСО, а також інші печатки та штампи установленої форми.

Передача функцій РСО будь-яким іншим підрозділам державного органу, органу місцевого самоврядування, підприємства, установи та організації не допускається.

Стаття 22. Допуск громадян до державної таємниці

Залежно від ступеня секретності інформації встановлюються такі форми допуску до державної таємниці:

– форма 1 – для роботи з секретною інформацією, що має ступені секретності "особливої важливості", "цілком таємно" та "таємно";

– форма 2 – для роботи з секретною інформацією, що має ступені секретності "цілком таємно" та "таємно";

– форма 3 – для роботи з секретною інформацією, що має ступінь секретності "таємно",

а також такі терміни дії допусків:

– для форми 1 – 5 років;

– для форми 2 – 7 років;

– для форми 3 – 10 років.

Допуск до державної таємниці надається дієздатним громадянам України віком від 18 років, які потребують його за умовами своєї службової, виробничої, наукової чи науково-технічної діяльності або навчання, органами Служби безпеки України після проведення їх перевірки. Порядок надання допуску до державної таємниці визначається Кабінетом Міністрів України.

В окремих випадках, які визначаються міністерствами, іншими центральними органами виконавчої влади, за погодженням із Службою безпеки України громадянам України віком від 16 років може надаватися допуск до державної таємниці із ступенями секретності "цілком таємно" та "таємно", а віком від 17 років – також до державної таємниці із ступенем секретності "особливої важливості".

Для розгляду питання про надання громадянам допуску до державної таємниці державними органами, органами місцевого самоврядування, підприємствами, установами, організаціями, де працюють, проходять службу або навчаються громадяни, оформляються документи, які надсилаються до органів Служби безпеки України. Перелік та форми таких документів, а також порядок їх надання визначаються Кабінетом Міністрів України.

Допуск до державної таємниці під час застосування до боржника судових процедур банкрутства у встановленому законодавством порядку надається органами Служби безпеки України арбітражному керуючому (розпоряднику майна, керуючому санацією, ліквідатору) після проведення його перевірки за поданням державного органу, органу місцевого самоврядування, підприємства, установи, організації, до сфери управління якого (якої) належить боржник або який (яка) є замовником робіт, пов’язаних з державною таємницею.

Якщо потреба громадянина у відомостях, що становлять державну таємницю, не пов'язана з місцем роботи, служби або навчання, документи про надання допуску до державної таємниці можуть оформлятися за місцем провадження діяльності, пов'язаної з державною таємницею.

Надання допуску передбачає:

– визначення необхідності роботи громадянина із секретною інформацією;

– перевірку громадянина у зв'язку з допуском до державної таємниці;

– взяття громадянином на себе письмового зобов'язання щодо збереження державної таємниці, яка буде йому довірена;

– одержання у письмовій формі згоди громадянина на передбачені законом обмеження прав у зв'язку з його допуском до державної таємниці;

– ознайомлення громадянина з мірою відповідальності за порушення законодавства про державну таємницю.

Стаття 23. Відмова у наданні допуску до державної таємниці

Допуск до державної таємниці не надається у разі:

1) відсутності у громадянина обгрунтованої необхідності в роботі із секретною інформацією;

2) сприяння громадянином діяльності іноземної держави, іноземної організації чи їх представників, а також окремих іноземців чи осіб без громадянства, що завдає шкоди інтересам національної безпеки України, або участі громадянина в діяльності політичних партій та громадських організацій, діяльність яких заборонена у порядку, встановленому законом;

3) відмови громадянина взяти на себе письмове зобов'язання щодо збереження державної таємниці, яка буде йому довірена, а також за відсутності його письмової згоди на передбачені законом обмеження прав у зв'язку з допуском до державної таємниці;

4) наявності у громадянина судимості за тяжкі або особливо тяжкі злочини або за вчинення кримінального правопорушення проти основ національної безпеки України, передбаченого статтею 111^{-1} Кримінального кодексу України, не погашеної чи не знятої в установленому порядку;

5) наявності у громадянина психічних розладів, які можуть завдати шкоди охороні державної таємниці, відповідно до переліку, затвердженого Міністерством охорони здоров'я України і Службою безпеки України.

У наданні допуску до державної таємниці може бути відмовлено також у разі:

1) повідомлення громадянином під час оформлення допуску недостовірних відомостей про себе;

2) постійного проживання громадянина за кордоном або оформлення ним документів на виїзд для постійного проживання за кордоном;

3) невиконання громадянином обов'язків щодо збереження державної таємниці, яка йому довірена або довірялася раніше.

Громадянина, якому відмовлено у допуску до державної таємниці, якщо виконання трудових чи службових обов'язків вимагає доступу до державної таємниці, а переміщення на інше робоче місце чи іншу посаду неможливе, може бути в передбаченому законодавством порядку переведено на іншу роботу або службу, не пов'язану з державною таємницею, чи звільнено.

Стаття 24. Перевірка громадян у зв'язку з допуском їх до державної таємниці

Перевірка громадян у зв’язку з їх допуском до державної таємниці здійснюється органами Служби безпеки України у строк до одного місяця у порядку, встановленому цим Законом і Законом України "Про оперативно-розшукову діяльність".

У ході перевірки органами Служби безпеки України з'ясовуються наявність чи відсутність обставин, передбачених пунктами 2 і 4 частини першої та частиною другою статті 23 цього Закону. За результатами перевірки органи Служби безпеки України надсилають протягом п'яти робочих днів з дня її закінчення до державних органів, органів місцевого самоврядування, підприємств, установ, організацій, що звернулися з приводу надання громадянам

допуску до державної таємниці, повідомлення про надання або відмову в наданні такого допуску.

Наявність чи відсутність обставин, передбачених пунктами 1, 3 і 5 частини першої статті 23 цього Закону, з'ясовується державним органом, органом місцевого самоврядування, підприємством, установою, організацією, що оформляє документи на допуск.

Повідомлення органів Служби безпеки України про відмову в наданні громадянам допуску до державної таємниці мають містити посилання на відповідні положення статті 23 цього Закону. Відмова не виключає повторного звернення державних органів, органів місцевого самоврядування, підприємств, установ, організацій з цього приводу в разі зміни обставин, за яких у наданні допуску до державної таємниці було відмовлено.

У разі виникнення кризової ситуації, що загрожує національній безпеці України, оголошення рішення про проведення мобілізації та (або) введення правового режиму воєнного стану допуск до державної таємниці громадянам України, які призиваються на військову службу, а також військовослужбовцям та працівникам Збройних Сил України, інших військових формувань, правоохоронних органів спеціального призначення, Державної спеціальної служби транспорту, Державної служби спеціального зв’язку та захисту інформації України, які переміщуються на посади, зайняття яких передбачає наявність допуску до державної таємниці, надається у десятиденний термін. Порядок проведення перевірки громадян у зв’язку з їх допуском до державної таємниці визначається Кабінетом Міністрів України.

Стаття 25. Оскарження громадянином відмови у наданні допуску до державної таємниці

Державний орган, орган місцевого самоврядування, підприємство, установа, організація зобов'язані у п'ятиденний строк з дня надходження повідомлення органу Служби безпеки України про відмову у наданні громадянину допуску до державної таємниці письмово повідомити такого громадянина про причини і підстави відмови.

Громадянин має право оскаржити рішення про відмову у наданні допуску до державної таємниці в порядку, встановленому законом.

Стаття 26. Переоформлення допуску до державної таємниці, підвищення або зниження його форми та скасування

Переоформлення громадянам допуску до державної таємниці здійснюється:

– у разі закінчення терміну дії допуску до державної таємниці за необхідності подальшої роботи з секретною інформацією;

– у разі необхідності підвищення чи зниження громадянину форми допуску для роботи із секретною інформацією вищого чи нижчого ступеня секретності;

– у разі необхідності проведення додаткової перевірки, пов'язаної з можливим виникненням обставин, передбачених пунктами 2 і 4 частини першої та частиною другою статті 23 цього Закону.

Скасування раніше наданого допуску до державної таємниці здійснюється органами Служби безпеки України у разі виникнення або виявлення обставин, передбачених статтею 23 цього Закону, або після припинення громадянином діяльності, у зв'язку з якою йому було надано допуск, втрати ним громадянства або визнання його недієздатним на підставі інформації, здобутої органами Служби безпеки України або отриманої від державних органів, органів місцевого самоврядування, підприємств, установ, організацій.

На прохання громадянина його допуск до державної таємниці скасовується протягом трьох днів з часу звернення з приводу скасування допуску.

Повідомлення про скасування громадянину допуску до державної таємниці з посиланням на відповідні положення статті 23 цього Закону орган Служби безпеки України надсилає до державного органу, органу місцевого самоврядування, підприємства, установи, організації, де такий громадянин провадить діяльність, пов'язану з державною таємницею. Громадянин має право оскаржити скасування йому допуску до державної таємниці в порядку, встановленому законом.

Громадянина, якому скасовано допуск до державної таємниці, якщо виконання трудових чи службових обов'язків вимагає доступу до державної таємниці, а переміщення на інше робоче місце чи іншу посаду неможливе, може бути в передбаченому законодавством порядку переведено на іншу роботу або службу, не пов'язану з державною таємницею, чи звільнено.

Порядок надання, переоформлення та скасування громадянам допуску до державної таємниці встановлюється Кабінетом Міністрів України.

Стаття 27. Доступ громадян до державної таємниці

Доступ до державної таємниці надається дієздатним громадянам України, яким надано допуск до державної таємниці та які потребують його за умовами своєї службової, виробничої, наукової чи науково-дослідної діяльності або навчання.

Рішення про надання доступу до конкретної секретної інформації (категорії секретної інформації) та її матеріальних носіїв приймають керівники державних органів, органів місцевого самоврядування, підприємств, установ та організацій, у яких виконуються роботи, пов'язані з державною таємницею, або зберігаються матеріальні носії секретної інформації.

Керівники державних органів, за винятком осіб, передбачених частиною шостою цієї статті, органів місцевого самоврядування, підприємств, установ та організацій доступ до державної таємниці у сфері, що стосується діяльності державного органу, органу місцевого самоврядування, підприємства, установи та організації, отримують за посадою після надання їм допуску до державної таємниці за відповідною формою.

Порядок надання доступу до державної таємниці особам, залученим до конфіденційного співробітництва з оперативними підрозділами правоохоронних та інших спеціально уповноважених органів, які проводять оперативно-розшукову, розвідувальну або контррозвідувальну діяльність, визначається керівниками зазначених органів за погодженням із Службою безпеки України. У

Службі безпеки України такий порядок надання доступу до державної таємниці визначається Головою Служби безпеки України.

Відмова надати громадянинові України доступ до конкретної секретної інформації та її матеріальних носіїв можлива лише у разі відсутності підстав, передбачених частиною першою цієї статті, та може бути оскаржена в порядку, встановленому частиною другою статті 25 цього Закону.

Президентові України, Голові Верховної Ради України, Прем'єр-міністрові України та іншим членам Кабінету Міністрів України, Голові Верховного Суду, Голові Конституційного Суду України, Генеральному прокурору, Голові Служби безпеки України, Голові та іншим членам Рахункової палати, народним депутатам України, Директору Бюро економічної безпеки України доступ до державної таємниці усіх ступенів секретності надається за посадою після взяття ними письмового зобов'язання щодо збереження державної таємниці.

Іноземцям та особам без громадянства доступ до державної таємниці надається у виняткових випадках на підставі міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України, або письмового розпорядження Президента України з урахуванням необхідності забезпечення національної безпеки України на підставі пропозицій Ради національної безпеки і оборони України.

Доступ до державної таємниці усіх ступенів секретності, ознайомлення з якою є необхідним народним депутатам України для виконання своїх повноважень у комітеті Верховної Ради України, до предмета відання якого віднесено питання забезпечення контрольних функцій Верховної Ради України за діяльністю органів спеціального призначення з правоохоронними функціями, правоохоронних органів спеціального призначення та розвідувальних органів, надається після проходження перевірки у зв’язку з допуском їх до державної таємниці.

Стаття 28. Обов'язки громадянина щодо збереження державної таємниці

Громадянин, якому надано допуск до державної таємниці, зобов'язаний:

– не допускати розголошення будь-яким способом державної таємниці, яка йому довірена або стала відомою у зв'язку з виконанням службових обов'язків;

– не брати участі в діяльності політичних партій та громадських організацій, діяльність яких заборонена в порядку, встановленому законом;

– не сприяти іноземним державам, іноземним організаціям чи їх представникам, а також окремим іноземцям та особам без громадянства у провадженні діяльності, що завдає шкоди інтересам національної безпеки України;

– виконувати вимоги режиму секретності;

– повідомляти посадових осіб, які надали йому доступ до державної таємниці, та відповідні режимно-секретні органи про виникнення обставин, передбачених статтею 23 цього Закону, або інших обставин, що перешкоджають збереженню довіреної йому державної таємниці, а також повідомляти у письмовій формі про свій виїзд з України;

– додержуватися інших вимог законодавства про державну таємницю.

Стаття 29. Обмеження прав у зв'язку з допуском та доступом до державної таємниці

Громадянин, якому було надано допуск та доступ до державної таємниці у порядку, встановленому законодавством, і який реально був обізнаний з нею, може бути обмежений у праві виїзду на постійне місце проживання в іноземну державу до розсекречування відповідної інформації, але не більш як на п'ять років з часу припинення діяльності, пов'язаної з державною таємницею.

Не обмежується виїзд у держави, з якими Україна має міжнародні договори, що передбачають такий виїзд і згода на обов'язковість яких надана Верховною Радою України.

На громадянина також поширюються обмеження свободи інформаційної діяльності, що випливають з цього Закону.

Стаття 30. Компенсація громадянам у зв'язку з виконанням робіт, які передбачають доступ до державної таємниці

У разі коли за умовами своєї професійної діяльності громадянин постійно працює з відомостями, що становлять державну таємницю, йому повинна надаватися відповідна компенсація за роботу в умовах режимних обмежень, види, розміри та порядок надання якої встановлюються Кабінетом Міністрів України.

Стаття 31. Обмеження на оприлюднення секретної інформації

Під час підготовки матеріалів для опублікування, поширення у пресі та інших засобах масової інформації або переміщення їх через державний кордон державні органи, органи місцевого самоврядування, підприємства, установи, організації та громадяни з метою охорони секретної інформації зобов'язані керуватися законами України "Про інформацію" та "Про доступ до публічної інформації", цим Законом та іншими нормативно-правовими актами про державну таємницю.

Контроль за додержанням законодавства про державну таємницю з метою запобігання її поширенню у пресі та інших засобах масової інформації здійснює центральний орган виконавчої влади з питань інформаційної політики.

Стаття 32. Обмеження щодо передачі державної таємниці іноземній державі чи міжнародній організації

Секретна інформація до скасування рішення про віднесення її до державної таємниці та матеріальні носії такої інформації до їх розсекречування можуть бути передані іноземній державі чи міжнародній організації лише на підставі міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, або письмового мотивованого розпорядження Президента України з урахуванням необхідності забезпечення національної безпеки України на підставі пропозицій Ради національної безпеки і оборони України.

Стаття 33. Обмеження, пов'язані з державною таємницею, щодо перебування і діяльності в Україні іноземців, осіб без громадянства та іноземних юридичних осіб, а також розташування та переміщення об'єктів і технічних засобів, що їм належать

Обмеження, пов'язані з державною таємницею, щодо перебування і діяльності в Україні іноземців, осіб без громадянства та іноземних юридичних осіб, а також розташування та переміщення об'єктів і технічних засобів, що їм належать, визначаються відповідним законодавством.

Стаття 34. Особливості здійснення державними органами їх функцій щодо державних органів, органів місцевого самоврядування, підприємств, установ і організацій, що провадять діяльність, пов'язану з державною таємницею

Державні органи, в тому числі правоохоронні, державного фінансового контролю та суди, з метою охорони державної таємниці мають за погодженням із Службою безпеки України встановлювати порядок здійснення своїх функцій щодо державних органів, органів місцевого самоврядування, підприємств, установ і організацій, що провадять діяльність, пов'язану з державною таємницею.

Державні органи, органи місцевого самоврядування, підприємства, установи і організації, що провадять діяльність, пов'язану з державною таємницею, вправі відмовити у виконанні запиту щодо надання секретної інформації чи інших подібних вимог зазначеним у частині першій цієї статті державним органам, якщо останні не встановили такого порядку або не додержуються його.

Про мотиви такої відмови одночасно повідомляється Служба безпеки України, яка протягом місяця зобов'язана прийняти рішення про її обгрунтованість.

Стаття 35. Технічний та криптографічний захисти секретної інформації

Технічний та криптографічний захисти секретної інформації здійснюються в порядку, встановленому Президентом України.

Стаття 36. Оперативно-розшукові заходи щодо охорони державної таємниці

Оперативно-розшукові заходи щодо охорони державної таємниці здійснюються відповідно до Закону України "Про оперативно-розшукову діяльність".

Розділ V. КОНТРОЛЬ ЗА ЗАБЕЗПЕЧЕННЯМ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ТА НАГЛЯД ЗА ДОДЕРЖАННЯМ ЗАКОНОДАВСТВА ПРО ДЕРЖАВНУ ТАЄМНИЦЮ

Стаття 37. Контроль за забезпеченням охорони державної таємниці

Керівники державних органів, органів місцевого самоврядування, підприємств, установ і організацій зобов'язані здійснювати постійний контроль за забезпеченням охорони державної таємниці.

Державні органи, органи місцевого самоврядування, підприємства, установи і організації, що розміщують замовлення у підрядників, зобов'язані контролювати стан охорони державної таємниці, яка була передана підрядникам у зв'язку з виконанням замовлення.

Державні органи, яким рішенням державного експерта з питань таємниць було надано право вирішувати питання про доступ державних органів, органів місцевого самоврядування, підприємств, установ, організацій до конкретної

секретної інформації, зобов'язані контролювати стан охорони державної таємниці в усіх державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, які виконують роботи, пов'язані з відповідною державною таємницею, або зберігають матеріальні носії зазначеної секретної інформації.

Контроль за додержанням законодавства про державну таємницю в системі Служби безпеки України здійснюється відповідно до Закону України "Про Службу безпеки України".

Служба безпеки України має право контролювати стан охорони державної таємниці в усіх державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, а також у зв'язку з виконанням цих повноважень одержувати безоплатно від них інформацію з питань забезпечення охорони державної таємниці. Висновки Служби безпеки України, викладені в актах офіційних перевірок за результатами контролю стану охорони державної таємниці, є обов'язковими для виконання посадовими особами підприємств, установ та організацій незалежно від їх форм власності.

Стаття 38. Нагляд за додержанням законодавства про державну таємницю

Нагляд за додержанням законодавства про державну таємницю здійснюється у порядку, визначеному законом.

Допуск та доступ посадових осіб, які здійснюють нагляд, до відомостей, що становлять державну таємницю, проводяться відповідно до цього Закону.

Розділ VI. ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА ПРО ДЕРЖАВНУ ТАЄМНИЦЮ

Стаття 39. Відповідальність за порушення законодавства про державну таємницю

Посадові особи та громадяни, винні у:

– розголошенні державної таємниці;

– втраті документів та інших матеріальних носіїв секретної інформації;

– недодержанні встановленого законодавством порядку передачі державної таємниці іншій державі чи міжнародній організації;

– засекречуванні інформації, зазначеної у частинах третій і четвертій статті 8 цього Закону;

– навмисному невіднесенні до державної таємниці інформації, розголошення якої може завдати шкоди інтересам національної безпеки України, а також необгрунтованому заниженні ступеня секретності або необгрунтованому розсекречуванні секретної інформації;

– безпідставному засекречуванні інформації, у тому числі з порушенням вимог Закону України "Про доступ до публічної інформації";

– наданні грифа секретності матеріальним носіям інформації, яка не становить державної таємниці, або ненаданні грифа секретності матеріальним носіям інформації, що становить державну таємницю, а також безпідставному скасуванні чи зниженні грифа секретності матеріальних носіїв секретної інформації;

– порушенні встановленого законодавством порядку надання допуску та доступу до державної таємниці;

– порушенні встановленого законодавством режиму секретності та невиконанні обов'язків щодо збереження державної таємниці;

– невжитті заходів щодо забезпечення охорони державної таємниці та незабезпеченні контролю за охороною державної таємниці;

– провадженні діяльності, пов'язаної з державною таємницею, без одержання в установленому порядку спеціального дозволу на провадження такої діяльності, а також розміщенні державних замовлень на виконання робіт, доведенні мобілізаційних завдань, пов'язаних з державною таємницею, в державних органах, органах місцевого самоврядування, на підприємствах, в установах, організаціях, яким не надано спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею;

– недодержанні вимог законодавства щодо забезпечення охорони державної таємниці під час здійснення міжнародного співробітництва, прийому іноземних делегацій, груп, окремих іноземців та осіб без громадянства і проведення роботи з ними;

– невиконанні норм і вимог технічного захисту секретної інформації, внаслідок чого виникає реальна загроза порушення цілісності цієї інформації або просочення її технічними каналами, -

– несуть дисциплінарну, адміністративну та кримінальну відповідальність згідно із законом.

А.6. Закон України «Про захист персональних даних»

Стаття 1. Сфера дії Закону

Цей Закон регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних.

Цей Закон поширюється на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів, а також на обробку персональних даних, що містяться у картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів.

Стаття 2. Визначення термінів

У цьому Законі нижченаведені терміни вживаються в такому значенні:

– база персональних даних – іменована сукупність упорядкованих персональних даних в електронній формі та/або у формі картотек персональних даних;

– володілець персональних даних – фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом;

– згода суб'єкта персональних даних – добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди. У сфері електронної комерції згода суб'єкта персональних даних може бути надана під час реєстрації в інформаційно-комунікаційній системі суб'єкта електронної комерції шляхом проставлення відмітки про надання дозволу на обробку своїх персональних даних відповідно до сформульованої мети їх обробки, за умови, що така система не створює можливостей для обробки персональних даних до моменту проставлення відмітки;

– знеособлення персональних даних – вилучення відомостей, які дають змогу прямо чи опосередковано ідентифікувати особу;

– картотека – будь-які структуровані персональні дані, доступні за визначеними критеріями, незалежно від того, чи такі дані централізовані, децентралізовані або розділені за функціональними чи географічними принципами;

– обробка персональних даних – будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем;

– одержувач – фізична чи юридична особа, якій надаються персональні дані, у тому числі третя особа;

– персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована;

– розпорядник персональних даних – фізична чи юридична особа, якій

володільцем персональних даних або законом надано право обробляти ці дані від імені володільця;

– суб’єкт персональних даних – фізична особа, персональні дані якої обробляються;

– третя особа – будь-яка особа, за винятком суб’єкта персональних даних, володільця чи розпорядника персональних даних та Уповноваженого Верховної Ради України з прав людини, якій володільцем чи розпорядником персональних даних здійснюється передача персональних даних.

Стаття 3. Законодавство про захист персональних даних

Законодавство про захист персональних даних складають Конституція України, цей Закон, інші закони та підзаконні нормативно-правові акти, міжнародні договори України, згода на обов'язковість яких надана Верховною Радою України.

Стаття 4. Суб'єкти відносин, пов'язаних із персональними даними

1. Суб'єктами відносин, пов'язаних із персональними даними, є:

– суб'єкт персональних даних;

– володілець персональних даних;

– розпорядник персональних даних;

– третя особа;

Уповноважений Верховної Ради України з прав людини (далі – Уповноважений).

2. Володільцем чи розпорядником персональних даних можуть бути підприємства, установи і організації усіх форм власності, органи державної влади чи органи місцевого самоврядування, фізичні особи – підприємці, які обробляють персональні дані відповідно до закону.

3. Розпорядником персональних даних, володільцем яких є орган державної влади чи орган місцевого самоврядування, крім цих органів, може бути лише підприємство державної або комунальної форми власності.

4. Володілець персональних даних може доручити обробку персональних даних розпоряднику персональних даних відповідно до договору, укладеного в письмовій формі.

5. Розпорядник персональних даних може обробляти персональні дані лише з метою і в обсязі, визначених у договорі.

Стаття 5. Об'єкти захисту

1. Об’єктами захисту є персональні дані.

2. Персональні дані можуть бути віднесені до конфіденційної інформації про особу законом або відповідною особою. Не є конфіденційною інформацією персональні дані, що стосуються здійснення особою, уповноваженою на виконання функцій держави або місцевого самоврядування, посадових або службових повноважень.

3. Персональні дані, зазначені у декларації особи, уповноваженої на виконання функцій держави або місцевого самоврядування, оформленій за формою, визначеною відповідно до Закону України "Про запобігання корупції", не належать до інформації з обмеженим доступом, крім відомостей, визначених Законом України "Про запобігання корупції".

Не належить до інформації з обмеженим доступом інформація про отримання у будь-якій формі фізичною особою бюджетних коштів, державного чи комунального майна, структуру, принципи формування та розмір оплати праці, винагороди, додаткового блага керівника, заступника керівника юридичної особи публічного права, керівника, заступника керівника, члена наглядової ради державного чи комунального підприємства або державної чи комунальної організації, що має на меті одержання прибутку, особи, яка постійно або тимчасово обіймає посаду члена виконавчого органу чи входить до складу наглядової ради господарського товариства, у статутному капіталі якого більше 50 відсотків акцій (часток, паїв) прямо чи опосередковано належать державі та/або територіальній громаді, крім випадків, передбачених статтею 6 Закону України "Про доступ до публічної інформації".

Не належить до інформації з обмеженим доступом інформація про фізичних осіб, які мають податковий борг, яка публікується на офіційному веб-порталі центрального органу виконавчої влади, що реалізує державну податкову політику, відповідно до вимог пункту 35.4 статті 35 Податкового кодексу України.

Законом може бути заборонено віднесення інших відомостей, що є персональними даними, до інформації з обмеженим доступом.

Стаття 6. Загальні вимоги до обробки персональних даних

1. Мета обробки персональних даних має бути сформульована в законах, інших нормативно-правових актах, положеннях, установчих чи інших документах, які регулюють діяльність володільця персональних даних, та відповідати законодавству про захист персональних даних.

Обробка персональних даних здійснюється відкрито і прозоро із застосуванням засобів та у спосіб, що відповідають визначеним цілям такої обробки.

У разі зміни визначеної мети обробки персональних даних на нову мету, яка є несумісною з попередньою, для подальшої обробки даних володілець персональних даних повинен отримати згоду суб’єкта персональних даних на обробку його даних відповідно до зміненої мети, якщо інше не передбачено законом.

2. Персональні дані мають бути точними, достовірними та оновлюватися в міру потреби, визначеної метою їх обробки.

3. Склад та зміст персональних даних мають бути відповідними, адекватними та ненадмірними стосовно визначеної мети їх обробки.

4. Первинними джерелами відомостей про фізичну особу є: видані на її ім'я документи; підписані нею документи; відомості, які особа надає про себе.

5. Обробка персональних даних здійснюється для конкретних і законних цілей, визначених за згодою суб’єкта персональних даних, або у випадках, передбачених законами України, у порядку, встановленому законодавством.

6. Не допускається обробка даних про фізичну особу, які є конфіденційною інформацією, без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

7. Якщо обробка персональних даних є необхідною для захисту життєво важливих інтересів суб'єкта персональних даних, обробляти персональні дані без його згоди можна до часу, коли отримання згоди стане можливим.

8. Персональні дані обробляються у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються, не довше, ніж це необхідно для законних цілей, у яких вони збиралися або надалі оброблялися.

9. Подальша обробка персональних даних в історичних, статистичних чи наукових цілях може здійснюватися за умови забезпечення їх належного захисту.

10. Типовий порядок обробки персональних даних затверджується Уповноваженим.

Стаття 7. Особливі вимоги до обробки персональних даних

1. Забороняється обробка персональних даних про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, засудження до кримінального покарання, а також даних, що стосуються здоров’я, статевого життя, біометричних або генетичних даних.

2. Положення частини першої цієї статті не застосовується, якщо обробка персональних даних:

1) здійснюється за умови надання суб'єктом персональних даних однозначної згоди на обробку таких даних;

2) необхідна для здійснення прав та виконання обов'язків володільця у сфері трудових правовідносин відповідно до закону із забезпеченням відповідного захисту;

3) необхідна для захисту життєво важливих інтересів суб'єкта персональних даних або іншої особи у разі недієздатності або обмеження цивільної дієздатності суб'єкта персональних даних;

4) здійснюється із забезпеченням відповідного захисту релігійною організацією, громадською організацією світоглядної спрямованості, політичною партією або професійною спілкою, що створені відповідно до закону, за умови, що обробка стосується виключно персональних даних членів цих об'єднань або осіб, які підтримують постійні контакти з ними у зв'язку з характером їх діяльності, та персональні дані не передаються третій особі без згоди суб'єктів персональних даних;

5) необхідна для обґрунтування, задоволення або захисту правової вимоги;

6) необхідна в цілях охорони здоров’я для:

– встановлення медичного діагнозу, для забезпечення піклування чи лікування або надання медичних послуг, моніторингу відповідності встановленим умовам надання таких послуг (у тому числі умовам договорів про медичне обслуговування населення та договорів про реімбурсацію за програмою медичних гарантій), функціонування електронної системи охорони здоров’я за умови, що такі дані обробляються медичним працівником, фахівцем з реабілітації або іншою особою закладу охорони здоров’я, реабілітаційного закладу чи фізичною особою – підприємцем, яка одержала ліцензію на провадження господарської діяльності з медичної практики, та її працівниками, на яких покладено обов’язки щодо забезпечення захисту персональних даних та

поширюється дія законодавства про лікарську таємницю, працівниками центрального органу виконавчої влади, що реалізує державну політику у сфері державних фінансових гарантій медичного обслуговування населення, працівниками закладу, що здійснює державний санітарно-епідеміологічний нагляд та діяльність у галузі громадського здоров'я, який одержав ліцензію на провадження господарської діяльності з медичної практики, на яких покладено обов'язки щодо забезпечення захисту персональних даних;

– контролю якості надання медичних послуг за умови, що такі дані обробляються працівниками центрального органу виконавчої влади, що реалізує державну політику у сфері контролю якості надання медичних послуг;

– обміну інформацією про фінансування медичних послуг та послуг у сфері охорони здоров'я за умови, що такі дані обробляються працівниками Фонду соціального страхування України, Пенсійного фонду України, Фонду соціального захисту осіб з інвалідністю, центрального органу виконавчої влади, що забезпечує формування та реалізує державну фінансову та бюджетну політику, на яких покладено обов'язки щодо забезпечення захисту персональних даних.

6[-1]) необхідна в цілях забезпечення ведення військового обліку призовників, військовозобов'язаних та резервістів (в обсягах даних, зазначених у статті 7 Закону України "Про Єдиний державний реєстр призовників, військовозобов'язаних та резервістів");

7) стосується вироків суду, виконання завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом та здійснюється державним органом в межах його повноважень, визначених законом;

8) стосується даних, які були явно оприлюднені суб'єктом персональних даних.

Стаття 8. Права суб'єкта персональних даних

1. Особисті немайнові права на персональні дані, які має кожна фізична особа, є невід'ємними і непорушними.

2. Суб'єкт персональних даних має право:

1) знати про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки, місцезнаходження або місце проживання (перебування) володільця чи розпорядника персональних даних або дати відповідне доручення щодо отримання цієї інформації уповноваженим ним особам, крім випадків, встановлених законом;

2) отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються його персональні дані;

3) на доступ до своїх персональних даних;

4) отримувати не пізніш як за тридцять календарних днів з дня надходження запиту, крім випадків, передбачених законом, відповідь про те, чи обробляються його персональні дані, а також отримувати зміст таких персональних даних;

5) пред'являти вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних;

6) пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними;

7) на захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи;

8) звертатися із скаргами на обробку своїх персональних даних до Уповноваженого або до суду;

9) застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних;

10) вносити застереження стосовно обмеження права на обробку своїх персональних даних під час надання згоди;

11) відкликати згоду на обробку персональних даних;

12) знати механізм автоматичної обробки персональних даних;

13) на захист від автоматизованого рішення, яке має для нього правові наслідки.

Стаття 9. Повідомлення про обробку персональних даних

1. Володілець персональних даних повідомляє Уповноваженого про обробку персональних даних, яка становить особливий ризик для прав і свобод суб’єктів персональних даних, упродовж тридцяти робочих днів з дня початку такої обробки.

Види обробки персональних даних, яка становить особливий ризик для прав і свобод суб’єктів персональних даних, та категорії суб’єктів, на яких поширюється вимога щодо повідомлення, визначаються Уповноваженим.

2. Повідомлення про обробку персональних даних подається за формою та в порядку, визначеними Уповноваженим.

3. Володілець персональних даних зобов’язаний повідомляти Уповноваженого про кожну зміну відомостей, що підлягають повідомленню, упродовж десяти робочих днів з дня настання такої зміни.

4. Інформація, що повідомляється відповідно до цієї статті, підлягає оприлюдненню на офіційному веб-сайті Уповноваженого в порядку, визначеному Уповноваженим.

Стаття 10. Використання персональних даних

1. Використання персональних даних передбачає будь-які дії володільця щодо обробки цих даних, дії щодо їх захисту, а також дії щодо надання часткового або повного права обробки персональних даних іншим суб'єктам відносин, пов'язаних із персональними даними, що здійснюються за згодою суб'єкта персональних даних чи відповідно до закону.

2. Використання персональних даних володільцем здійснюється у разі створення ним умов для захисту цих даних. Володільцю забороняється розголошувати відомості стосовно суб'єктів персональних даних, доступ до персональних даних яких надається іншим суб'єктам відносин, пов'язаних з такими даними.

3. Використання персональних даних працівниками суб'єктів відносин, пов'язаних з персональними даними, повинно здійснюватися лише відповідно до їхніх професійних чи службових або трудових обов'язків. Ці працівники зобов'язані не допускати розголошення у будь-який спосіб персональних даних, які їм було довірено або які стали відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків, крім випадків, передбачених законом. Таке зобов'язання чинне після припинення ними діяльності, пов'язаної з персональними даними, крім випадків, установлених законом.

4. Відомості про особисте життя фізичної особи не можуть використовуватися як чинник, що підтверджує чи спростовує її ділові якості.

5. Якщо особа, яка є резидентом Дія Сіті відповідно до Закону України "Про стимулювання розвитку цифрової економіки в Україні", виступає суб'єктом відносин, пов'язаних з персональними даними, використання таких персональних даних гіг-спеціалістами резидента Дія Сіті має здійснюватися лише відповідно до їхніх обов'язків за гіг-контрактами. Ці гіг-спеціалісти зобов'язані не допускати розголошення у будь-який спосіб персональних даних, які їм було довірено або які стали їм відомі у зв'язку з виконанням обов'язків за гіг-контрактом, крім випадків, передбачених законом. Таке зобов'язання є чинним після припинення ними діяльності, пов'язаної з персональними даними, крім випадків, установлених законом.

Стаття 11. Підстави для обробки персональних даних

1. Підставами для обробки персональних даних є:

1) згода суб'єкта персональних даних на обробку його персональних даних;

2) дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень;

3) укладення та виконання правочину, стороною якого є суб'єкт персональних даних або який укладено на користь суб'єкта персональних даних чи для здійснення заходів, що передують укладенню правочину на вимогу суб'єкта персональних даних;

4) захист життєво важливих інтересів суб'єкта персональних даних;

5) необхідність виконання обов'язку володільця персональних даних, який передбачений законом;

6) необхідність захисту законних інтересів володільця персональних даних або третьої особи, якій передаються персональні дані, крім випадків, коли потреби захисту основоположних прав і свобод суб'єкта персональних даних у зв'язку з обробкою його даних переважають такі інтереси.

Стаття 12. Збирання персональних даних

1. Збирання персональних даних є складовою процесу їх обробки, що передбачає дії з підбору чи впорядкування відомостей про фізичну особу.

2. Суб'єкт персональних даних повідомляється про володільця персональних даних, склад та зміст зібраних персональних даних, свої права, визначені цим Законом, мету збору персональних даних та осіб, яким передаються його персональні дані:

– в момент збору персональних даних, якщо персональні дані збираються у суб’єкта персональних даних;

– в інших випадках протягом тридцяти робочих днів з дня збору персональних даних.

Стаття 13. Накопичення та зберігання персональних даних

1. Накопичення персональних даних передбачає дії щодо поєднання та систематизації відомостей про фізичну особу чи групу фізичних осіб або внесення цих даних до бази персональних даних.

2. Зберігання персональних даних передбачає дії щодо забезпечення їх цілісності та відповідного режиму доступу до них.

Стаття 14. Поширення персональних даних

1. Поширення персональних даних передбачає дії щодо передачі відомостей про фізичну особу за згодою суб'єкта персональних даних.

2. Поширення персональних даних без згоди суб’єкта персональних даних або уповноваженої ним особи дозволяється у випадках, визначених законом, і лише (якщо це необхідно) в інтересах національної безпеки, економічного добробуту, прав людини та для проведення Всеукраїнського перепису населення.

3. Виконання вимог встановленого режиму захисту персональних даних забезпечує сторона, що поширює ці дані.

4. Сторона, якій передаються персональні дані, повинна попередньо вжити заходів щодо забезпечення вимог цього Закону.

Стаття 15. Видалення або знищення персональних даних

1. Персональні дані видаляються або знищуються в порядку, встановленому відповідно до вимог закону.

2. Персональні дані підлягають видаленню або знищенню у разі:

– закінчення строку зберігання даних, визначеного згодою суб'єкта персональних даних на обробку цих даних або законом;

– припинення правовідносин між суб'єктом персональних даних та володільцем чи розпорядником, якщо інше не передбачено законом;

– видання відповідного припису Уповноваженого або визначених ним посадових осіб секретаріату Уповноваженого;

– набрання законної сили рішенням суду щодо видалення або знищення персональних даних.

3. Персональні дані, зібрані з порушенням вимог цього Закону, підлягають видаленню або знищенню у встановленому законодавством порядку.

4. Персональні дані, зібрані під час виконання завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом, видаляються або знищуються відповідно до вимог закону.

Стаття 16. Порядок доступу до персональних даних

1. Порядок доступу до персональних даних третіх осіб визначається умовами згоди суб’єкта персональних даних на обробку цих даних, наданої володільцю персональних даних, або відповідно до вимог закону. Порядок доступу третіх осіб до персональних даних, які перебувають у володінні розпорядника публічної інформації, визначається Законом України "Про доступ

до публічної інформації", крім даних, що отримує від інших органів центральний орган виконавчої влади, що забезпечує формування та реалізує державну фінансову та бюджетну політику, під час здійснення верифікації та моніторингу державних виплат.

2. Доступ до персональних даних третій особі не надається, якщо зазначена особа відмовляється взяти на себе зобов'язання щодо забезпечення виконання вимог цього Закону або неспроможна їх забезпечити.

3. Суб'єкт відносин, пов'язаних з персональними даними, подає запит щодо доступу (далі – запит) до персональних даних володільцю персональних даних.

4. У запиті зазначаються:

1) прізвище, ім'я та по батькові, місце проживання (місце перебування) і реквізити документа, що посвідчує фізичну особу, яка подає запит (для фізичної особи – заявника);

2) найменування, місцезнаходження юридичної особи, яка подає запит, посада, прізвище, ім'я та по батькові особи, яка засвідчує запит; підтвердження того, що зміст запиту відповідає повноваженням юридичної особи (для юридичної особи – заявника);

3) прізвище, ім'я та по батькові, а також інші відомості, що дають змогу ідентифікувати фізичну особу, стосовно якої робиться запит;

4) відомості про базу персональних даних, стосовно якої подається запит, чи відомості про володільця чи розпорядника персональних даних;

5) перелік персональних даних, що запитуються;

6) мета та/або правові підстави для запиту.

5. Строк вивчення запиту на предмет його задоволення не може перевищувати десяти робочих днів з дня його надходження.

Протягом цього строку володілець персональних даних доводить до відома особи, яка подає запит, що запит буде задоволено або відповідні персональні дані не підлягають наданню, із зазначенням підстави, визначеної у відповідному нормативно-правовому акті.

Запит задовольняється протягом тридцяти календарних днів з дня його надходження, якщо інше не передбачено законом.

6. Суб'єкт персональних даних має право на одержання будь-яких відомостей про себе у будь-якого суб'єкта відносин, пов'язаних з персональними даними, за умови надання інформації, визначеної у пункті 1 частини четвертої цієї статті, крім випадків, установлених законом.

Стаття 17. Відстрочення або відмова у доступі до персональних даних

1. Відстрочення доступу суб'єкта персональних даних до своїх персональних даних не допускається.

2. Відстрочення доступу до персональних даних третіх осіб допускається у разі, якщо необхідні дані не можуть бути надані протягом тридцяти календарних днів з дня надходження запиту. При цьому загальний термін вирішення питань, порушених у запиті, не може перевищувати сорока п'яти календарних днів.

Повідомлення про відстрочення доводиться до відома третьої особи, яка подала запит, у письмовій формі з роз'ясненням порядку оскарження такого рішення.

У повідомленні про відстрочення зазначаються:

1) прізвище, ім'я та по батькові посадової особи;

2) дата відправлення повідомлення;

3) причина відстрочення;

4) строк, протягом якого буде задоволено запит.

3. Відмова у доступі до персональних даних допускається, якщо доступ до них заборонено згідно із законом.

У повідомленні про відмову зазначаються:

1) прізвище, ім'я, по батькові посадової особи, яка відмовляє у доступі;

2) дата відправлення повідомлення;

3) причина відмови.

Стаття 18. Оскарження рішення про відстрочення або відмову в доступі до персональних даних

1. Рішення про відстрочення або відмову у доступі до персональних даних може бути оскаржено до Уповноваженого Верховної Ради України з прав людини або суду.

2. Якщо запит зроблено суб'єктом персональних даних щодо даних про себе, обов'язок доведення в суді законності відмови у доступі покладається на володільця персональних даних, до якого подано запит.

Стаття 19. Оплата доступу до персональних даних

1. Доступ суб'єкта персональних даних до даних про себе здійснюється безоплатно.

2. Доступ інших суб'єктів відносин, пов'язаних з персональними даними, до персональних даних певної фізичної особи чи групи фізичних осіб може бути платним у разі додержання умов, визначених цим Законом. Оплаті підлягає робота, пов'язана з обробкою персональних даних, а також робота з консультування та організації доступу до відповідних даних.

3. Розмір плати за послуги з надання доступу до персональних даних органами державної влади визначається Кабінетом Міністрів України.

4. Органи державної влади та органи місцевого самоврядування мають право на безперешкодний і безоплатний доступ до персональних даних відповідно до їх повноважень.

Стаття 20. Зміни і доповнення до персональних даних

1. Володільці чи розпорядники персональних даних зобов'язані вносити зміни до персональних даних на підставі вмотивованої письмової вимоги суб'єкта персональних даних.

2. Володільці чи розпорядники персональних даних зобов’язані вносити зміни до персональних даних також за зверненням інших суб’єктів відносин, пов’язаних із персональними даними, якщо на це є згода суб’єкта персональних даних чи відповідна зміна здійснюється згідно з приписом Уповноваженого або визначених ним посадових осіб секретаріату Уповноваженого чи за рішенням суду, що набрало законної сили.

3. Зміна персональних даних, які не відповідають дійсності, проводиться невідкладно з моменту встановлення невідповідності.

Стаття 21. Повідомлення про дії з персональними даними

1. Про передачу персональних даних третій особі володілець персональних даних протягом десяти робочих днів повідомляє суб'єкта персональних даних, якщо цього вимагають умови його згоди або інше не передбачено законом.

2. Повідомлення, зазначені у частині першій цієї статті, не здійснюються у разі:

– передачі персональних даних за запитами при виконанні завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом;

– виконання органами державної влади та органами місцевого самоврядування своїх повноважень, передбачених законом;

– здійснення обробки персональних даних в історичних, статистичних чи наукових цілях;

– повідомлення суб’єкта персональних даних відповідно до вимог частини другої статті 12 цього Закону.

3. Про зміну, видалення чи знищення персональних даних або обмеження доступу до них володілець персональних даних протягом десяти робочих днів повідомляє суб'єкта персональних даних, а також суб'єктів відносин, пов'язаних із персональними даними, яким ці дані було передано.

Стаття 22. Контроль за додержанням законодавства про захист персональних даних

1. Контроль за додержанням законодавства про захист персональних даних у межах повноважень, передбачених законом, здійснюють такі органи:

– Уповноважений;

– суди.

Стаття 23. Повноваження Уповноваженого Верховної Ради України з прав людини у сфері захисту персональних даних

1. Уповноважений має такі повноваження у сфері захисту персональних даних:

– отримувати пропозиції, скарги та інші звернення фізичних і юридичних осіб з питань захисту персональних даних та приймати рішення за результатами їх розгляду;

– проводити на підставі звернень або за власною ініціативою виїзні та безвиїзні, планові, позапланові перевірки володільців або розпорядників персональних даних в порядку, визначеному Уповноваженим, із забезпеченням відповідно до закону доступу до приміщень, де здійснюється обробка персональних даних;

– отримувати на свою вимогу та мати доступ до будь-якої інформації (документів) володільців або розпорядників персональних даних, які необхідні для здійснення контролю за забезпеченням захисту персональних даних, у тому числі доступ до персональних даних, відповідних баз даних чи картотек, інформації з обмеженим доступом;

– затверджувати нормативно-правові акти у сфері захисту персональних даних у випадках, передбачених цим Законом;

– за підсумками перевірки, розгляду звернення видавати обов'язкові для виконання вимоги (приписи) про запобігання або усунення порушень законодавства про захист персональних даних, у тому числі щодо зміни, видалення або знищення персональних даних, забезпечення доступу до них, надання чи заборони їх надання третій особі, зупинення або припинення обробки персональних даних;

– надавати рекомендації щодо практичного застосування законодавства про захист персональних даних, роз'яснювати права і обов'язки відповідних осіб за зверненням суб'єктів персональних даних, володільців або розпорядників персональних даних, структурних підрозділів або відповідальних осіб з організації роботи із захисту персональних даних, інших осіб;

– взаємодіяти із структурними підрозділами або відповідальними особами, які відповідно до цього Закону організовують роботу, пов'язану із захистом персональних даних при їх обробці; оприлюднювати інформацію про такі структурні підрозділи та відповідальних осіб;

– звертатися з пропозиціями до Верховної Ради України, Президента України, Кабінету Міністрів України, інших державних органів, органів місцевого самоврядування, їх посадових осіб щодо прийняття або внесення змін до нормативно-правових актів з питань захисту персональних даних;

– надавати за зверненням професійних, самоврядних та інших громадських об'єднань чи юридичних осіб висновки щодо проектів кодексів поведінки у сфері захисту персональних даних та змін до них;

– складати протоколи про притягнення до адміністративної відповідальності та направляти їх до суду у випадках, передбачених законом;

– інформувати про законодавство з питань захисту персональних даних, проблеми його практичного застосування, права і обов'язки суб'єктів відносин, пов'язаних із персональними даними;

– здійснювати моніторинг нових практик, тенденцій та технологій захисту персональних даних;

– організовувати та забезпечувати взаємодію з іноземними суб'єктами відносин, пов'язаних із персональними даними, у тому числі у зв'язку з виконанням Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до неї, інших міжнародних договорів України у сфері захисту персональних даних;

– брати участь у роботі міжнародних організацій з питань захисту персональних даних.

2. Уповноважений Верховної Ради України з прав людини включає до своєї щорічної доповіді про стан додержання та захисту прав і свобод людини і громадянина в Україні звіт про стан додержання законодавства у сфері захисту персональних даних.

Стаття 24. Забезпечення захисту персональних даних

1. Володільці, розпорядники персональних даних та треті особи зобов'язані забезпечити захист цих даних від випадкових втрати або знищення,

від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних.

2. В органах державної влади, органах місцевого самоврядування, а також у володільцях чи розпорядниках персональних даних, що здійснюють обробку персональних даних, яка підлягає повідомленню відповідно до цього Закону, створюється (визначається) структурний підрозділ або відповідальна особа, що організовує роботу, пов'язану із захистом персональних даних при їх обробці.

Інформація про зазначений структурний підрозділ або відповідальну особу повідомляється Уповноваженому Верховної Ради України з прав людини, який забезпечує її оприлюднення.

3. Структурний підрозділ або відповідальна особа, що організовує роботу, пов'язану із захистом персональних даних при їх обробці:

– інформує та консультує володільця або розпорядника персональних даних з питань додержання законодавства про захист персональних даних;

– взаємодіє з Уповноваженим Верховної Ради України з прав людини та визначеними ним посадовими особами його секретаріату з питань запобігання та усунення порушень законодавства про захист персональних даних.

4. Фізичні особи – підприємці, у тому числі лікарі, які мають відповідну ліцензію, адвокати, нотаріуси особисто забезпечують захист персональних даних, якими вони володіють, згідно з вимогами закону.

Стаття 25. Обмеження дії цього Закону

1. Обмеження дії статей 6, 7 і 8 цього Закону може здійснюватися у випадках, передбачених законом, наскільки це необхідно у демократичному суспільстві в інтересах національної безпеки, економічного добробуту або захисту прав і свобод суб'єктів персональних даних чи інших осіб.

2. Дозволяється обробка персональних даних без застосування положень цього Закону, якщо така обробка здійснюється:

– фізичною особою виключно для особистих чи побутових потреб;

– виключно для журналістських та творчих цілей, за умови забезпечення балансу між правом на повагу до особистого життя та правом на свободу вираження поглядів.

3. Дія цього Закону не поширюється на відносини щодо отримання архівної інформації репресивних органів.

Стаття 26. Фінансування робіт із захисту персональних даних

Фінансування робіт та заходів щодо забезпечення захисту персональних даних здійснюється за рахунок коштів Державного бюджету України та місцевих бюджетів, коштів суб'єктів відносин, пов'язаних із персональними даними.

Стаття 27. Застосування положень цього Закону

1. Положення щодо захисту персональних даних, викладені в цьому Законі, можуть доповнюватися чи уточнюватися іншими законами, за умови, що вони встановлюють вимоги щодо захисту персональних даних, що не суперечать вимогам цього Закону.

2. Професійні, самоврядні та інші громадські об'єднання чи юридичні особи можуть розробляти кодекси поведінки з метою забезпечення ефективного захисту прав суб'єктів персональних даних, додержання законодавства про

захист персональних даних з урахуванням специфіки обробки персональних даних у різних сферах. При розробленні такого кодексу поведінки або внесенні змін до нього відповідне об’єднання чи юридична особа може звернутися за висновком до Уповноваженого.

Стаття 28. Відповідальність за порушення законодавства про захист персональних даних

Порушення законодавства про захист персональних даних тягне за собою відповідальність, встановлену законом.

Стаття 29. Міжнародне співробітництво та передача персональних даних

1. Співробітництво з іноземними суб'єктами відносин, пов'язаних із персональними даними, регулюється Конституцією України, цим Законом, іншими нормативно-правовими актами та міжнародними договорами України.

2. Якщо міжнародним договором України, згода на обов'язковість якого надана Верховною Радою України, встановлено інші правила, ніж ті, що передбачені законодавством України, то застосовуються правила міжнародного договору України.

3. Передача персональних даних іноземним суб’єктам відносин, пов’язаних із персональними даними, здійснюється лише за умови забезпечення відповідною державою належного захисту персональних даних у випадках, встановлених законом або міжнародним договором України.

Держави – учасниці Європейського економічного простору, а також держави, які підписали Конвенцію Ради Європи про захист осіб у зв’язку з автоматизованою обробкою персональних даних, визнаються такими, що забезпечують належний рівень захисту персональних даних.

Кабінет Міністрів України визначає перелік держав, які забезпечують належний захист персональних даних.

Персональні дані не можуть поширюватися з іншою метою, ніж та, з якою вони були зібрані.

4. Персональні дані можуть передаватися іноземним суб’єктам відносин, пов’язаних з персональними даними, також у разі:

– надання суб’єктом персональних даних однозначної згоди на таку передачу;

– необхідності укладення чи виконання правочину між володільцем персональних даних та третьою особою – суб’єктом персональних даних на користь суб’єкта персональних даних;

– необхідності захисту життєво важливих інтересів суб’єктів персональних даних;

– необхідності захисту суспільного інтересу, встановлення, виконання та забезпечення правової вимоги;

– надання володільцем персональних даних відповідних гарантій щодо невтручання в особисте і сімейне життя суб’єкта персональних даних.

Стаття 30. Прикінцеві положення

1. Цей Закон набирає чинності з 1 січня 2011 року.

2. Установити, що в період дії воєнного стану в Україні та протягом шести місяців після його припинення чи скасування, як виняток з положень абзаців першого – третього частини третьої статті 29 цього Закону, передача персональних даних іноземним суб'єктам відносин, пов'язаних із персональними даними, що необхідні для надання медичної допомоги та/або реабілітаційної допомоги із застосуванням телемедицини, може здійснюватися із забезпеченням захисту персональних даних відповідно до законодавства тієї країни, в якій медичному працівнику, фахівцю з реабілітації чи закладу охорони здоров'я, що надає медичну та/або реабілітаційну допомогу, надано право на провадження медичної практики (крім громадян Російської Федерації та Республіки Білорусь).

3. Кабінету Міністрів України протягом шести місяців з дня набрання чинності цим Законом:

– забезпечити прийняття нормативно-правових актів, передбачених цим Законом;

– забезпечити приведення своїх нормативно-правових актів у відповідність із цим Законом.

А.7. Постанова КМУ від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури.

1. Ці Загальні вимоги визначають організаційно-методологічні, технічні та технологічні умови кіберзахисту об’єктів критичної інфраструктури, що є обов’язковими до виконання підприємствами, установами та організаціями, які відповідно до законодавства віднесені до об’єктів критичної інфраструктури.

2. У цих Загальних вимогах терміни вживаються у такому значенні:

– критичні бізнес/операційні процеси об’єкта критичної інфраструктури – процеси організації функціонування об’єктів критичної інфраструктури, реалізація загроз на які призводить до виведення з ладу або порушення функціонування самого об’єкта критичної інфраструктури та відповідно справляє негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіює майнову шкоду та/або становить загрозу для суспільства, життя і здоров’я людей; для організації функціонування цього процесу можуть використовуватися декілька інформаційно-телекомунікаційних систем;

– система інформаційної безпеки – сукупність організаційних та технічних заходів, а також засобів і методів захисту інформації, які впроваджуються на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури з метою запобігання кіберінцидентам, виявлення та захисту від кібератак, порушення конфіденційності, цілісності та доступності інформаційних ресурсів, що обробляються (передаються, зберігаються) на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури, запобігання порушенню режиму функціонування та/або недоступності служб (функцій) об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, порушенню функціонування компонентів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури; забезпечення спостережності за діями користувачів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури та функціонуванням засобів захисту об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;

– політика інформаційної безпеки – політика, що визначає підхід підприємства, установи та організації, які відповідно до законодавства віднесені до об’єктів критичної інфраструктури, до інформаційної безпеки, вимоги, правила, обмеження, рекомендації, що регламентують порядок дотримання та забезпечення інформаційної безпеки.

Інші терміни вживаються у значенні, наведеному в Законах України “Про основні засади забезпечення кібербезпеки України”, “Про захист інформації в інформаційно-телекомунікаційних системах”, Правилах забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених постановою Кабінету Міністрів України від 29 березня 2006 р. № 373 (Офіційний вісник України, 2006 р., № 13, ст. 878).

3. Кіберзахист об’єкта критичної інфраструктури забезпечується шляхом впровадження на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури комплексної системи захисту інформації або системи інформаційної безпеки з підтвердженою відповідністю.

4. Кіберзахист об’єкта критичної інфраструктури є складовою частиною робіт із створення (модернізації) та експлуатації об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури. Заходи з кіберзахисту передбачаються та впроваджуються на всіх стадіях життєвого циклу об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури.

5. Кіберзахист об’єкта критичної інфраструктури забезпечується власником та/або керівником об’єкта критичної інфраструктури відповідно до цих Загальних вимог та законодавства в сфері захисту інформації та кібербезпеки.

6. У випадку, якщо на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, положення цих Загальних вимог повинні бути враховані під час створення (модернізації) на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури комплексної системи захисту інформації, а їх відповідність перевіряється під час її державної експертизи в сфері технічного захисту інформації.

Створення комплексної системи захисту інформації об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури та її державна експертиза здійснюються відповідно до вимог законодавства в сфері захисту інформації та охорони державної таємниці.

7. У випадку, якщо на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури не обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, положення цих Загальних вимог враховуються під час створення (модернізації) системи інформаційної безпеки об’єкта критичної інфраструктури. Виконання Загальних вимог перевіряється під час незалежного аудиту інформаційної безпеки на об’єкті критичної інфраструктури.

Створення системи інформаційної безпеки об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури здійснюється відповідно до вимог технічного завдання на створення системи інформаційної безпеки.

Технічне завдання формується за результатами оцінки ризиків, які зазначаються в звіті за результатами оцінки ризиків на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури. Методичною основою для оцінки ризиків на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури є стандарт ДСТУ ISO/IEC 27005.

Власник та/або керівник об’єкта критичної інфраструктури організовує проведення незалежного аудиту інформаційної безпеки на об’єкті критичної

інфраструктури згідно з вимогами законодавства в сфері захисту інформації та кібербезпеки.

8. Власник та/або керівник об'єкта критичної інфраструктури організовує невідкладне інформування урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA (у разі наявності – галузевої команди реагування на комп'ютерні надзвичайні події), а також функціонального підрозділу контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Центрального управління СБУ (Ситуаційний центр забезпечення кібербезпеки СБУ) або відповідного підрозділу регіонального органу СБУ про кіберінциденти та кібератаки, які стосуються його об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

9. Державні органи отримують доступ до Інтернету через систему захищеного доступу державних органів до Інтернету Державного центру кіберзахисту, через операторів, провайдерів телекомунікацій, які мають захищені вузли доступу до глобальних мереж передачі даних із створеними комплексними системами захисту інформації з підтвердженою відповідністю, або через власні системи захищеного доступу до Інтернету із створеними комплексними системами захисту інформації з підтвердженою відповідністю. Ця вимога не поширюється на інформаційно-телекомунікаційні системи закордонних дипломатичних установ України.

10. Власник та/або керівник об'єкта критичної інфраструктури з метою усунення можливих наслідків кіберінцидентів та кібератак забезпечує створення резервних копій інформаційних ресурсів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури та критичних бізнес/операційних процесів об'єкта критичної інфраструктури для оперативного їх відновлення у разі пошкодження або знищення.

Державні органи для збереження резервних копій своїх інформаційних ресурсів та їх оперативного відновлення використовують основний та резервний захищений дата-центр збереження державних електронних інформаційних ресурсів Державного центру кіберзахисту.

11. Державні органи з метою здійснення захищеного інформаційного обміну, зберігання резервних копій інформаційних ресурсів, підключення до системи захищеного доступу державних органів до Інтернету Державного центру кіберзахисту використовують ресурси Національної телекомунікаційної мережі.

12. Організаційні та технічні заходи з кіберзахисту, які впроваджуються на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури, повинні забезпечувати:

– формування на об'єкті критичної інфраструктури загальної політики інформаційної безпеки;

– управління доступом користувачів та адміністраторів до об'єктів захисту об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

– ідентифікацію та автентифікацію користувачів та адміністраторів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;

– реєстрацію подій компонентами об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури та їх періодичний аудит;

– мережевий захист компонентів та інформаційних ресурсів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;

– доступність та відмовостійкість компонентів та інформаційних ресурсів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;

– визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури;

– визначення умов використання програмного та апаратного забезпечення об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;

– визначення умов розміщення компонентів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури.

Перелік базових вимог із забезпечення кіберзахисту об’єктів критичної інфраструктури, які повинні бути впроваджені під час створення комплексної системи захисту інформації (системи інформаційної безпеки) об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, наведено у додатку.

Перелік базових вимог із забезпечення кіберзахисту об’єктів критичної інфраструктури може бути доповнено відповідно до технології обробки інформації на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури, особливостей функціонування та програмно-апаратного складу об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, складу інформаційних ресурсів та компонентів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, які підлягають захисту, тощо.

Під час доповнення переліку базових вимог із забезпечення кіберзахисту об’єктів критичної інфраструктури для кожної загрози об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури передбачаються захід або комплекс заходів, що забезпечують блокування однієї чи декількох загроз або знижують ризик її реалізації, та враховуються умови функціонування об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури. У разі коли перелік мінімальних заходів не дає можливості забезпечити блокування (нейтралізацію) усіх загроз об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, повинні бути визначені додаткові заходи, які ці загрози блокують.

Формування додаткових заходів із забезпечення кіберзахисту об’єктів критичної інфраструктури розробник комплексної системи захисту інформації (системи інформаційної безпеки) об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури здійснює з урахуванням

вимог нормативних документів у сфері технічного захисту інформації, міжнародних стандартів з питань інформаційної безпеки.

13. У разі відсутності можливості виконання окремих вимог із забезпечення кіберзахисту, наведених у додатку, і/або неможливості їх застосування до окремих об'єктів захисту чи користувачів та адміністраторів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, у тому числі внаслідок їх можливого негативного впливу на функціонування об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, або неможливості їх здійснення на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури через особливості функціонування, або відсутності складу компонентів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури повинні бути розроблені і впроваджені компенсуючі заходи, що забезпечують блокування (нейтралізацію) загроз об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, або обґрунтовано виключені окремі вимоги з переліку базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури.

Власник та/або керівник об'єкта критичної інфраструктури у ході розроблення організаційних і технічних заходів щодо забезпечення кіберзахисту об'єкта критичної інфраструктури обґрунтовує застосування компенсуючих заходів або виключення окремих вимог з переліку базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури. При цьому під час проведення незалежного аудиту інформаційної безпеки об'єкта критичної інфраструктури або державної експертизи комплексної системи захисту інформації об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури має бути оцінена достатність і адекватність компенсуючих заходів, які застосовані для блокування (нейтралізації) загроз об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури та зменшення ризиків об'єкта критичної інфраструктури, або обґрунтованість виключення окремих вимог з переліку базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури.

Рішення з обґрунтуванням щодо впровадження компенсуючих заходів або виключення окремих вимог з переліку базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури оформлюється окремим рішенням за підписом власника та/або керівника об'єкта критичної інфраструктури.

14. Міністерства та інші центральні органи виконавчої влади можуть розробляти конкретизовані вимоги з кіберзахисту з урахуванням секторальної (галузевої) специфіки функціонування об'єктів критичної інфраструктури, які відносяться до сфери їх управління. Такі вимоги з кіберзахисту погоджуються з Адміністрацією Держспецзв'язку.

СБУ має право подавати міністерствам та іншим центральним органам виконавчої влади обов'язкові для розгляду пропозиції щодо таких вимог з кіберзахисту.

Додаток до Загальних вимог

ПЕРЕЛІК базових вимог із забезпечення кіберзахисту об’єктів критичної інфраструктури

Формування на об’єкті критичної інфраструктури загальної політики інформаційної безпеки

1. Об’єкт критичної інфраструктури повинен мати у своєму складі підрозділ або посадову особу з інформаційної безпеки, що відповідають за політику інформаційної безпеки, прийняту на об’єкті критичної інфраструктури, та контроль за її дотриманням. Під час визначення відповідальних за інформаційну безпеку перевага повинна надаватися особам, які мають фахову освіту та досвід роботи у сфері технічного захисту інформації або інформаційної безпеки.

Підрозділ або посадова особа з інформаційної безпеки повинні бути підпорядковані безпосередньо керівнику об’єкта критичної інфраструктури.

Функції підрозділу або посадової особи з інформаційної безпеки можуть бути покладені на службу захисту інформації підприємства, установи, організації.

2. На об’єкті критичної інфраструктури повинні бути визначені права та обов’язки всіх категорій користувачів та адміністраторів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, обов’язки адміністраторів з обслуговування компонентів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури (далі – компоненти об’єкта) та забезпечення її інформаційної безпеки, які оформлюються окремим рішенням за підписом власника та/або керівника об’єкта критичної інфраструктури.

На об’єкті критичної інфраструктури повинні бути призначені відповідальні за функціонування та інформаційну безпеку критичних бізнес/операційних процесів з числа керівників об’єкта критичної інфраструктури, працівники яких забезпечують функціонування цих критичних процесів.

3. На об’єкті критичної інфраструктури повинен бути визначений перелік інформаційних, програмних та апаратних ресурсів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, рівень їх критичності для об’єкта критичної інфраструктури та/або функціонування об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури та можливий рівень наслідків у випадку порушення конфіденційності, цілісності та доступності інформації, недоступності служб (функцій) об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, порушення функціонування компонентів об’єкта.

4. На об’єкті критичної інфраструктури повинно бути затверджено політику управління ризиками інформаційної безпеки і методику їх оцінювання та оброблення. Методичною основою для вибору методики є стандарт ДСТУ ISO/IEC 27005.

5. Власник/керівник об’єкта критичної інфраструктури зобов’язаний не рідше одного разу на рік організовувати та проводити обстеження своїх об’єктів критичної інформаційної інфраструктури об’єкта критичної інфраструктури з метою оновлення даних щодо програмно-апаратного складу об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, технології обробки інформації на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури, переліку критичних інформаційних ресурсів та компонентів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, які підлягають захисту, тощо. Методичною основою для проведення обстеження об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури є вимоги нормативного документа системи технічного захисту інформації 3.7-003-05 “Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі”.

Якщо за результатами обстеження об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури виявлено, що на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури змінено технологію обробки інформації, впроваджено нові програмні або апаратні компоненти, змінено перелік критичних інформаційних ресурсів та компонентів об’єкта, які підлягають захисту, тощо, здійснюється перегляд переліку загроз об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, ризиків інформаційної безпеки та рівня прийнятного ризику.

У випадку виявлення нових загроз та/або ризиків здійснюється оновлення технічного завдання на створення комплексної системи захисту інформації (системи інформаційної безпеки) об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, іншої документації та впровадження оновлених вимог на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури.

6. Власник/керівник об’єкта критичної інфраструктури зобов’язаний забезпечити розроблення та підтримання в актуальному стані технічної, проектної та іншої документації на комплексну систему захисту інформації (систему інформаційної безпеки) об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури (в захищеній від модифікації формі, зокрема електронній) з обов’язковим описом реалізованих у системі організаційних та технічних заходів безпеки інформації.

Мінімальний перелік документації об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури визначається в технічному завданні на створення комплексної системи захисту інформації (системи інформаційної безпеки) об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури.

Програмні та апаратні компоненти об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинні бути налаштовані відповідно до затвердженої політики інформаційної безпеки та технічної, проектної та іншої документації на комплексну систему захисту

інформації (систему інформаційної безпеки) об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури.

В інтересах національної безпеки інформація щодо програмно-апаратного складу об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, налаштування та конфігураційна інформація програмних та апаратних компонентів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, інформація про параметри та режими їх функціонування, журнали реєстрації подій (логи) та дані аудиту компонентів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, інформація про облікові записи користувачів, їх атрибути та права доступу, об’єкти захисту та їх атрибути доступу, інша інформація, яка розкриває параметри та особливості функціонування компонентів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, є інформацією з обмеженим доступом. Ступінь обмеження доступу до цієї інформації визначається відповідно до закону.

7. На об’єкті критичної інфраструктури необхідно затвердити політику інформаційної безпеки, яка визначає:

– мету та основні принципи забезпечення захисту інформаційних ресурсів, критичних бізнес/операційних процесів тощо на об’єкті критичної інфраструктури;

– опис критичних бізнес/операційних процесів, який повинен включати схему кожного критичного бізнес-процесу з описом компонентів та користувачів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, які задіяні в цьому процесі;

– вимоги до порядку визначення, надання, зміни та скасування прав доступу користувачів та адміністраторів до служб (функцій), інформації та компонентів об’єкта та порядок контролю (аудиту) використання прав доступу користувачами та адміністраторами. При цьому необхідно дотримуватися принципу надання необхідних та мінімально достатніх повноважень користувачам та адміністраторам відповідно до їх службових обов’язків;

– політику фізичної безпеки та захисту об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури від навколишнього природного середовища;

– вимоги до забезпечення інформаційної безпеки під час взаємодії з постачальниками;

– політику управління обліковими записами в програмному та апаратному забезпеченні об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури. Політика повинна визначати порядок створення, блокування та зупинення облікових записів користувачів та адміністраторів в компонентах об’єкта;

– вимоги до порядку формування, надання, скасування та контролю (аудиту) за використанням автентифікаційних атрибутів користувачів та адміністраторів, у тому числі зовнішніх носіїв автентифікаційних даних, для доступу до служб (функцій), інформації та компонентів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури. Повинні бути

визначені також вимоги до складності паролів, періодичності їх зміни, блокування роботи користувача за певної кількості спроб підбору пароля, порядок поводження із зовнішніми носіями автентифікаційних даних тощо;

– політику забезпечення безперебійної роботи об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, зокрема порядок резервування даних та компонентів об’єкта, зберігання резервних копій даних, відновлення даних з резервних копій та заміни компонентів об’єкта у випадку виходу їх з ладу тощо;

– порядок дій персоналу об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури у випадках відмов або збоїв об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури в цілому або окремих його компонентів;

– порядок використання змінних (зовнішніх) пристроїв та носіїв інформації на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури;

– політику мережевого захисту, зокрема щодо сегментації мережі об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, захисту від вірусів, зловмисного коду, шкідливого програмного забезпечення, встановлення та налаштування засобів мережевого захисту тощо;

– політику проведення модернізації (оновлення) компонентів об’єкта, внесення змін до складу та в налаштування компонентів об’єкта. Повинні бути визначені відповідальні особи, які мають право проводити ці робити, а також порядок дотримання політики безпеки, яка прийнята на об’єкті критичної інфраструктури, під час проведення таких робіт;

– опис критичних бізнес/операційних процесів, який повинен включати схему кожного критичного бізнес-процесу з описом компонентів та користувачів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, які задіяні в цьому процесі;

– політику управління оновленнями (порядок отримання, перевірки, розповсюдження та застосування оновлень програмного забезпечення компонентів об’єкта);

– політику реєстрації та аудиту подій, що реєструються компонентами об’єкта. Політика повинна містити перелік подій, які реєструються кожним компонентом об’єкта, параметри ведення журналів (логів) реєстрації подій та їх архівування, порядок та періодичність аудиту журналів (логів) реєстрації подій адміністраторами об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури на предмет виявлення ознак кібератак або кіберінцидентів;

– політику управління інцидентами кібербезпеки, яка повинна містити перелік подій, що кваліфікуються як кіберінциденти, описи дій користувачів та адміністраторів у разі їх виникнення, порядок інформування посадових осіб об’єкта критичної інфраструктури, урядової команди реагування на комп’ютерні надзвичайні події України CERT-UA (у разі наявності – галузевої команди реагування на комп’ютерні надзвичайні події);

– політику використання електронної пошти користувачами об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;

– політику проведення внутрішнього аудиту інформаційної безпеки об’єкта критичної інфраструктури.

Політика інформаційної безпеки може затверджуватися окремими рішеннями за підписом власника та/або керівника об’єкта критичної інфраструктури. Повинен бути встановлений порядок внесення змін до таких документів.

8. Вимоги затвердженої на об’єкті критичної інфраструктури політики інформаційної безпеки повинні бути доведені під підпис або в інший спосіб до всіх його працівників. На об’єкті критичної інфраструктури повинна бути визначена відповідальність його співробітників за порушення встановленої політики інформаційної безпеки.

9. Власник/керівник об’єкта критичної інфраструктури повинен впровадити програми підвищення обізнаності/навчання працівників з питань інформаційної безпеки та забезпечити щорічний контроль рівня обізнаності.

10. У підрозділі або посадової особи з інформаційної безпеки об’єкта критичної інфраструктури повинен бути створений та підтримуватися в актуальному стані перелік програмного та апаратного забезпечення, що використовується на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури в захищеній від модифікації формі, зокрема електронній.

Управління доступом користувачів та адміністраторів до об’єктів захисту об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури

11. Механізм розподілу прав доступу до об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинен:

– охоплювати всі інформаційні ресурси об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури (інформацію, яка зберігається та обробляється на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури, технологічну інформацію програмного та апаратного забезпечення об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, журнали реєстрації подій тощо);

– визначати права на виконання операцій для всіх користувачів та адміністраторів (за необхідності також активних процесів) над інформаційними ресурсами об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури (читання, модифікація, створення, видалення тощо);

– за необхідності також визначати права доступу користувачів та адміністраторів до служб (функцій) об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури.

12. За можливості реалізації на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинна надаватися перевага централізованому поширенню інформації щодо налаштувань прав та атрибутів доступу, параметрів реєстрації подій, інших параметрів безпеки та системних налаштувань компонентів об’єкта.

Ідентифікація та автентифікація користувачів та адміністраторів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури

13. Користувачі та адміністратори об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури (за необхідності також активні процеси) повинні отримувати доступ до служб (функцій), інформації та компонентів об’єкта в межах визначених їм прав доступу тільки після успішного проходження процедури автентифікації на підставі унікального персоніфікованого ідентифікатора (імені) користувача і деякої інформації, що вводиться користувачем (пароль), та/або фізичного ідентифікатора, що надається користувачем (ключ, сертифікат, токен тощо).

14. Засоби об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинні надавати можливість ідентифікації кожної операції користувача та адміністратора на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури та їх протоколювання в журналах реєстрації подій.

15. Для надання доступу до служб (функцій) та інформації об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинна використовуватися багатофакторна автентифікація користувачів та адміністраторів. Допускається використання двофакторної автентифікації тільки в тому програмному забезпеченні компонентів об’єкта, яке не підтримує багатофакторну автентифікацію.

16. На об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинні бути заблоковані або змінені облікові записи адміністраторів та їх паролів, встановлені за замовчуванням, в усіх компонентах об’єкта. Забороняється використовувати облікові записи та паролі за замовчуванням в програмному та апаратному забезпеченні об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури.

17. На об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинні бути видалені або заблоковані неперсоналізовані і гостьові облікові записи користувачів і адміністраторів та використовуватися виключно персоналізовані облікові записи користувачів і адміністраторів в усіх компонентах об’єкта. Під час звільнення з посади працівника його обліковий запис повинен бути негайно заблокований або видалений в усіх компонентах об’єкта.

18. Обладнання, яке підключається до системи управління технологічними процесами об’єкта критичної інфраструктури, повинно бути ідентифіковане (наприклад, за IP-адресою, MAC-адресою тощо), а також повинні бути вжиті заходи, які унеможливлюють роботу обладнання в мережі без відповідної ідентифікації.

Реєстрація подій компонентами об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури та їх періодичний аудит

19. Компоненти об’єкта повинні забезпечити реєстрацію, збереження в електронних журналах та захист від модифікації інформації щонайменше про такі події:

– доступ та дії з інформацією, яка зберігається та обробляється на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури, а також з налаштуваннями програмного та апаратного забезпечення об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, журналами реєстрації подій тощо (читання, модифікація, створення, видалення тощо);

– реєстрація подій, пов’язаних із встановленням та зміною прав доступу до служб (функцій), інформації та компонентів об’єкта;

– вхід/вихід користувачів та адміністраторів в/із компонентів об’єкта;

– невдалі спроби входу користувачів та адміністраторів на об’єкт критичної інформаційної інфраструктури об’єкта критичної інфраструктури та перевищення граничної кількості спроб введення пароля;

– реєстрація, видалення (блокування) облікових записів користувачів та адміністраторів у компонентах об’єкта;

– зміна пароля користувача в компонентах об’єкта;

– реєстрація подій, пов’язаних із зміною конфігураційних налаштувань компонентів об’єкта;

– спроби здійснення несанкціонованого доступу до ресурсів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;

– негативні результати перевірок цілісності даних та програмного і апаратного забезпечення об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;

– всі дії адміністратора з журналами реєстрації подій компонентів об’єкта та налаштування ним параметрів реєстрації.

– Повний перелік подій, які реєструються компонентами об’єкта, визначається виходячи із встановленої на об’єкті критичної інфраструктури політики інформаційної безпеки.

20. Журнали реєстрації подій компонентів об’єкта повинні містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнали реєстрації повинні містити інформацію, достатню для встановлення користувача, процесу і мережевого об’єкта, що мали відношення до кожної зареєстрованої події.

21. Має бути забезпечений захист журналів реєстрації подій компонентів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури від несанкціонованого доступу, модифікації або руйнування. Електронні журнали реєстрації подій повинні зберігатися не менше ніж один рік з дати реєстрації останньої події.

22. На об’єкті критичної інфраструктури повинно бути впроваджено систему збору та аналізу журналів реєстрації подій програмного та апаратного забезпечення об’єкта критичної інформаційної інфраструктури об’єкта

критичної інфраструктури. Така система повинна мати можливість встановлення фільтрів, які дозволяють робити вибірку і аналіз журналів та подій за різними критеріями та за потреби мати інтерфейси обміну з іншими системами.

Оброблення журналів реєстрації подій не повинно впливати на функціонування критичних бізнес/операційних процесів об'єкта критичної інфраструктури.

23. На об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури повинна бути забезпечена можливість роботи з архівними журналами реєстрації подій за попередні періоди шляхом завантаження журналів на об'єкт критичної інформаційної інфраструктури об'єкта критичної інфраструктури із зовнішнього джерела. При цьому дані, що завантажуються, повинні тільки доповнювати існуючі журнали, але не затирати і не змінювати інформації, що вже зберігається в них.

Архівні журнали реєстрації подій зберігаються на фізично відокремленому компоненті об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури або окремому носії даних не менше року з дати їх утворення.

Забезпечення мережевого захисту компонентів та інформаційних ресурсів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури

24. На об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури повинні використовуватися засоби захисту від зловмисного коду, шкідливого програмного забезпечення та вірусів. Повинно бути забезпечене централізоване управління засобами захисту від зловмисного коду, шкідливого програмного забезпечення та вірусів.

25. Доступ адміністраторам до компонентів об'єкта повинен надаватися виключно з IP-адрес (робочих станцій), які визначені для адміністрування об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

26. У разі неможливості фізичного розділення зовнішньої мережі та об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури на межі (периметрі) між зовнішніми мережами, іншими інформаційно-телекомунікаційними системами, що обслуговують об'єкт критичної інфраструктури, та об'єктом критичної інформаційної інфраструктури об'єкта критичної інфраструктури повинні бути встановлені засоби мережевого захисту, що виконують щонайменше такі функції захисту:

– захист від атак "нульового дня" (вразливості програмного забезпечення, які ще невідомі користувачам чи розробникам програмного забезпечення та проти яких ще не розроблені механізми захисту), виявлення зловмисного коду та шкідливого програмного забезпечення;

– фільтрація трафіку та розмежування доступу між мережею об'єкта критичної інфраструктури та зовнішніми мережами за критеріями дозволених та заборонених служб, протоколів, портів, мережевих адрес, мережевих з'єднань, небажаних веб-сайтів тощо. Блокування трафіку та з'єднань, які не відповідають визначеним критеріям;

– фільтрація та аналіз трафіку за визначеними відповідно до політики інформаційної безпеки критеріями;

– моніторинг трафіку на наявність зловмисного коду, вірусів зловмисного програмного забезпечення та за іншими визначеними відповідно до політики інформаційної безпеки критеріями;

– виявлення та запобігання атакам та вторгненням, спрямованим на програмні та апаратні компоненти та інформацію об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

– захист від атак типу "відмова в обслуговуванні";

– захист від несанкціонованого доступу через Інтернет;

– балансування навантаження;

– маскування структури і мережевих адрес мережі;

– завершення з'єднання з вузлом у разі атаки;

– здійснення реєстрації подій, що мають відношення до безпеки.

Для захисту об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури повинні використовуватися програмно-апаратні засоби, потужність яких визначається виходячи із потужності трафіку, який передбачається в мережі, з урахуванням його потенційного збільшення.

27. На об'єкті критичної інфраструктури необхідно здійснити розподіл об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури на фізичному та/або логічному рівні (сегментацію мережі) і обмежити доступ між сегментами мережі з використанням міжмережевих екранів або аналогічних за функціональністю засобів мережевого захисту.

28. Реалізована архітектура об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури повинна надавати можливість розподілу мережі щонайменше на такі частини / зони:

– зовнішня зона (DMZ-zone): зона із зовнішніми діапазонами адресації мережі для розміщення зовнішніх (публічних) інформаційних ресурсів та сервісів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

– зона прикладних застосувань об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури (APP-zone): захищена внутрішня зона із внутрішньою адресацією, призначена для розміщення серверів застосувань, доступна для виконання функціональних запитів користувачів інформаційних сервісів;

– зона сховищ даних об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури (DB-zone): захищена внутрішня зона із внутрішньою адресацією, призначена для розміщення баз даних, для доступу за запитами прикладних застосувань зони (APP-zone);

– зона прикладних застосувань системи безпеки (Security-zone): захищена внутрішня зона із внутрішньою адресацією, призначена для розміщення сервісів та служб захисту інформації;

– тестова зона (Test-zone): захищена внутрішня зона із внутрішньою адресацією, призначена для тестування нових компонентів та/або оновлень програмного та апаратного забезпечення об'єкта критичної інформаційної

інфраструктури об’єкта критичної інфраструктури, перед тим як впровадити їх в промислову експлуатацію на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури.

29. Сервери та обладнання, що забезпечують функціонування сервісів та віддалений доступ клієнтів / користувачів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури із зовнішніх мереж, повинні бути розміщені в зовнішній зоні об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури. З’єднання серверів та обладнання, які розміщені в зовнішній зоні, із серверами та обладнанням внутрішньої мережі об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинні захищатися міжмережевим екраном.

30. Робочі станції, з яких виконуються дії щодо адміністрування програмного та апаратного забезпечення об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, а також серверні частини засобів захисту інформації повинні бути розміщені в зоні прикладних застосувань системи безпеки (Security-zone) мережі, захищеної за допомогою міжмережевого екрана.

31. Сегмент інформаційної інфраструктури об’єкта критичної інфраструктури, в якому перебуває система керування технологічними процесами, повинен бути відокремленим від інших систем об’єкта критичної інфраструктури. У випадку логічного відокремлення на межі сегмента повинен бути встановлений міжмережевий екран.

32. Повинні бути визначені та відключені (заблоковані) програмні порти компонентів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, які є небезпечними для забезпечення кібербезпеки.

33. Власник/керівник об’єкта критичної інфраструктури зобов’язаний проводити перевірку ефективності заходів щодо захисту об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури від зовнішнього проникнення шляхом виконання періодичних (не рідше одного разу на рік) тестів на проникнення (Penetration test). У разі отримання негативних результатів після проведення тестів необхідно вжити заходів для усунення їх причин.

34. На об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури передача даних бездротовими мережами повинна здійснюватися виключно захищеними з’єднаннями із забезпеченням її конфіденційності та цілісності. Забороняється використання на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури технологій Wi-Fi та Bluetooth.

35. Для захисту даних, які передаються через незахищене середовище між віддаленими користувачами, адміністраторами та об’єктом критичної інформаційної інфраструктури об’єкта критичної інфраструктури, між компонентами об’єкта (поза контрольованою територією об’єкта критичної інфраструктури), між об’єктом критичної інформаційної інфраструктури об’єкта критичної інфраструктури та іншими (зовнішніми) інформаційно-телекомунікаційними системами, необхідно використовувати захищені з’єднання із забезпеченням конфіденційності та цілісності цих даних.

36. Систему управління технологічними процесами об’єкта інфраструктури дозволяється підключати до глобальних мереж передачі даних, зокрема до Інтернету, тільки у випадку неможливості функціонування технологічного процесу без підключення до Інтернету та за умови впровадження всіх заходів захисту відповідно до Загальних вимог до кіберзахисту об’єктів критичної інфраструктури або конкретизованих вимог з кіберзахисту з урахуванням секторальної (галузевої) специфіки функціонування об’єкта критичної інфраструктури, який відноситься до відповідної сфери управління.

37. До глобальних мереж передачі даних, зокрема Інтернету, об’єкти критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинні підключатися через тих операторів, провайдерів телекомунікацій, які мають захищені вузли доступу до глобальних мереж передачі даних із створеними комплексними системами захисту інформації з підтвердженою відповідністю. У договорі з надавачем цих послуг зазначаються зобов’язання щодо виконання тієї частини Загальних вимог до кіберзахисту об’єктів критичної інфраструктури, які він надає об’єкту критичної інформаційної інфраструктури об’єкта критичної інфраструктури, та наявність комплексної системи захисту інформації з підтвердженою відповідністю.

Забезпечення доступності та відмовостійкості компонентів та інформаційних ресурсів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури

38. Інформаційна інфраструктура об’єкта критичної інфраструктури повинна будуватися на базі відмовостійкого підходу. Для забезпечення відмовостійкості об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинно здійснюватися, як мінімум, таке:

– періодичне створення резервних копій інформаційних ресурсів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури та критичних бізнес/операційних процесів об’єкта критичної інфраструктури, включаючи інформацію, яка зберігається на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури, технологічну інформацію компонентів об’єкта та образів серверів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, а також їх відновлення у випадку втрати або пошкодження;

– резервування критичних для функціонування об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури та бізнес/операційних процесів об’єкта критичної інфраструктури програмних та апаратних компонентів для забезпечення його сталого функціонування у випадку виходу з ладу одного з критичних компонентів. У разі використання на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури віртуальних серверів необхідно забезпечити їх резервування;

– дублювання (кластеризація) критичних для функціонування об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури та бізнес/операційних процесів об’єкта критичної інфраструктури програмних та апаратних компонентів об’єкта для забезпечення його сталого функціонування, зниження навантаження та збільшення продуктивності;

– використання засобів балансування навантаження;

– використання джерел безперебійного живлення для критичних компонентів об’єкта;

– зв’язок з Інтернетом з використанням двох та більше каналів передачі даних, які надаються різними операторами мережі передачі даних (провайдерами), – для об’єкта критичної інфраструктури, які надають свої послуги через Інтернет.

39. Під час розроблення, модернізації або оновлення компонентів системи управління технологічними процесами об’єкта критичної інфраструктури необхідно використовувати тестову програмно-апаратну платформу, яка підключена до окремого (тестового) виділеного сегмента його мережі для тестування нових компонентів та/або оновлень програмного та апаратного забезпечення, перед тим як впровадити їх в промислову експлуатацію.

Визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури

40. На об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинна проводитися перевірка всіх змінних (зовнішніх) пристроїв та носіїв інформації перед кожним їх використанням на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури засобами захисту від зловмисного коду, шкідливого програмного забезпечення та вірусів.

41. На об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинна здійснюватися ідентифікація всіх змінних (зовнішніх) пристроїв та носіїв інформації за допомогою унікального ідентифікатора.

Повинно бути унеможливлено використання змінних (зовнішніх) пристроїв та носіїв інформації, які не зареєстровані на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури.

42. На об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинно бути відключено автоматичний запуск програм із змінних (зовнішніх) пристроїв та носіїв інформації.

43. Порти компонентів мережевого обладнання, робочих станцій та серверів, які не використовуються, мають бути заблоковані адміністраторами об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури.

Визначення умов використання програмного та апаратного забезпечення об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури

44. На об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинна проводитися перевірка на цілісність та автентичність оновлень компонентів об’єкта. У разі порушення цілісності або непідтвердження автентичності оновлення воно повинно бути відхилене і не повинно застосовуватися, а цю подію необхідно запротоколювати в журналі подій.

45. У складі об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинно використовуватися програмне та апаратне забезпечення, для якого не припинено підтримку виробника. Повинні використовуватися офіційні стабільні версії прикладного програмного забезпечення та драйверів.

На об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинна надаватися перевага програмному забезпеченню, яке має більш вищий рівень гарантій відповідно до нормативного документа системи технічного захисту інформації 2.5-004-99 “Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу”, за результатами державної експертизи у сфері технічного захисту інформації.

46. На об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинно блокуватися самостійне встановлення або видалення користувачами програмного забезпечення на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури. Право на встановлення або видалення програмного забезпечення повинен мати тільки уповноважений адміністратор.

47. Засоби об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинні забезпечувати неприйняття файла/повідомлення в обробку у разі отримання негативного результату перевірки електронного підпису файла/повідомлення, що надійшов/надійшло. Ця подія повинна відображатися в журналі реєстрації подій.

48. Програмні та апаратні засоби, які використовуються у складі об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, не повинні мати походження з іноземної держави, до якої застосовано санкції згідно із Законом України “Про санкції”, чи бути розроблені/виготовлені юридичною особою – резидентом такої іноземної держави або юридичною особою, частка статутного капіталу якої перебуває у власності зазначеної іноземної держави, або юридичною особою, яка перебуває під контролем юридичної особи такої іноземної держави.

Визначення умов розміщення компонентів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури

49. Компоненти та/або інформація об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, крім систем управління технологічними процесами, можуть перебувати в сторонньому (не власному) центрі обробки даних тільки за умови, що центр обробки даних розташований на території України (за винятком тимчасово окупованої території України), а власником центру обробки даних є резидент України. При цьому у договорі із центром обробки даних повинні зазначатися його зобов’язання щодо виконання тієї частини Загальних вимог до кіберзахисту об’єктів критичної інфраструктури, які він надає об’єкту критичної інфраструктури.

Компоненти та інформація (дані) систем управління технологічними процесами об’єкта критичної інфраструктури повинні бути розміщені тільки у власному центрі обробки даних.

50. З метою створення резервних копій своїх інформаційних ресурсів та їх оперативного відновлення у разі пошкодження або знищення державні органи використовують основний та резервний захищений дата-центр збереження державних електронних інформаційних ресурсів Державного центру кіберзахисту.

51. Компоненти об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинні розміщуватися у приміщеннях, які унеможливлюють несанкціонований фізичний доступ до них сторонніх осіб.

Повинен бути забезпечений контрольований фізичний доступ до приміщень та/або комутаційних шаф, де розташовані робочі станції, сервери, мережеві компоненти та комутаційні вузли структурованої кабельної системи об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури.

52. Забороняється підключати робочі місця адміністраторів та операторів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури до інших інформаційно-телекомунікаційних систем.

53. Схеми (креслення) розміщення обладнання структурованої кабельної системи та кабельних каналів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, схеми підключення обладнання, таблиці маркування кабелів структурованої кабельної системи та кабельних з’єднань зберігаються в актуальному стані.

А.8. ДСТУ 3396.0,1,2-97

ДСТУ 3396.0-96. Державний стандарт України. Захист інформації. Технічний захист інформації. Основні положення

Чинний від 1997-01-01

1 ГАЛУЗЬ ВИКОРИСТАННЯ

Цей стандарт установлює об'єкт захисту, мету, основні організаційно-технічні положення технічного захисту інформації (ТЗІ), неправомірний доступ до якої може завдати шкоди громадянам, організаціям (юридичним особам) та державі, а також категорії нормативних документів з ТЗІ.

Вимоги стандарту обов'язкові для підприємств та установ усіх форм власності і підпорядкування, громадян – суб'єктів підприємницької діяльності, органів державної влади, органів місцевого самоврядування, військових частин усіх військових формувань, представництв України за кордоном, які володіють, користуються та розпоряджаються інформацією, що підлягає технічному захисту.

Видання офіційне

2 НОРМАТИВНІ ПОСИЛАННЯ

У цьому стандарті наведено посилання на такі документи:

ДСТУ 1.0-93 Державна система стандартизації України. Основні положення;

ДСТУ 1.2-93 Державна система стандартизації України. Порядок розроблення державних стандартів;

ДСТУ 1.3-93 Державна система стандартизації України. Порядок розроблення, побудови, викладу, оформлення, узгодження, затвердження, позначення та реєстрації технічних умов;

ДСТУ 1.4-93 Державна система стандартизації України. Стандарт підприємства. Основні положення;

ДСТУ 1.5-93 Державна система стандартизації України. Загальні вимоги до побудови, викладу, оформлення і змісту стандартів;

ДБН А. 1.1 – і-93 Система стандартизації та нормування в будівництві. Основні положення;

ДБН А.1.1-2-93 Система стандартизації та нормування в будівництві. Порядок розробки, вимоги до побудови, викладу та оформлення нормативних документів.

3 ЗАГАЛЬНІ ПОЛОЖЕННЯ

3.1 Об'єктом технічного захисту с інформація, що становить державну або іншу передбачену законодавством України таємницю, конфіденційна інформація, що є державною власністю чи передана державі у володіння, користування, розпорядження (далі інформація з обмеженим доступом – ІзОД).

3.2 Об'єкт захисту, мету і завдання ТЗІ визначають і встановлюють особи, які володіють, користуються, розпоряджаються ІзОД у межах прав і повноважень, наданих законами України, підзаконними актами та нормативними документами з ТЗІ.

3.3 Носіями ІзОД можуть бути фізичні поля, сигнали, хімічні речовини, що утворюються в процесі інформаційної діяльності, виробництва й експлуатації продукції різного призначення (далі інформаційна діяльність).

3.4 Середовищем поширення носіїв ІзОД можуть бути лінії зв'язку, сигналізації, керування, енергетичні мережі, прикінцевеі проміжне обладнання, інженерні комунікації і споруди, відгороджувалі ні будівельні конструкції, а також світлопроникні елементи будинків і споруд (отвори), повітряне, водне та інше середовища, грунт, рослинність тощо.

3.5 Витік або порушення цілісності ІзОД (спотворення, модифікація, руйнування, знищення) можуть бути результатом реалізації загроз безпеці інформації (далі-загроза).

3.6 Метою ТЗІ с запобігання витоку або порушенню цілісності ІзОД.

3.7 Мста ТЗІ може бути досягнута побудовою системи захисту інформації, що є організованою сукупністю методів і засобів забезпечення ТЗІ.

Технічний захист інформації здійснюється поетапно:

1 етап – визначення й аналіз загроз;

2 етап – розроблення системи захисту інформації;

3 етап – реалізація плану захисту інформації;

4 етап – контроль фукціювання та керування системою захисту інформації.

4 ПОБУДОВА СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

4.1 Визначення й аналіз загроз

4.1.1 На першому етапі необхідно здійснити аналіз об'єктів захисту, ситуаційного плану, умов функціювання підприємства, установи, організації, оцінити ймовірність прояву загроз та очікувану шкоду під їх реалізації, підготувати засадничі дані для побудови окремої моделі загроз.

4.1.2 Джерелами загроз може бути діяльність іноземних розвідок, а також навмисні або ненавмисні дії юридичних і фізичних осіб.

4.1.3 Загрози можуть здійснюватися:

— технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо-, радіотехнічні, хімічні та інші канали;

— каналами спеціального впливу шляхом формування полів і сигналів з мстою руйнування системи захисту або порушення цілісності інформації;.

— несанкційованим доступом шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту для використання інформації або нав'язування хибної інформації, застосування підкладних пристроїв чи програм та вкорінення комп'ютерних вірусів.

4.1.4 Опис загроз і схематичне подання шляхів їх здійснення складають окрему модель загроз.

4.2 Розроблення системи захисту інформації

4.2.1 На другому етапі слід здійснити розроблення плану ТЗІ, що містить організаційні, первинні технічні та основні технічні заходи захисту ІзОД, визначити зони безпеки інформації.

Організаційні заходи регламентують порядок інформаційної діяльності з урахуванням норм і вимог ТЗІ для всіх періодів життевого циклу об'єкта захисту.

Первинні технічні заходи передбачають захист інформації блокуванням загроз без використання засобів ТЗІ.

Основні технічні заходи передбачають захист інформації з використанням засобів забезпечення ТЗІ.

4.2.2 Для технічного захисту інформації слід застосовувати спосіб приховування або спосіб технічної дезінформації.

4.2.3 Заходи захисту інформації повинні:

— бути відповідними загрозам;

— бути розробленими з урахуванням можливої шкоди від їх реалізації і вартості захисних заходів та обмежень, що вносяться ними;

— забезпечувати задану ефективність захисту інформації на встановленому рівні протягом часу обмеження доступу до неї або можливості здійснення загроз.

4.2.4 Рівень захисту інформації означується системою кількісних та якісних показників, які забезпечують розв'язання завдання захисту інформації на основі норм та вимог ТЗІ.

4.2.5 Мінімально необхідний рівень захисту інформації забезпечують обмежувальними і фрагментарними заходами протидії найнебезпечнішій загрозі.

Підвищення рівня захисту інформації досягається нарощуванням технічних заходів протидії безлічі загроз.

4.2.6 Порядок розрахунку та інструментального визначення зон безпеки інформації, реалізації заходів ТЗІ, розрахунку ефективності захисту та порядок атестації технічних засобів забезпечення інформаційної діяльності, робочих місць (приміщень) установлюються нормативними документамиз ТЗІ

4.3 Реалізація плану захисту інформації

4.3.1 На третьому етапі слід реалізувати організаційні, первинні технічні та основні технічні заходи захисту ІзОД, установити необхідні он» Безпеки інформації, провести атестацію технічних засобів забезпечення інформаційної діяльності, робочих місць (приміщені.) на відповідність вимогам безпеки інформації.

4.3.2 Технічний захист інформації забезпечується застосуванням захищених програм і технічних засобів забезпечення інформаційної діяльності, програмних і технічних засобів захисту інформації (далі – засоби ТЗІ) та засобів контролю, які мають сертифікат відповідності вимогам нормативних документів з технічного захисту системи УкрСЕПРО або дозпіл на їх використання від органу, уповноваженого Кабінетом Міністрів України, а також застосуванням спеціальних інженерно-технічних споруд, засобів і систем (далізасоби забезпечення ТЗІ).

4.3.3 Засоби ТЗІ можуть функціюватн автономно або спільно з технічними засобами забезпечення інформаційної діяльності у вигляді самостійних пристроїв або вбудованих у них складових елементів.

4.3.4 Склад засобів забезпечення ТЗІ, перелік їх постачальників, а також послуг з установлення, монтажу, налагодження та обслуговування визначаються особами, які володіють, користуються і розпоряджаються ІзОД самостійно або за рекомендаціями спеціалістів з ТЗІ згідно з нормативними документами з ТЗІ.

4.3.5 Надання послуг з ТЗІ, атестацію та сервісне обслуговування засобів забезпечення ТЗІ можуть здійснювати юридичні і фізичні скоби, які мають ліцензію на право проведення цих робіт, видану органом, уповноваженим Кабінетом Міністрів України.

4.4 Контроль функціювання та керування системою захисту ін формації

4.4.1 На четвертому етапі слід провести аналіз функціювання системи захисту інформації, перевірку виконання заходів ТЗІ, контроль ефективності захисту, підготувати та видати засадничі дані для керування системою захисту інформації.

4.4.2 Керування системою захисту інформації полягає у адаптації заходів ТЗІ до поточного завдання захисту інформації.

За фактами зміни умов здійснення або виявлення нових загроз заходи ТЗІ реалізуються у найкоротший строк.

4.4.3 У разі потреби підвищення рівня захисту інформації необхідно виконати роботи, передбачені 1, 2 та 3 етапами побудови системи захисту інформації.

4.4.4 Порядок проведення перевірок і контролю ефективності захисту інформації встановлюється нормативними документами з ТЗІ.

5 НОРМАТИВНІ ДОКУМЕНТИ З ТЗІ

5.1 Нормативні документи розробляються в ході проведення комплексу робіт із стандартизації та нормування у галузі ТЗІ..

5.2 Нормативні документи повинні забезпечувати:

— проведення єдиної технічної політики;

— створення і розвиток сдиної термінологічної системи;

— функціювання багаторівневих систем захисту інформації на основі взаємнопогодженнх положень, правил/методик, вимог та норм;

— функціювання систем сертифікації, ліцензування й атестації згідно з вимогами безпеки інформації;

— розвиток сфери послуг у галузі ТЗІ;

— установлення порядку розроблення, виробництва, експлуатації засобів забезпечення ТЗІ;

— організацію проектування будівельних робіт у частині забезпечення ТЗІ;

— підготовку та перепідготовку кадрів у системі ТЗІ.

5.3 Нормативні документи з ТЗІ поділяються на:

— нормативні документи із стандартизації у галузі ТЗІ;

— державні стандарти та прирівняні до них нормативні документи;

— нормативні акти міжвідомчого значення, шо реєструються у Міністерстві юстиції України;

— нормативні документи міжвідомчого значення технічного характеру, то реєструються органом, уповноваженим Кабінетом Міністрів України;

— нормативні документи відомчого значення органів державної влади та органів місцевого самоврядування.

5.4 Порядок проведення робіт із стандартизації та нормування у галузі ТЗІ встановлюється ДСТУ І 0, ДОН А.І.І-І, документами системи ТЗІ.

5.5 Порядок розроблення, оформлення, погодження, затвердження, реєстрації, видання, впровадження, перевірки, перегляду, зміни та скасування нормативних документів установлюється ДСТУ 1.2, ДСТУ І.З, ДСТУ 1.4, ДСТУ 1.5.ДБН А. 1.1-2, документами системи ТЗІ.

ДСТУ 3396.1-96. Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт

Чинний від 01.07.1997 р.

1 Галузь використання

Цей стандарт установлює вимоги до порядку проведення робіт з технічного захисту інформації (ТЗІ).

Вимоги стандарту обов`язкові для підприємств та установ усіх форм власності й підпорядкування, громадян-суб`єктів підприємницької діяльності, органів державної влади, органів місцевого самоврядування, військових частин усіх військових формувань, представництв України за кордоном, які володіють, користуються та розпоряджаються інформацією, що підлягає технічному захисту.

2. Нормативні посилання

У цьому стандарті наведено посилання на такий стандарт: ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.

3 Загальні положення

3.1 Інформація з обмеженим доступом (ІзОД) в процесі інформаційної діяльності (ІД), основними видами якої є одержання, використання, поширення та зберігання ІзОД, може зазнавати впливу загроз її безпеці (далі – загроза), у результаті чого може відбутися її витік або порушення цілісності інформації.

Схильність ІзОД до впливу загроз визначає її вразливість.

Здатність системи захисту інформації протистояти впливу загроз визначає захищеність ІзОД.

3.2 Можливі такі варіанти захисту інформації:

– досягнення необхідного рівня захисту ІзОД за мінімальних затрат і допустимого рівня обмежень видів ІД;

– досягнення необхідного рівня захисту ІзОД за допустимих затрат і заданого рівня обмежень видів ІД;

– досягнення максимального рівня захисту ІзОД за необхідних затрат і мінімального рівня обмежень видів ІД.

Захист інформації, яка не є державною таємницею, забезпечується, як правило, застосуванням першого чи другого варіанту.

Захист інформації, яка становить державну таємницю, забезпечується, як правило, застосуванням третього варіанту.

3.3 Зміст та послідовність робіт з протидії загрозам або їхньої нейтралізації повинні відповідати зазначеним в ДСТУ 3396.0-96 етапам функціювання системи захисту інформації і полягає в:

– проведенні обстеження підприємства, установи, організації (далі – підприємство);

– розробленні і реалізації організаційних, первинних технічних, основних технічних заходів з використанням засобів забезпечення ТЗІ (додаток А);

– прийманні робіт з ТЗІ;

– атестації засобів (систем) забезпечення ІД на відповідність вимогам нормативних документів з ТЗІ.

3.4 Порядок проведення робіт з ТЗІ або окремих їхніх етапів установлюється наказом (розпорядженням) керівника підприємства.

Роботи повинні виконуватися силами підприємства під керівництвом спеціалістів з ТЗІ.

Для участі в роботах, подання методичної допомоги, оцінювання повноти та якості реалізації заходів захисту можуть залучатися спеціалісти з ТЗІ інших організацій, які мають ліцензію органа, уповноваженого Кабінетом Міністрів України.

4 Організація проведення обстеження

4.1 Метою обстеження підприємства є вивчення його ІД, визначення об`єктів захисту – ІзОД, виявлення загроз, їхній аналіз та побудова окремої моделі загроз.

4.2 Обстеження повинно бути проведено комісією, склад якої визначається відповідальною за ТЗІ особою і затверджується наказом керівника підприємства.

4.3 У ході обстеження необхідно:

– провести аналіз умов функціювання підприємства, його розташування на місцевості (ситуаційного плану) для визначення можливих джерел загроз;

– дослідити засоби забезпечення ІД, які мають вихід за межі контрольованої території;

– вивчити схеми засобів і систем життєзабезпечення підприємства (електроживлення, уземлення, автоматизації, пожежної та охоронної сигналізацій), а також інженерних комунікацій та металоконструкцій;

– дослідити інформаційні потоки, технологічні процеси передачі, одержання, використання, розповсюдження і зберігання (далі – оброблення) інформації і провести необхідні вимірювання;

– визначити наявність та технічний стан засобів забезпечення ТЗІ;

– перевірити наявність на підприємстві нормативних документів, які забезпечують функціювання системи захисту інформації, організацію проектування будівельних робіт з урахуванням вимог ТЗІ, а також нормативної та експлуатаційної документації, яка забезпечує ІД;

– виявити наявність транзитних, незадіяних (повітряних, настінних, зовнішніх та закладених у каналізацію) кабелів, кіл і проводів;

– визначити технічні засоби і системи, застосування яких не обгрунтовано службовою чи виробничою необхідністю і які підлягають демонтуванню;

– визначити технічні засоби, що потребують переобладнання (перемонтування) та встановлення засобів ТЗІ.

4.4 За результатами обстеження слід скласти акт, який повинен бути затверджений керівником підприємства.

4.5 Матеріали обстеження необхідно використовувати під час розроблення окремої моделі загроз, яка повинна включати:

– генеральний та ситуаційний плани підприємства, схеми розташування засобів і систем забезпечення ІД, а також інженерних комунікацій, які виходять за межі контрольованої території;

– схеми та описи каналів витоку інформації, каналів спеціального впливу і шляхів несанкційованого доступу до ІзОД;

– оцінку шкоди, яка передбачається від реалізації загроз.

5 Організація розроблення системи захисту інформації

5.1 На підставі матеріалів обстеження та окремої моделі загроз необхідно визначити головні задачі захисту інформації і скласти технічне завдання (ТЗ) на розроблення системи захисту інформації.

5.2 ТЗ повинно включати основні розділи:

– вимоги до системи захисту інформації;

– вимоги до складу проектної та експлуатаційної документації;

– етапи виконання робіт;

– порядок внесення змін і доповнень до розділів ТЗ;

– вимоги до порядку проведення випробування системи захисту.

5.3 Основою функціювання системи захисту інформації є план ТЗІ, що повинен містити такі документи:

– перелік розпорядчих, організаційно-методичних, нормативних документів з ТЗІ, а також вказівки щодо їхнього застосування;

– інструкції про порядок реалізації організаційних, первинних технічних та основних технічних заходів захисту;

– інструкції, що встановлюють обов`язки, права та відповідальність персоналу;

– календарний план ТЗІ.

5.4 ТЗ і план ТЗІ розробляють спеціалісти з ТЗІ, узгоджують із зацікавленими підрозділами (організаціями).

Затверджує їх керівник підприємства.

6 Реалізація організаційних заходів захисту

6.1 Організаційні заходи захисту інформації – комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення задач захисту шляхом регламентації діяльності персоналу і порядку функціювання засобів (систем) забезпечення ІД та засобів (систем) забезпечення ТЗІ.

6.2 У процесі розроблення і реалізації організаційних заходів потрібно:

– визначити окремі задачі захисту ІзОД;

– обґрунтувати структуру і технологію функціювання системи захисту інформації;

– розробити і впровадити правила реалізації заходів ТЗІ;

– визначити і встановити права та обов`язки підрозділів та осіб, що беруть участь в обробленні ІзОД;

– придбати засоби забезпечення ТЗІ та нормативні документи і забезпечити ними підприємство;

– установити порядок упровадження захищених засобів оброблення інформації, програмних і технічних засобів захисту інформації, а також засобів контролю ТЗІ;

– установити порядок контролю функціювання системи захисту інформації та її якісних характеристик;

– визначити зони безпеки інформації;

– установити порядок проведення атестації системи захисту інформаціїі, її елементів і розробити програми атестаційного випробування;

– забезпечити керування системою захисту інформації.

6.3 Оперативне вирішення задач ТЗІ досягається організацією керування системою захисту інформації, для чого необхідно:

– вивчати й аналізувати технологію проходження ІзОД у процесі ІД;

– оцінювати схильність ІзОД до впливу загроз у конкретний момент часу;

– оцінювати очікувану ефективність застосування засобів забезпечення ТЗІ;

– визначати (за необхідності) додаткову потребу в засобах забезпечення ТЗІ;

– здійснювати збирання, оброблення та реєстрацію даних, які відносяться до ТЗІ;

– розробляти і реалізовувати пропозиції щодо коригування плану ТЗІ в цілому або окремих його елементів.

7 Реалізація первинних технічних заходів захисту

7.1 У процесі реалізації первинних технічних заходів потрібно забезпечити:

– блокування каналів витоку інформації;

– блокування несанкційованого доступу до інформації чи її носіїв;

– перевірку справності та працездатності технічних засобів забезпечення ІД.

7.2 Блокування каналів витоку інформації може здійснюватися:

– демонтуванням технічних засобів, ліній зв'язку, сигналізації та керування, енергетичних мереж, використання яких не пов'язано з життєзабезпеченням підприємства та обробленням ІзОД;

– видаленням окремих елементів технічних засобів, які є середовищем поширення полів та сигналів, з приміщень, де циркулює ІзОД;

– тимчасовим відключенням технічних засобів, які не беруть участі в обробленні ІзОД, від ліній зв'язку, сигналізації, керування та енергетичних мереж;

– застосуванням способів та схемних рішень із захисту інформації, що не порушують основних технічних характеристик засобів забезпечення ІД.

7.3 Блокування несанкційованого доступу до інформації або її носіїв може здійснюватися:

– створенням умов роботи в межах установленого регламенту;

– унеможливленням використання програмних, програмно-апаратних засобів, що не пройшли перевірки (випробування).

7.4 Перевірку справності та працездатності технічних засобів і систем забезпечення ІД необхідно проводити відповідно до експлуатаційних документів.

Виявлені несправні блоки й елементи можуть сприяти витоку або порушенню цілісності інформації і підлягають негайній заміні (демонтуванню).

8 Реалізація основних технічних заходів захисту

8.1 У процесі реалізації основних технічних заходів захисту потрібно:

– установити засоби виявлення та індикації загроз і перевірити їхню працездатність;

– установити захищені засоби оброблення інформації, засоби ТЗІ та перевірити їхню працездатність;

– застосувати програмні засоби захисту в засобах обчислювальної техніки, автоматизованих системах, здійснити їхнє функційне тестування і тестування на відповідність вимогам захищеності;

– застосувати спеціальні інженерно-технічні споруди, засоби (системи).

8.2 Вибір засобів забезпечення ТЗІ зумовлюється фрагментарним або комплексним способом захисту інформації.

Фрагментарний захист забезпечує протидію певній загрозі.

Комплексний захист забезпечує одночасну протидію безлічі загроз.

8.3 Засоби виявлення та індикації загроз застосовують для сигналізації та оповіщення власника (користувача, розпорядника) ІзОД про витік інформації чи порушення її цілісності.

8.4 Засоби ТЗІ застосовуються автономно або спільно з технічними засобами забезпечення ІД для пасивного або активного приховування ІзОД.

Для пасивного приховування застосовують фільтри-обмежувачі, лінійні фільтри, спеціальні абонентські пристрої захисту та електромагнітні екрани.

Для активного приховування застосовують вузькосмугові й широкосмугові генератори лінійного та просторового зашумлення.

8.5 Програмні засоби застосовуються для забезпечення:

– ідентифікації та автентифікації користувачів, персоналу і ресурсів системи оброблення інформації;

– розмежування доступу користувачів до інформації, засобів обчислювальної техніки і технічних засобів автоматизованих систем;

– цілісності інформації та конфігурації автоматизованих систем;

– реєстрації та обліку дій користувачів;

– маскування оброблюваної інформації;

– реагування (сигналізації, відключення, зупинення робіт, відмови у запиті) на спроби несанкційованих дій.

8.6 Спеціальні інженерно-технічні споруди, засоби та системи застосовуються для оптичного, акустичного, електромагнітного та іншого екранування носіїв інформації.

До них належать спеціально обладнані світлопроникні, технологічні та санітарно-технічні отвори, а також спеціальні камери, перекриття, навіси, канали тощо.

8.7 Розміщення, монтування та прокладання спеціальних інженернотехнічних засобів і систем, серед них систем уземлення та електроживлення засобів забезпечення ІД, слід здійснювати відповідно до вимог нормативних документів з ТЗІ.

8.8 Технічні характеристики, порядок застосування та перевірки засобів забезпечення ТЗІ наводять у відповідній експлуатаційній документації.

9 Приймання, визначення повноти та якості робіт

9.1 За результатами виконання рекомендацій акта обстеження та реалізації заходів захисту ІзОД слід скласти у довільній формі акт приймання робіт з ТЗІ, який повинен підписати виконавець робіт, особа, відповідальна за ТЗІ, та затвердити керівник підприємства.

Примітка.

За потреби акт приймання робіт може бути погоджений із зацікавленими організаціями.

9.2 Для визначення повноти та якості робіт з ТЗІ слід провести атестацію.

Атестація виконується організаціями, які мають ліцензії на право діяльності в галузі ТЗІ.

9.3 Об`єктами атестації є системи забезпечення ІД та їхні окремі елементи, де циркулює інформація, що підлягає технічному захисту.

9.4 У ході атестації потрібно:

– установити відповідність об`єкта, що атестується, вимогам ТЗІ;

– оцінити якість та надійність заходів захисту інформації;

– оцінити повноту та достатність технічної документації для об`єкта атестації;

– визначити необхідність внесення змін і доповнень до організаційнорозпорядчих документів тощо.

Порядок атестації встановлюється нормативними документами системи ТЗІ

ДСТУ 3396.2-97. ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ. Захист інформації. Технічний захист інформації. Терміни та визначення

Чинний від 01.01.1998 р.

1 Галузь використання

Цей стандарт установлює терміни та визначення понять у сфері технічного захисту інформації (ТЗІ). Терміни, регламентовані у цьому стандарті, обов'язкові для використання в усіх видах організаційної та нормативної документації, а також для робіт зі стандартизації, і рекомендовані для використання у довідковій та навчально-методичній літературі, що належить до сфери технічного захисту інформації. Терміни стандарту є обов'язковими для використання підприємствами та установами усіх форм власності і підпорядкування, громадянами – суб'єктами підприємницької діяльності, міністерствами

(відомствами), центральними і місцевими органами державної виконавчої влади, військовими частинами усіх військових формувань, представництвами України за кордоном, які володіють, використовують та розпоряджаються інформацією, що становить державну чи іншу передбачену законом таємницю або є конфіденційною інформацією, яка належить державі.

2 Основні положення

2.1 Для кожного поняття встановлено один стандартизований термін. Терміни-синоніми подано як довідкові, вони не є стандартизованими.

2.2 Узята в круглі дужки частина терміна може бути опущена в разі використання терміна в документах з технічного захисту інформації.

2.3 У разі необхідності подані визначення можна змінювати, вводячи до них похідні ознаки з уточненням значення вживаних термінів. У випадках, коли в терміні містяться всі необхідні й достатні ознаки понять, замість їхнього визначення поставлено риску.

2.4 У стандарті як довідкові подано переклади термінів англійською (en) та російською (ru) мовами, визначень – російською мовою.

2.5 У стандарті наведено абетковий покажчик термінів українською мовою та абеткові покажчики англійських та російських перекладів термінів.

2.6 Стандартизовані терміни набрано напівгрубим шрифтом, їхні короткі форми, подані абревіатурою, прямим світлим, а синоніми – курсивом.

3 Нормативні посилання

Цей стандарт містить посилання на стандарт: ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення

4 Види інформації, які підлягають технічному захисту

4.1 інформація Відомості про об'єкти, процеси та явища (ДСТУ 2226)

4.1.1 інформація з обмеженим доступом Інформація, право доступу до якої обмежено встановленими правовими нормами і (чи) правилами

en limited access information

ru (информация с ограниченным доступом Информация, право доступа к которой ограничено установленными правовыми нормами и (или) правилами)

4.1.1.1 таємна інформація Інформація з обмеженим доступом, яка містить відомості, що становлять державну або іншу передбачену законом таємницю

en secret information

ru (секретная информация Информация сограниченным дос- тупом, которая содержит сведения, составляющие государственную или иную предусмотренную законом тайну)

4.1.1.2 конфіденційна інформація Інформація з обмеженим доступом, якою володіють, користуються чи розпоряджаються окремі фізичні чи юридичні особи або держава і порядок доступу до якої встановлюється ними

en confidential information

ru (конфиденциальная информация Информация с ограниченным доступом, находящаяся во владении, пользовании или распоряжении отдельных физических или юридических лиц либо государства и порядок доступа к которой устанавливается ими)

5 Загроза для інформації

5.1 витік інформації Неконтрольоване поширення інформації, яке призводить до її несанкціонованого одержання

en information leakage

ru (утечка информации Неконтролируемое распространение информации, которое ведет к ее несанкционированному получению)

5.2 порушення цілісності інформації Спотворення інформації, її руйнування або знищення

en information integrity violation

ru (нарушение целостности информации Искажение информации, ее разрушение или уничтожение)

5.3 блокування інформації Унеможливлення санкціононованого доступу до інформації

en block ofinformation

ru (блокирование информации Исключение возможности санкционированного доступа к информации)

5.4 загроза для інформації Витік, можливість блокування чи порушення цілісності інформації. Примітка. Загрози для інформації можуть виникати під час використання технічних засобів чи технологій, недосконалих щодо захисту інформації

en threat to information

ru (угроза для информации Утечка, возможность блокирования или нарушения целостности информации) Примечание. Угрозы для информации могут возникать при использовании технических средств или технологий, несовершенных в защите информации

5.4.1 модель загроз для інформації Формалізований опис методів та засобів здійснення загроз для інформації

en model of threats to information

ru (модель угроз безопасности информации Формализованное описание методов и средств осуществления угроз для информации)

5.5 доступ до інформації (ТЗІ) Можливість одержаання, оброблення інформації, її блокування та (чи) порушення цілісності

en access to information

ru (доступ к информации Возможность получения, обработки информации, ее блокированияи (или) нарушения целостности)

5.6 несанкціонований доступ (до інформації); НСД Доступ до інформації, за якого порушуються встановлений порядок його здіснення та (чи) правові норми

en unauthorized access (to information)

ru (несанкционированный доступ (к информации); НСД Доступ к информации, при котором нарушаются установленный порядок его осуществления и (или) правовые нормы)

5.7 закладний пристрій (ТЗІ); з а к л а д к а Потай встановлюваний технічний засіб, який створює загрозу для інформації

en secret intelligence device (bug)

ru (закладное устройство (ТЗИ); з а к л а д к а Скрытно установленное техническое средство, создающее угрозу для информации)

5.8 програмна закладка Потай впроваджена програма, яка створює загрозу для інформації, що міститься у комп'ютері

en program bug

ru (программная закладка(ТЗИ); Скрытно внедренная програм- ма, создающая угрозу для информации, содержащейся в компьютере)

5.9 комп'ютерний вірус Програма, що розмножується та поширюється самочинно Примітка. Комп'ютерний вірус може порушувати цілісність інформації, програмне забезпечення та (чи) режим роботи обчислювальної техніки

en computer virus

ru (компьютерный вирус Самопроизвольноно размножающаяся и распространяющаяся программа) Примечание. Компьютерный вирус может нарушать целостность информации, программное обеспечение и (или) режим работы вычислительной техники

5.10 спеціальний вплив (ТЗИ) Вплив на технічні засоби, що призводить до здійснення загрози для інформації

en special influence

ru (специальное воздействие (ТЗИ) Воздействие на технические средства, приводящее к осуществлению угроз для информации)

5.11 технічна розвідка Несанкціоноване здобування інформації за допомогою технічних засобів та її аналіз

en technical intelligence

ru (техническая разведка Несанкционированное получение сведений путем сбора информации техническими средствами и ее анализ)

5.11.1 модель технічної розвідки Формалізований опис методів, засобів та можливостей технічної розвідки

en technical intelligence model

ru (модель технической разведки Формализованное описание методов, средств и возможностей технической разведки)

6 Технічні канали витоку інформації

6.1 носій інформації (ТЗІ) Матеріальний об'єкт, що містить інформацію з обмеженим доступом

en information carrier

ru (носитель информации (ТЗИ) Материальный объект, содержащий информацию с ограниченным доступом)

6.2 інформативний сигнал (ТЗІ) Фізичне поле та(чи) хімічна речовина, що містять інформацію з обмеженим доступом

en information signal

ru (информативный сигнал Физическое поле и химическое вещество, содержащие информацию с ограниченным доступом)

6.3 (технічний) канал витоку інформації Сукупність носія інформації, середовища його поширення та засобу технічної розвідки

en (technical) channel of information leakage

ru (технический) канал утечки информации Совокупность носителя информации, среды его распространения и средства технической разведки)

6.3.1 самочинний (технічний) канал витоку інформації; ненавмисний канал витоку інформації Технічний канал витоку інформації, в якому носії інформації та (чи) середовище їх поширення формуються самочинно

en unpremeditated (technical) channel of information leakage

ru (непреднамеренный (технический) канал утечки информации Технический канал утечки информации, в котором носители информации и (или) среда их распространения формируются самопроизвольно)

6.3.2 штучний (технічний) канал витоку інформації; навмисний канал витоку інформації

en premeditated (technical) channel of information leakage

ru (преднамеренный (технический) канал утечки информации)

6.4 побічне електромагнітне випромінення і навід; ПЕМВН Електромагнітне випромінення та навід, що є побічним результатом функціонування технічного засобу і може бути носієм інформації

en spurious elektromagnetic radiation and breakthrough

ru (побочное электромагнитное излучение и наводка; ПЭМИН Электромагнитное излучение и наводка, являющиеся побочным результатом функционирования технического средства и может быть носителем информации)

7 Технічний захист інформації

7.1 технічний захист інформації; ТЗІ Діяльність, спрямована на запобігання порушенню цілісності, блокуванню та (чи) витоку інформації технічними каналами

en technikal protection of information

ru (техническая защита информаци; ТЗИ Деятельность, направленная на предотвращение нарушения целостности, блокирования и (или) утечки информации по техническим каналам)

7.2 (технічний) засіб із захистом; захищений (технічний) засіб; захищена техніка Технічний засіб, у якому додатково до основного призначення передбачено функцію захисту інформації від загроз

en facility with protect

ru ((техническое) средство с защитой; защищенное (техническое) средство; защищенная техника Техническое средство, в котором дополнительно к основному назначению предусмотрена функция защиты информации от угроз)

7.3 засіб технічного захисту інформації Пристрій та (чи) програмний засіб, основне призначення яких – захист інформації від загроз

en facility of technical protection of information

ru (средство технической защиты информации Устройство и (или) программное средство, основное назначение которых – защита информации от угроз)

7.4 приховування інформації Спосіб технічного захисту інформації, який полягає в унеможливленні або суттєвому утрудненні несанкціонованого одержання інформації

en hiding

ru (сокрытие (информации) Способ технической защиты информации, состоящий в исключении или существенном затруднении несанкционированного получения информации)

7.4.1 пасивне приховування інформації Приховування інформації ослабленням енергетичних характеристик фізичних полів або зниженням концентрації речовин

en passive hiding

ru (пассивное сокрытие информации Сокрытие информации путем ослабления энергетических характеристик физических полей или снижения концентрации веществ)

7.4.2 активне приховування інформації Приховування інформації створенням таких фізичних полів та речовин, які утруднюють здобування інформації або спричиняють невизначеність її змісту

en active hiding

ru (активное сокрытие информации Сокрытие информации путем формирования таких физических полей и веществ, которые затрудняют получение информации или создают неопределенность ее содержания)

7.5 дезінформування Спосіб технічного захисту інформації, який полягає у формуванні свідомо хибної інформації для унеможливлення несанкціонованого доступу до істинної інформації

en misinformation

ru (дезинформирование Способ технической защиты информации, состоящий в формировании заведомо ложной информации для исключения несанкционированного доступа к истинной информации)

8 Організація технічного захисту інформації

8.1. система технічного захисту інформації Сукупність організаційних структур, нормативно-правових документів та матеріально-технічної бази Прімитка. Основними елементами матеріально-технічної бази системи ТЗІ є технічні засоби із захистом, засоби технічного захисту інформації та засоби контролю за ефективністю технічного захисту інформації

en system of technical protection of information

ru (система технической защиты информации Совокупность организационных структур, нормативно-правовых документов и материально-технической базы технической защиты информации Примечание. Основными элементами материально-технической базы системы ТЗИ являются технические средства с защитой и средства контроля за эффективностью технической защиты информации)

8.2 зона безпеки інформації Простір, за межами якого інформація убезпечена

en security zone of information

ru (зона безопасности информации Пространство, за пределами которого обеспечена безопасность информации)

8.3. рівень (технічного) захисту інформації Сукупність вимог (в тому числі і тих, що нормуються), які визначається режимом доступу до інформації та загрозами для неї

en technical protection information level

ru (уровень (технической) защиты информации Совокупность требований (в том числе и нормируемых), которые определяются режимом доступа к информации и угрозами для нее)

8.4 ефективність технічного захисту інформації Ступінь відповідності вжитих заходів щодо технічного захисту інформації встановленим вимогам

en efficiency (of technical) protection of information

ru (эффективность (технической) защиты информации Степень соответствия принятых мер по технической защите информации установленым нормам

А.9. ДСТУ ISO/IEC 15408-1:2017

ISO/IEC 15408-1:2022. Інформаційна безпека, кібербезпека та захист конфіденційності. Критерії оцінки ІТ-безпеки. Частина 1. Вступ і загальна модель

Цей документ встановлює загальні концепції та принципи оцінювання безпеки ІТ і визначає загальну модель оцінювання, що надається різними частинами стандарту, який у цілому призначений для використання в якості основи для оцінки властивостей безпеки ІТ-продуктів.

Цей документ містить огляд усіх частин серії ISO/IEC 15408. Він описує різні частини серії ISO/IEC 15408; визначає терміни та скорочення, які слід використовувати в усіх частинах стандарту; встановлює основну концепцію мети оцінювання (TOE); описує контекст оцінювання та описує аудиторію, якій адресовані критерії оцінювання. Дано вступ до основних концепцій безпеки, необхідних для оцінки ІТ-продуктів.

Цей документ представляє:

– ключові поняття профілів захисту (PP), модулів PP, конфігурацій PP, пакетів, цілей безпеки (ST) і типів відповідності;

– опис організації компонентів безпеки по всій моделі;

– різні операції, за допомогою яких функціональні компоненти та компоненти гарантії, наведені в ISO/IEC 15408-2 та ISO/IEC 15408-3, можуть бути налаштовані шляхом використання дозволених операцій;

– загальну інформацію про методи оцінювання, наведені в ISO/IEC 18045;

– настанова щодо застосування ISO/IEC 15408-4 для розробки методів оцінювання (EM) і діяльності з оцінювання (EA), виведених із ISO/IEC 18045;

– загальну інформацію про попередньо визначені рівні гарантії оцінювання (EAL), визначені в ISO/IEC 15408-5;

– інформація щодо обсягу схем оцінювання.

А.10. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу»

Чинний від 1999-07-01

1 Галузь використання

Цей документ установлює терміни і визначення понять у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

Терміни, що установлюються цим документом, обов'язкові для застосування в усіх видах документації і літератури, що входять до системи технічного захисту інформації.

Для кожного поняття встановлено один термін. Застосування синонімів терміна не допускається.

Для довідки наведені іноземні еквіваленти термінів, що запроваджуються, а також алфавітні покажчики термінів.

2 Нормативні посилання

Під час розробки цього нормативного документа використані наступні стандарти:

– ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення.

– ДСТУ 2941-94. Системи обробки інформації. Розробка систем. Терміни і визначення.

– ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни і визначення.

3 Позначення і скорочення

В цьому НД ТЗІ використовуються наступні позначення і скорочення:

– АС – автоматизована система;

– КЗЗ – комплекс засобів захисту;

– КС – комп'ютерна система;

– КСЗІ— комплексна система захисту інформації;

– НСД – несанкціонований доступ;

– ОС – обчислювальна система;

– ПЗ – програмне забезпечення;

– ПРД – правила розмежування доступу;

– ТЗІ – технічний захист інформації.

4 Терміни і визначення

4.1 Основні поняття

4.1.1 Обчислювальна система; ОС (computer system) – сукупність програмних-апаратних засобів, призначених для обробки інформації.

4.1.2 Автоматизована система; АС (automated system) – організаційно-технічна система, що реалізує інформаційну технологію і об'єднує ОС, фізичне середовище, персонал і інформацію, яка обробляється.

4.1.3 Комп'ютерна система; КС (computer system, target of evaluation) – сукупність програмно-апаратніх засобів, яка подана для оцінки.

4.1.4 Політика безпеки інформації (information security policy) – сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок обробки інформації.

4.1.5 Загроза (threat) – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків АС.

4.1.6 Безпека інформації (information security) – стан інформації, в якому за-безпечується збереження визначених політикою безпеки властивостей інформації.

4.1.7 Захист інформації в АС (information protection, information security, computer system security) – діяльність, яка спрямована на забезпечення безпеки оброблюваної в АС інформації та АС в цілому, і дозволяє запобігти або ускладнити можливість реалізації загроз, а також знизити величину потенційних збитків внаслідок реалізації загроз.

4.1.8 Комплексна система захисту інформації; КСЗІ – сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС.

4.1.9 Комплекс засобів захисту; КЗЗ (trusted computing base; TCB) – сукупність програмно-апаратних засобів, які забезпечують реалізацію політики безпеки інформації.

4.1.10 Захищена комп'ютерна система; захищена КС (trusted computer system, trusted computer product) – комп'ютерна система, яка здатна забезпечувати захист оброблюваної інформації від певних загроз.

4.1.11 Об'єкт комп'ютерної системи; об'єкт КС (product object, system object) – елемент ресурсу КС, що знаходиться під керуванням КЗЗ і характеризується певними атрибутами і поводженням.

4.1.12 Пасивний об'єкт (passive object) – об'єкт КС, який в конкретному акті доступу виступає як пасивний компонент системи, над яким виконується дія і/або який служить джерелом чи приймальником інформації.

4.1.13 Об'єкт-процес (process object) – виконувана в даний момент програма, яка повністю характеризується своїм контекстом (поточним станом регістрів обчислювальної системи, адресним простором, повноваженнями і т.ін.).

4.1.14 Користувач (user) – фізична особа, яка може взаємодіяти з КС через наданий їй інтерфейс.

4.1.15 Об'єкт-користувач (user object) – подання фізичного користувача в КС, що створюється в процесі входження користувача в систему і повністю характеризується своїм контекстом (псевдонімом, ідентифікаційним кодом, повноваженнями і т.ін.).

4.1.16 Ідентифікатор об'єкта КС (object identifier) – унікальний атрибут об'єкта КС, що дозволяє однозначно виділити даний об'єкт серед подібних.

4.1.17 Потік інформації (information flow) – передавання інформації від одного до іншого об'єкта КС.

4.1.18 Доступ до інформації (access to information) – вид взаємодії двох об'єктів КС, внаслідок якого створюється потік інформації від одного об'єкта до іншого і/або відбувається зміна стану системи.

4.1.19 Правила розмежування доступу; ПРД (access mediation rules) – частина політики безпеки, що регламентує правила доступу користувачів і процесів до пасивних об'єктів.

4.1.20 Тип доступу (access type) – суттєвість доступу до об’єкта, що характеризує зміст здійснюваної взаємодії, а саме: проведені дії, напрям потоків інформації, зміни в стані системи (наприклад, читання, запис, запуск на виконання, видаляння, дозапис).

4.1.21 Запит на доступ (access request) – звернення одного об’єкта КС до іншого з метою отримання певного типу доступу.

4.1.22 Санкціонований доступ до інформації (authorized access to information) – доступ до інформації, що не порушує ПРД.

4.1.23 Несанкціонований доступ до інформації; НСД до інформації (unauthorized access to information) – доступ до інформації, здійснюваний з порушенням ПРД.

4.1.24 Захист від несанкціонованого доступу; захист від НСД (protection from unauthorized access) – запобігання або істотне утруднення несанкціонованого доступу до інформації.

4.1.25 Право доступу (access right) – дозвіл або заборона здійснення певного типу доступу.

4.1.26 Повноваження (privilege) – права користувача або процесу на виконання певних дій, зокрема на одержання певного типу доступу до об’єктів.

4.1.27 Керування доступом (access control) – сукупність заходів з визначення повноважень і прав доступу, контролю за додержанням ПРД.

4.1.28 Розмежування доступу (access mediation) – сукупність процедур, що реалізують перевірку запитів на доступ і оцінку на підставі ПРД можливості надання доступу.

4.1.29 Авторизація (authorization) – надання повноважень; встановлення відповідності між повідомленням (пасивним об’єктом) і його джерелом (створившим його користувачем або процесом).

4.1.30 Авторизований користувач (authorized user) – користувач, що володіє певними повноваженнями.

4.1.31 Роль користувача (user role) – сукупність функцій щодо керування КС, КЗЗ і обробки інформації, доступних користувачеві.

4.1.32 Адміністратор (administrator, administrative user) – користувач, роль якого включає функції керування КС і/або КЗЗ.

4.1.33 Адміністратор безпеки (security administrator) – адміністратор, відповідальний за дотримання політики безпеки.

4.1.34 Порушник (user violator) – користувач, який здійснює несанкціонований доступ до інформації.

4.2 Властивості інформації і загрози

4.2.1 Ознайомлення (disclosure) – одержання користувачем або процесом інформації, що міститься в об’єкті.

4.2.2 Модифікація (modification) – зміна користувачем або процесом інформації, що міститься в об’єкті.

4.2.3 Критична інформація (sensitive information) – інформація, що вимагає захисту; будь-яка інформація, втрата або неправильне використання якої (модифікація, ознайомлення) може нанести шкоду власникові інформації або АС, або будь-якій іншій фізичній (юридичній) особі чи групі осіб.

4.2.4 Конфіденційність інформації (information confidentiality) – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом.

4.2.5 Цілісність інформації (information integrity) – властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом.

4.2.6 Цілісність системи (system integrity) – властивість системи, яка полягає в тому, що жоден її компонент не може бути усунений, модифікований або доданий з порушенням політики безпеки.

4.2.7 Доступність (availability) – властивість ресурсу системи (КС, послуги, об'єкта КС, інформації), яка полягає в тому, що користувач і/або процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний.

4.2.8 Спостереженість (accountability) – властивість КС, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об'єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки і/або забезпечення відповідальності за певні дії.

4.2.9 Атака (attack) – спроба реалізації загрози.

4.2.10 Проникнення (penetration) – успішне подолання механізмів захисту системи.

4.2.11 Вразливість системи (system vulnerability) – нездатність системи протистояти реалізації певної загрози або сукупності загроз.

4.2.12 Компрометація (compromise) – порушення політики безпеки; несанкціоноване ознайомлення.

4.2.13 Втрата інформації (information leakage) – неконтрольоване розповсюдження інформації, що веде до її несанкціонованого одержання.

4.2.14 Прихований канал (covert channel) – спосіб одержання інформації за рахунок використання шляхів передачі інформації, існуючих у КС, але не керованих КЗЗ, або спостереження за існуючими потоками інформації.

4.2.15 Прихований канал з пам'яттю (storage covert channel) – прихований канал, що реалізується шляхом прямого або непрямого запису інформації в певну область пам'яті одним процесом і прямим чи непрямим читанням даної області пам'яті іншим процесом.

4.2.16 Часовий прихований канал (timing covert channel) – прихований канал, що дозволяє передавати інформацію від одного процесу до іншого шляхом модулювання першим процесом часових характеристик системи (наприклад, часу зайнятості центрального процесора), що спостерігаються іншим процесом.

4.2.17 Пропускна здатність прихованого каналу (covert channel bandwidth) – кількість інформації, що одержується використанням прихованого каналу за одиницю часу.

4.2.18 Відмова (fault, failure) – втрата здатності КС або її компонента виконувати певну функцію.

4.2.19 Відмова в обслуговуванні (denial of service) – будь-яка дія або послідовність дій, що призводять будь-яку частину (компонент) системи до виходу із ладу; нездатність системи виконувати свої функції (надавати декларовані послуги) внаслідок виходу із ладу якого-небудь компонента або інших причин.

4.2.20 Невизнання участі (repudiation) – відмова одного з об'єктів КС від факту участі в події, що трапилась.

4.2.21 Відмова від авторства (repudiation of origin) – заперечення причетності до утворення або передачі якого-небудь документа чи повідомлення.

4.2.22 Відмова від одержання (repudiation of receipt) – заперечення причетності до одержання якого-небудь документа або повідомлення.

4.2.23 Комп'ютерний вірус (computer virus) – програма, що володіє здатністю до самовідтворення і, як правило, здатна здійснювати дії, які можуть порушити функціонування КС і/або зумовити порушення політики безпеки.

4.2.24 Програмна закладка (program bug) – потайно впроваджена програма або недокументовані властивості програмного забезпечення, використання яких може призвести до обходу КЗЗ і/або порушення політики безпеки.

4.2.25 Люк (trap door) – залишені розробником недокументовані функції, використання яких дозволяє обминути механізми захисту.

4.2.26 Троянський кінь (Trojan horse) – програма, яка, будучи авторизованим процесом, окрім виконання документованих функцій, здатна здійснювати приховані дії від особи авторизованого користувача в інтересах розробника цієї програми.

4.2.27 Збирання сміття – загроза, що полягає в захопленні і аналізі користувачем або процесом спільно використовуваних об'єктів, звільнених іншим користувачем чи процесом, з метою одержання інформації, що в них знаходиться.

4.3 Створення і експлуатація захищених систем

4.3.1 Модель загроз (model of threats) – абстрактний формалізований або неформалізований опис методів і засобів здійснення загроз.

4.3.2 Модель порушника (user violator model) – абстрактний формалізований або неформалізований опис порушника.

4.3.3 Ризик (risk) – функція ймовірності реалізації певної загрози, виду і величини завданих збитків.

4.3.4 Аналіз ризику (risk analysis) – процес визначення загроз безпеці інформації та їх характеристик, слабких сторін КСЗІ (відомих і припустимих), оцінки потенційних збитків від реалізації загроз та ступеню їх прийнятності для експлуатації АС.

4.3.5 Керування ризиком (risk management) – сукупність заходів, що проводяться протягом всього життєвого циклу АС щодо оцінки ризику, вибору, реалізації і впровадження заходів забезпечення безпеки, спрямована на досягнення прийнятного рівня залишкового ризику.

4.3.6 Залишковий ризик (residual risk) – ризик, що залишається після впровадження заходів забезпечення безпеки.

4.3.7 Заходи забезпечення безпеки (safeguards) – послуги, функції, механізми, правила і процедури, призначені для забезпечення захисту інформації.

4.3.8 Послуга безпеки (security service) – сукупність функцій, що забезпечують захист від певної загрози або від множини загроз.

4.3.9 Механізми захисту (security mechanism) – конкретні процедури і алгоритми, що використовуються для реалізації певних функцій і послуг безпеки.

4.3.10 Засоби захисту (protection facility) – програмні, програмно-апаратні та апаратні засоби, що реалізують механізми захисту.

4.3.11 Політика безпеки послуги (service security policy) – правила, згідно з якими функціонують механізми, що реалізують послугу.

4.3.12 Рівень послуги (level of service) – міра ефективності і/або стійкості механізмів, що реалізують послугу, відносно до введеної для даної послуги шкали оцінки.

4.3.13 Гарантії (assurance) – сукупність вимог (шкала оцінки) для визначення міри упевненості, що КС коректно реалізує політику безпеки.

4.3.14 Рівень гарантій (assurance level) – міра упевненості в тому, що КС коректно реалізує політику безпеки.

4.3.15 Модель політики безпеки (security policy model) – абстрактний формалізований або неформалізований опис політики безпеки інформації.

4.3.16 Домен комп'ютерної системи; домен КС (domain) – ізольована логічна область КС, що характеризується унікальним контекстом, всередині якої об'єкти володіють певними властивостями, повноваженнями і зберігають певні відносини між собою.

4.3.17 Тестування на проникання (penetration testing) – випробування, метою яких є здійснення спроби обминути або відключити механізми захисту.

4.3.18 Оцінка вразливості (vulnerability assessment) – дослідження об'єкта оцінки з метою визначення можливості реалізації загроз.

4.3.19 Оцінка безпеки інформації (information security evaluation) – процес, метою якого є визначення відповідності стану безпеки інформації в КС встановленим вимогам.

4.3.20 Критерії оцінки захищеності; критерії (security evaluation criteria) – сукупність вимог (шкала оцінки), що використовується для оцінки ефективності функціональних послуг безпеки і коректності їх реалізації.

4.3.21 Рейтинг (rating) – упорядкований перелік рівнів послуг і рівня гарантій, виявлених в процесі оцінки КС.

4.3.22 Функціональний профіль (functionality profile) – упорядкований перелік рівнів функціональних послуг, який може використовуватись як формальна специфікація функціональності КС.

4.4 Принципи, послуги і механізми забезпечення безпеки

4.4.1 Довірче керування доступом (discretionary access control) – принцип керування доступом, який полягає в тому, що звичайним користувачам дозволено керувати (довіряють керування) потоками інформації між іншими користувачами і об'єктами свого домена (наприклад, на підставі права володіння об'єктами) без втручання адміністратора.

4.4.2 Адміністративне керування доступом (mandatory access control) – принцип керування доступом, який полягає в тому, що керувати потоками інформації між користувачами і об'єктами дозволено тільки спеціально авторизованим користувачам, а звичайні користувачі не мають можливості створити потоки інформації, які могли б призвести до порушення встановлених ПРД.

4.4.3 Експорт інформації (information export) – виведення інформації з-під керування КЗЗ назовні.

4.4.4 Імпорт інформації (information import) – уведення інформації ззовні під керування КЗЗ.

4.4.5 Ідентифікація (identification) – процедура присвоєння ідентифікатора об'єкту КС або встановлення відповідності між об'єктом і його ідентифікатором; впізнання.

4.4.6 Автентифікація (authentication) – процедура перевірки відповідності пред'яв-леного ідентифікатора об'єкта КС на предмет належності його цьому об'єкту; встановлення або підтвердження автентичності.

4.4.7 Інформація автентифікації (authentication information) – інформація, що використовується для автентифікації.

4.4.8 Пароль (password) – секретна інформація автентифікації, що являє собою послідовність символів, яку користувач повинен ввести через обладнання вводу інформації, перш ніж йому буде надано доступ до КС або до інформації.

4.4.9 Персональний ідентифікаційний номер; ПІН (personal identification number, PIN) – вид паролю, що звичайно складається тільки із цифр, і який, як правило, має бути пред'явлений нарівні з носимим ідентифікатором.

4.4.10 Достовірний канал (trusted path) – захищений шлях передачі інформації між користувачем і КЗЗ, що не може бути імітований, а інформація, що передається ним, не може бути отримана або модифікована стороннім користувачем або процесом.

4.4.11 Реєстрація (audit, auditing) – послуга, що забезпечує збирання і аналіз інформації щодо використання користувачами і процесами функцій і об'єктів, контрольованих КЗЗ.

4.4.12 Журнал реєстрації (audit trail) – упорядкована сукупність реєстраційних записів, кожен з яких заноситься КЗЗ за фактом здійснення контрольованої події.

4.4.13 Довірча конфіденційність (discretionary confidentiality) – послуга, що забезпечує конфіденційність інформації відповідно до принципів довірчого керування доступом.

4.4.14 Адміністративна конфіденційність (mandatory confidentiality) – послуга, що забезпечує конфіденційність інформації відповідно до принципів адміністративного керування доступом.

4.4.15 Довірча цілісність (discretionary integrity) – послуга, що забезпечує цілісність інформації відповідно до принципів довірчого керування доступом.

4.4.16 Адміністративна цілісність (mandatory integrity) – послуга, що забезпечує цілісність інформації відповідно до принципів адміністративного керування доступом.

4.4.17 Очищення пам'яті (memory clearing) – знищення даних в пам'яті шляхом встановлення полів цих даних в заданий або випадковий стан.

4.4.18 Розділюваний об'єкт (shared object) – об'єкт КС, який одночасно або почергово використовується різними користувачами і/або процесами.

4.4.19 Повторне використання об'єкта (object reuse) – послуга, що забезпечує очищення пам'яті і призупинення дії повноважень щодо розділюваного об'єкта, який раніше використовувався одним користувачем або процесом, перед наданням його іншому користувачеві або процесу.

4.4.20 Аналіз прихованих каналів (covert channels analyse) – послуга, яка забезпечує гарантію того, що приховані канали в КС відсутні, знаходяться під наглядом або, принаймні, відомі.

4.4.21 Керування потоками (flow control) – сукупність функцій і процедур, які забезпечують неможливість передачі інформації прихованими каналами, тобто в обхід КЗЗ.

В більш вузькому значенні часто розуміється сукупність процедур, які забезпечують неможливість передачі інформації від об'єкта КС з більш високим рівнем доступу до об'єкта КС з більш низьким рівнем доступу.

4.4.22 Відкат (rollback) – послуга, що забезпечує повернення об'єкта КС до відомого попереднього стану після виконання над об'єктом певної операції або серії операцій.

4.4.23 Квота (quota) – обмеження можливості використання певного ресурсу КС користувачем або процесом.

4.4.24 Стійкість до відмов (fault tolerance) – послуга, що забезпечує здатність КС продовжувати функціонування в умовах виникнення збоїв і відмов окремих компонентів.

4.4.25 Ініціалізація (initialization) – встановлення системи або об'єкта у відомий чи визначений стан.

4.4.26 Диспетчер доступу (reference monitor) – реалізація концепції абстрактного автомата, яка забезпечує дотримання ПРД і характеризується такими трьома особливостями: забезпечує безперервний і повний контроль за доступом, захищений від модифікації і має невеликі розміри.

4.4.27 Ядро захисту (security kernel) – частина КЗЗ, в якій зосереджено мінімально необхідний набір механізмів, що реалізують ПРД.

4.4.28 Атрибут доступу (tag, access mediation information) – будь-яка зв'язана з об'єктом КС інформація, яка використовується для керування доступом.

4.4.29 Матриця доступу (access matrix) – n-мірна таблиця, вздовж кожного виміру якої відкладені ідентифікатори об’єктів КС одного типу (об’єктів-користувачів, об’єктів-процесів чи пасивних об’єктів), і містить як елементи права доступу за кожним із типів доступу.

4.4.30 Список доступу (access control list) – перелік користувачів і/або процесів з зазначенням їх прав доступу до об’єкта КС, з яким пов’язаний цей перелік.

4.4.31 Список повноважень (privilege list, profile) – перелік об’єктів з зазначенням прав доступу до них з боку користувача або процесу, з яким пов’язаний цей перелік.

4.4.32 Мітка (label) – атрибут доступу, що відображає категорію доступу об’єкта КС.

4.4.33 Категорія доступу (security level) – комбінація ієрархічних і неієрархічних атрибутів доступу, що відображає рівень критичності (наприклад, конфіденційності) інформації або повноважень користувача щодо доступу до такої інформації.

4.4.34 Рівень доступу (access level) – ієрархічна частина категорії доступу пасивного об’єкта.

4.4.35 Рівень допуску (clearance) – ієрархічна частина категорії доступу користувача або процесу, що визначає максимальний рівень доступу пасивного об’єкта, до якого може одержати доступ користувач чи процес.

4.4.36 Криптографічне перетворення – перетворення даних, яке полягає в їх шифруванні, вироблення імітовставки або цифрового підпису.

4.4.37 Шифрування даних – процес зашифрування або розшифрування.

4.4.38 Зашифрування даних (data encryption) – процес перетворення відкритого тексту в шифртекст.

4.4.39 Розшифрування даних (data decryption) – процес перетворення шифртексту у відкритий текст.

4.4.40 Відкритий текст (clear text) – дані з доступним семантичним змістом.

4.4.41 Шифртекст (ciphertext) – дані, отримані у результаті зашифрування відкритого тексту.

4.4.42 Ключ (key) – конкретний стан деяких параметрів алгоритму криптографічного перетворення, що забезпечує вибір одного перетворення із сукупності можливих для даного алгоритму.

4.4.43 Імітовставка (data authentication code) – блок інформації фіксованої довжини, що одержується із відкритого тексту і ключа, однозначно відповідний даному відкритому тексту.

4.4.44 Цифровий підпис (digital signature) – дані, одержані в результаті криптографічного перетворення блоку даних і/або його параметрів (геш-функції, довжини, дати утворення, ідентифікатора відправника і т.ін.), що дозволяють приймальнику даних впевнитись в цілісності блоку і справжності джерела даних і забезпечити захист від підробки і підлогу.

4.4.45 Завірення (notarization) – реєстрація даних у довіреної третьої особи з метою забезпечення надалі впевненості в правильності таких характеристик як зміст, джерело даних, час відправлення чи одержання тощо.

А.11. НД ТЗІ 2.5-004-99. «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу»

1 Галузь використання

Цей нормативний документ (далі – Критерії) – установлює критерії оцінки захищеності інформації, оброблюваної в комп'ютерних системах, від несанкціонованого доступу.

Критерії є методологічною базою для визначення вимог з захисту інформації в комп'ютерних системах від несанкціонованого доступу; створення захищених комп'ютерних систем і засобів захисту від несанкціонованого доступу; оцінки захищеності інформації в комп'ютерних системах і їх придатності для обробки критичної інформації (інформації, що вимагає захисту).

Критерії надають:

1. Порівняльну шкалу для оцінки надійності механізмів захисту інформації від несанкціонованого доступу, реалізованих в комп'ютерних системах.

2. Базу (орієнтири) для розробки комп'ютерних систем, в яких мають бути реалізовані функції захисту інформації.

Критерії можуть застосовуватися до всього спектра комп'ютерних систем, включаючи однорідні системи, багатопроцесорні системи, бази даних, вбудовані системи, розподілені системи, мережі, об'єктно-орієнтовані системи та ін.

Цей документ призначено для постачальників (розробників), споживачів (замовників, користувачів) комп'ютерних систем, які використовуються для обробки (в тому числі збирання, зберігання, передачі і т. ін.) критичної інформації, а також для органів, що здійснюють функції оцінювання захищеності такої інформації та контролю за її обробкою.

Цей документ відображає сучасний стан проблеми і підходів до її розв'язання. З розвитком нових тенденцій в галузі і за умови достатньої обгрунтованості документ є відкритим для включення до його складу Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України нових послуг.

2 Нормативні посилання

У цьому НД ТЗІ наведено посилання на такі нормативні документи:

ДСТУ 3230-95. Управління якістю і забезпечення якості. Терміни і визначення.

ДСТУ 2853-94. Програмні засоби ЕОМ. Підготовка і проведення випробувань.

ДСТУ 2851-94. Програмні засоби ЕОМ. Документування результатів випробувань.

НД ТЗІ 1.1-004-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

3 Визначення

В цьому нормативному документі використовуються терміни і визначення, що відповідають встановленим нормативним документом ТЗІ 1.1-003-99

“Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу“.

4 Позначення і скорочення

В цьому нормативному документі використовуються такі позначення і скорочення:

Загальні терміни:

– АС – автоматизована система;
– КС – комп'ютерна система;
– КЗЗ – комплекс засобів захисту;
– НСД – несанкціонований доступ;
– ОС – обчислювальна система;
– ПЗ – програмне забезпечення;
– ПЗП – постійний запам’ятовуючий пристрій;
– ПРД – правила розмежування доступу;

Позначення послуг:

– КД – довірча конфіденційність;
– КА – адміністративна конфіденційність;
– КО – повторне використання об'єктів;
– КК – аналіз прихованих каналів;
– КВ – конфіденційність при обміні;
– ЦД – довірча цілісність;
– ЦА – адміністративна цілісність;
– ЦО – відкат;
– ЦВ – цілісність при обміні;
– ДР – використання ресурсів;
– ДВ – стійкість до відмов;
– ДЗ – гаряча заміна;
– ДВ – відновлення після збоїв;
– НР – реєстрація;
– НИ – ідентифікація і автентифікація;
– НК – достовірний канал;
– НО – розподіл обов'язків;
– НЦ – цілісність КЗЗ;
– НТ – самотестування;
– НВ – автентифікація при обміні;
– НА – автентифікація відправника;
– НП – автентифікація одержувача.

5 Побудова і структура критеріїв захищеності інформації

В процесі оцінки спроможності комп'ютерної системи забезпечувати захист оброблюваної інформації від несанкціонованого доступу розглядаються вимоги двох видів:

– вимоги до функцій захисту (послуг безпеки);
– вимоги до гарантій.

В контексті Критеріїв комп'ютерна система розглядається як набір функціональних послуг. Кожна послуга являє собою набір функцій, що

дозволяють протистояти певній множині загроз. Кожна послуга може включати декілька рівнів. Чим вище рівень послуги, тим більш повно забезпечується захист від певного виду загроз. Рівні послуг мають ієрархію за повнотою захисту, проте не обов'язково являють собою точну підмножину один одного. Рівні починаються з першого (1) і зростають до значення n, де n – унікальне для кожного виду послуг.

Функціональні критерії розбиті на чотири групи, кожна з яких описує вимоги до послуг, що забезпечують захист від загроз одного із чотирьох основних типів.

Конфіденційність. Загрози, що відносяться до несанкціонованого ознайомлення з інформацією, становлять загрози конфіденційності. Якщо існують вимоги щодо обмеження можливості ознайомлення з інформацією, то відповідні послуги треба шукати в розділі "Критерії конфіденційності". В цьому розділі описані такі послуги (в дужках наведені умовні позначення для кожної послуги): довірча конфіденційність, адміністративна конфіденційність, повторне використання об'єктів, аналіз прихованих каналів, конфіденційність при обміні (експорті/імпорті).

Цілісність. Загрози, що відносяться до несанкціонованої модифікації інформації, становлять загрози цілісності. Якщо існують вимоги щодо обмеження можливості модифікації інформації, то відповідні послуги треба шукати в розділі "Критерії цілісності". В цьому розділі описані такі послуги: довірча цілісність, адміністративна цілісність, відкат і цілісність при обміні.

Доступність. Загрози, що відносяться до порушення можливості використання комп'ютерних систем або оброблюваної інформації, становлять загрози доступності. Якщо існують вимоги щодо захисту від відмови в доступі або захисту від збоїв, то відповідні послуги треба шукати в розділі "Критерії доступності". В цьому розділі описані такі послуги: використання ресурсів, стійкість до відмов, гаряча заміна, відновлення після збоїв.

Спостереженість. Ідентифікація і контроль за діями користувачів, керованість комп'ютерною системою становлять предмет послуг спостереженості і керованості. Якщо існують вимоги щодо контролю за діями користувачів або легальністю доступу і за спроможністю комплексу засобів захисту виконувати свої функції, то відповідні послуги треба шукати у розділі "Критерії спостереженості". В цьому розділі описані такі послуги: реєстрація, ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність комплексу засобів захисту, самотестування, автентифікація при обміні, автентифікація відправника (невідмова від авторства), автентифікація одержувача одержувача (невідмова від одержання).

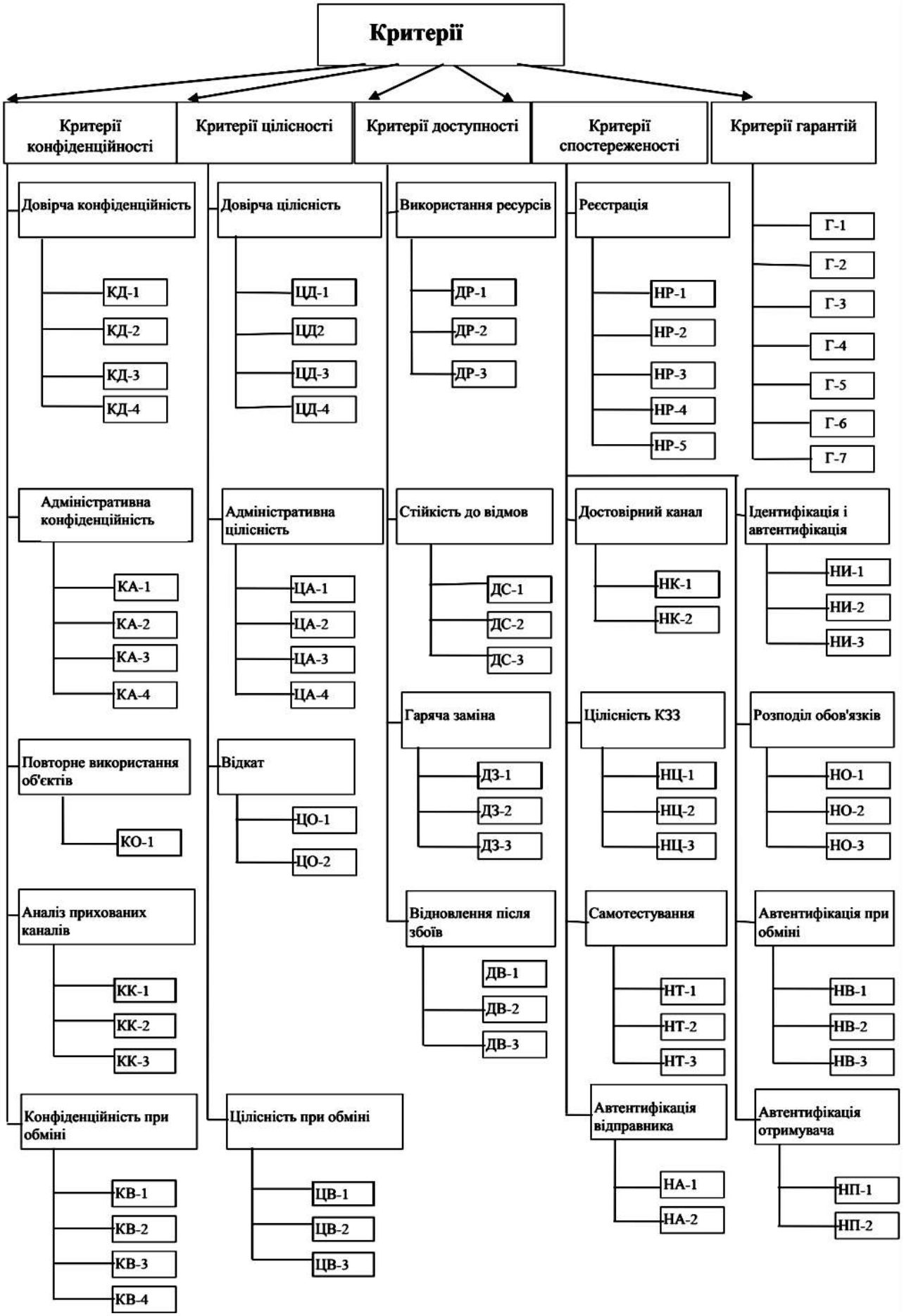


Рисунок 1 – Структура критеріїв

Крім функціональних критеріїв, що дозволяють оцінити наявність послуг безпеки в комп'ютерній системі, цей документ містить критерії гарантій, що дозволяють оцінити коректність реалізації послуг. Критерії гарантій включають вимоги до архітектури комплексу засобів захисту, середовища розробки, послідовності розробки, випробування комплексу засобів захисту, середовища функціонування і експлуатаційної документації. В цих Критеріях вводиться сім рівнів гарантій (Г-1,..., Г-7), які є ієрархічними. Ієрархія рівнів гарантій відбиває поступово наростаючу міру певності в тому, що реалізовані в комп'ютерній системі послуги дозволяють протистояти певним загрозам, що механізми, які їх реалізують, в свою чергу коректно реалізовані і можуть забезпечити очікуваний споживачем рівень захищеності інформації під час експлуатації комп'ютерної системи.

Структуру Критеріїв показано на рисунку 1.

Всі описані послуги є більш-менш незалежними. Якщо ж така залежність виникає, тобто реалізація якої-небудь послуги неможлива без реалізації іншої, то цей факт відбивається як необхідні умови для даної послуги (або її рівня). За винятком послуги *аналіз прихованих каналів* залежність між функціональними послугами і гарантіями відсутня. **Рівень послуги *цілісність комплексу засобів захисту* НЦ-1 є необхідною умовою абсолютно для всіх рівнів всіх інших послуг.**

Порядок оцінки комп'ютерної системи на предмет відповідності цим Критеріям визначається відповідними нормативними документами. Експертна комісія, яка проводить оцінку комп'ютерної системи, визначає, які послуги і на якому рівні реалізовані в даній комп'ютерній системі, і як дотримані вимоги гарантій. Результатом оцінки є рейтинг, що являє собою упорядкований ряд (перелічення) буквено-числових комбінацій, що позначають рівні реалізованих послуг, в поєднанні з рівнем гарантій. Комбінації упорядковуються в порядку опису послуг в критеріях. Для того, щоб до рейтингу комп'ютерної системи міг бути включений певний рівень послуги чи гарантій, повинні бути виконані всі вимоги, перелічені в критеріях для даного рівня послуги або гарантій.

6 Критерії конфіденційності

Для того, щоб КС могла бути оцінена на предмет відповідності критеріям конфіденційності, КЗЗ оцінюваної КС повинен надавати послуги з захисту об'єктів від несанкціонованого ознайомлення з їх змістом (компрометації). Конфіденційність забезпечується такими послугами: довірча конфіденційність, адміністративна конфіденційність, повторне використання об'єктів, аналіз прихованих каналів, конфіденційність при обміні.

6.1 Довірча конфіденційність

Ця послуга дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

<table>
<tr><th>КД-1. Мінімальна довірча конфіденційність</th><th>КД-2. Базова довірча конфіденційність</th><th>КД-3. Повна довірча конфіденційність</th><th>КД-4. Абсолютна довірча конфіденційність</th></tr>
<tr><td colspan="2">Політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься</td><td colspan="2">Політика довірчої конфіденційності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС</td></tr>
<tr><td colspan="4">КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу</td></tr>
<tr><td>процесу і захищеного об'єкта</td><td colspan="2">користувача і захищеного об'єкта</td><td>користувача, процесу і захищеного об'єкта</td></tr>
<tr><td colspan="4">Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта</td></tr>
<tr><td colspan="4">КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити</td></tr>
<tr><td>конкретні процеси і/або групи процесів, які мають право одержувати інформацію від об'єкта</td><td>конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта</td><td>конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта</td><td>конкретних користувачів і процеси (і групи користувачів і процесів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта</td></tr>
<tr><td>—</td><td colspan="3">КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити
конкретних користувачів і/або групи користувачів, які мають право ініціювати процес
конкретних користувачів (і групи користувачів), які мають, а також тих, що не мають права ініціювати процес</td></tr>
<tr><td colspan="4">Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації. Як частина політики довірчої конфіденційності повинні бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту</td></tr>
<tr><td colspan="2">НЕОБХІДНІ УМОВИ: НИ-1</td><td colspan="2">НЕОБХІДНІ УМОВИ: КО-1, НИ-1</td></tr>
</table>

6.2 Адміністративна конфіденційність

Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від захищених об'єктів до користувачів. Рівні даної послуги ран жируються на підставі повноти захисту і вибірковості процесу.

КО-1. Повторне використання об'єктів
Політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною
НЕОБХІДНІ УМОВИ: НЕМАЄ

6.3 Повторне використання об'єктів

Ця послуга дозволяє забезпечити коректність повторного використання розділюваних об'єктів, гарантуючи, що в разі, якщо розділюваний об'єкт виділяється новому користувачу або процесу, то він не містить інформації, яка залишилась від попереднього користувача або процесу.

КО-1. Повторне використання об'єктів
Політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною
НЕОБХІДНІ УМОВИ: НЕМАЄ

6.4 Аналіз прихованих каналів

Аналіз прихованих каналів виконується з метою виявлення і усунення потоків інформації, які існують, але не контролюються іншими послугами. Рівні даної послуги ран жируються на підставі того, чи виконується тільки виявлення, контроль або перекриття прихованих каналів.

КК-1. Виявлення прихованих каналів	**КК-2. Контроль прихованих каналів**	**КК-3. Перекриття прихованих каналів**
Повинен бути виконаний аналіз прихованих каналів		
Всі приховані канали, які існують в апаратному і програмному забезпеченні, а також в програмах ПЗП, повинні бути документовані Має бути документована максимальна пропускна здатність кожного знайденого прихованого каналу, одержана на підставі теоретичної оцінки або вимірів Для прихованих каналів, які можуть використовуватися спільно, повинна бути документована сукупна пропускна здатність		Всі (затверджена підмножина) знайдені під час аналізу приховані канали повинні бути усунені
—	КЗЗ повинен забезпечувати реєстрацію використання затвердженої підмножини знайдених прихованих каналів	
НЕОБХІДНІ УМОВИ: КО-1, Г-3	НЕОБХІДНІ УМОВИ: КО-1, НР-1, Г-3	НЕОБХІДНІ УМОВИ: КО-1, Г-3

6.5 Конфіденційність при обміні

Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ран жируються на підставі повноти захисту і вибірковості керування.

<table>
<tr><th>КВ-1. Мінімальна конфіден-ційність при обміні</th><th>КВ-2. Базова конфіден-ційність при обміні</th><th>КВ-3. Повна конфіден-ційність при обміні</th><th>КВ-4. Абсолютна конфіден-ційність при обміні</th></tr>
<tr><td colspan="2">Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів і інтерфейсних процесів, до яких вона відноситься</td><td colspan="2">Політика конфіденційності при обміні, що реалізується КЗЗ, повинна відноситись до всіх об'єктів і існуючих інтерфейсних процесів</td></tr>
<tr><td colspan="4">Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуються, і спроможність користувачів і/або процесів керувати рівнем захищеності</td></tr>
<tr><td colspan="4">КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається</td></tr>
<tr><td>—</td><td colspan="3">Запити на призначення або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження</td></tr>
<tr><td>—</td><td colspan="3">Запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу
— і приймальника об'єкта</td></tr>
<tr><td>—</td><td colspan="3">Запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу
— і джерела об'єкта</td></tr>
<tr><td colspan="2">—</td><td colspan="2">Представлення захищеного об'єкта має бути функцією атрибутів доступу інтерфейсного процесу, самого об'єкта, а також його джерела і приймальника</td></tr>
</table>

			Політика конфіденційності при обміні повинна включати опис інформації, яку можливо отримати шляхом сумісного аналізу ряду одержаних об'єктів Повинен бути виконаний аналіз прихованих каналів обміну. Всі знайдені приховані канали обміну і максимальна пропускна здатність кожного із них мають бути документовані. Повинна бути забезпечена реєстрація використання затвердженої підмножини знайдених прихованих каналів, їх часткове перекриття або усунення
НЕОБХІДНІ УМОВИ: НЕМАЄ	НО-1	НО-1, НВ-1	НО-1, НВ-1, НР-1, Г-3

7 Критерії цілісності

Для того, щоб КС могла бути оцінена на предмет відповідності критеріям цілісності, КЗЗ оцінюваної КС повинен надавати послуги з захисту оброблюваної інформації від несанкціонованої модифікації. Цілісність забезпечується такими послугами: довірча цілісність, адміністративна цілісність, відкат, цілісність при обміні.

7.1 Довірча цілісність

Ця послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

<table>
<tr><th>ЦД-1. Мінімальна довірча цілісність</th><th>ЦД-2. Базова довірча цілісність</th><th>ЦД-3. Повна довірча цілісність</th><th>ЦД-4. Абсолютна довірча цілісність</th></tr>
<tr><td colspan="2">Політика довірчої цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься</td><td colspan="2">Політика довірчої цілісності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС</td></tr>
<tr><td colspan="4">КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу</td></tr>
<tr><td>користувача і захищеного об'єкта</td><td colspan="2">процесу і захищеного об'єкта</td><td>процесу, користувача і захищеного об'єкта</td></tr>
<tr><td colspan="4">Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта</td></tr>
<tr><td colspan="4">КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити</td></tr>
<tr><td>конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт</td><td>конкретні процеси і/або групи процесів, які мають право модифікувати об'єкт</td><td>конкретні процеси (і групи процесів), які мають, а також тих, що не мають права модифікувати об'єкт</td><td>конкретних користувачів і процеси (і групи користувачів і процесів), які мають, а також тих, що не мають права модифікувати об'єкт</td></tr>
</table>

<table>
<tr><td>—</td><td colspan="2">КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити
конкретних користувачів і/або групи користувачів, які мають право ініціювати процес
конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права ініціювати процес</td></tr>
<tr><td colspan="3">Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту</td></tr>
<tr><td colspan="2">НЕОБХІДНІ УМОВИ: НИ-1</td><td>НЕОБХІДНІ УМОВИ: КО-1, НИ-1</td></tr>
</table>

7.2 Адміністративна цілісність

Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від користувачів до захищених об'єктів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

<table>
<tr><th>ЦА-1. Мінімальна адміністративна цілісність</th><th>ЦА-2. Базова адміністративна цілісність</th><th>ЦА-3. Повна адміністративна цілісність</th><th>ЦА-4. Абсолютна адміністративна цілісність</th></tr>
<tr><td colspan="2">Політика адміністративної цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься</td><td colspan="2">Політика адміністративної цілісності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС</td></tr>
<tr><td colspan="4">КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу</td></tr>
<tr><td>користувача і захищеного об'єкта</td><td colspan="2">процесу і захищеного об'єкта</td><td>процесу, користувача і захищеного об'єкта</td></tr>
<tr><td colspan="4">Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження</td></tr>
<tr><td colspan="4">КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити</td></tr>
<tr><td>конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт</td><td>конкретні процеси і/або групи процесів, які мають право модифікувати об'єкт</td><td>конкретні процеси (і групи процесів), які мають, а також тих, які не мають права модифікувати об'єкт</td><td>конкретних користувачів і процеси (і групи користувачів і процесів), які мають, а також тих, які не мають права модифікувати об'єкт</td></tr>
<tr><td rowspan="2">—</td><td colspan="3">КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного процесу шляхом керування належністю користувачів і процесів до відповідних доменів визначити</td></tr>
<tr><td>конкретних користувачів і/або групи користувачів, які мають право ініціювати процес</td><td colspan="2">конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права ініціювати процес</td></tr>
</table>

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту	
НЕОБХІДНІ УМОВИ: НО-1, НИ-1	НЕОБХІДНІ УМОВИ: КО-1, НО-1, НИ-1

7.3 Відкат

Ця послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкатити) захищений об'єкт до попереднього стану. Рівні даної послуги ранжируються на підставі множини операцій, для яких забезпечується відкат.

<table>
<tr><th>ЦО-1. Обмежений відкат</th><th>ЦО-2. Повний відкат</th></tr>
<tr><td colspan="2">Політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься</td></tr>
<tr><td colspan="2">Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити</td></tr>
<tr><td>певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу</td><td>всі операції, виконані над захищеним об'єктом за певний проміжок часу</td></tr>
<tr><td colspan="2">НЕОБХІДНІ УМОВИ: НИ-1</td></tr>
</table>

7.4 Цілісність при обміні

Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

<table>
<tr><th>ЦВ-1: Мінімальна цілісність при обміні</th><th>ЦВ-2: Базова цілісність при обміні</th><th>ЦВ-3: Повна цілісність при обміні</th></tr>
<tr><td colspan="3">Політика цілісності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів КС і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовуваними механізмами, і спроможність користувачів і/або процесів керувати рівнем захищеності</td></tr>
<tr><td colspan="3">КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається</td></tr>
<tr><td rowspan="2">–</td><td colspan="2">а також фактів його видалення або дублювання</td></tr>
<tr><td colspan="2">Запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу</td></tr>
<tr><td>—</td><td colspan="2">і приймальника об'єкта</td></tr>
<tr><td>—</td><td colspan="2">Запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу</td></tr>
<tr><td>—</td><td colspan="2">і джерела об'єкта</td></tr>
<tr><td>—</td><td colspan="2">Запити на присвоєння або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження</td></tr>
<tr><td colspan="2">—</td><td>Представлення захищеного об'єкта має бути функцією атрибутів доступу інтерфейсного процесу, самого об'єкта, а також його джерела і приймальника</td></tr>
<tr><td>НЕОБХІДНІ УМОВИ: НЕМАЄ</td><td>НО-1</td><td>НО-1, НВ-1</td></tr>
</table>

8 Критерії доступності

Для того, щоб КС могла бути оцінена на відповідність критеріям доступності, КЗЗ оцінюваної КС повинен надавати послуги щодо забезпечення можливості використання КС в цілому, окремих функцій або оброблюваної інформації на певному проміжку часу і гарантувати спроможність КС функціонувати у випадку відмови її компонентів. Доступність може забезпечуватися в КС такими послугами: використання ресурсів, стійкість до відмов, гаряча заміна, відновлення після збоїв.

8.1 Використання ресурсів

Ця послуга дозволяє користувачам керувати використанням послуг і ресурсів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування доступністю послуг КС.

<table>
<tr><th>ДР-1. Квоти</th><th>ДР-2. Недопущення захоплення ресурсів</th><th>ДР-3. Пріоритетність використання ресурсів</th></tr>
<tr><td>Політика використання ресурсів, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься</td><td colspan="2">Політика використання ресурсів, що реалізується КЗЗ, повинна відноситися до всіх об'єктів КС</td></tr>
<tr><td colspan="2">Політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу</td><td>окремому користувачу і довільним групам користувачів</td></tr>
<tr><td colspan="3">Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження</td></tr>
<tr><td>—</td><td colspan="2">Повинна існувати можливість встановлювати обмеження таким чином, щоб КЗЗ мав можливість запобігти діям, які можуть призвести до неможливості доступу інших користувачів до функцій КЗЗ або захищених об'єктів. КЗЗ повинен контролювати такі дії, здійснювані з боку окремого користувача</td><td>окремого користувача і довільних груп користувачів</td></tr>
<tr><td colspan="3">НЕОБХІДНІ УМОВИ: НО-1</td></tr>
</table>

8.2 Стійкість до відмов

Стійкість до відмов гарантує доступність КС (можливість використання інформації, окремих функцій або КС в цілому) після відмови її компонента. Рівні даної послуги ранжируються на підставі спроможності КЗЗ забезпечити можливість функціонування КС в залежності від кількості відмов і послуг, доступних після відмови.

<table>
<tr><th>ДС-1. Стійкість при обмежених відмовах</th><th>ДС-2. Стійкість з погіршенням характеристик обслуговування</th><th>ДС-3. Стійкість без погіршення характеристик обслуговування</th></tr>
<tr><td colspan="3">Розробник повинен провести аналіз відмов компонентів КС</td></tr>
<tr><td>Політика стійкості до відмов, що реалізується КЗЗ, повинна визначати множину компонентів КС, до яких вона відноситься, і типи їх відмов, після яких КС в змозі продовжувати функціонування</td><td colspan="2">Політика стійкості до відмов, що реалізується КЗЗ, повинна відноситися до всіх компонентів КС</td></tr>
<tr><td colspan="3">Повинні бути чітко вказані рівні відмов, при перевищенні яких відмови призводять до зниження характеристик обслуговування або недоступності послуги</td></tr>
<tr><td colspan="2">Відмова одного захищеного компонента не повинна призводити до недоступності всіх послуг, а має в гіршому випадку проявлятися в зниженні характеристик обслуговування</td><td>Відмова одного захищеного компонента не повинна призводити до недоступності всіх послуг або до зниження характеристик обслуговування</td></tr>
<tr><td colspan="3">КЗЗ повинен бути спроможний повідомити адміністратора про відмову будь-якого захищеного компонента</td></tr>
<tr><td colspan="3">НЕОБХІДНІ УМОВИ: НО-1</td></tr>
</table>

8.3 Гаряча заміна

Ця послуга дозволяє гарантувати доступність КС (можливість використання інформації, окремих функцій або КС в цілому) в процесі заміни окремих компонентів. Рівні даної послуги ранжируються на підставі повноти реалізації.

ДЗ-1. Модернізація	**ДЗ-2. Обмежена гаряча заміна**	**ДЗ-3. Гаряча заміна будь-якого компонента**
Політика гарячої заміни, що реалізується КЗЗ, повинна визначати політику проведення модернізації КС	Політика гарячої заміни, що реалізується КЗЗ, повинна визначати множину компонентів КС, які можуть бути замінені без переривання обслуговування	Політика гарячої заміни, що реалізується КЗЗ, повинна забезпечувати можливість заміни будь-якого компонента без переривання обслуговування
Адміністратор або користувачі, яким надані відповідні повноваження, повинні мати можливість провести модернізацію (upgrade) КС. Модернізація КС не повинна призводити до необхідності ще раз проводити інсталяцію КС або до переривання виконання КЗЗ функцій захисту	Адміністратор або користувачі, яким надані відповідні повноваження, повинні мати можливість замінити будь-який захищений компонент	
НЕОБХІДНІ УМОВИ: НО-1	НЕОБХІДНІ УМОВИ: НО-1, ДС-1	

8.4 Відновлення після збоїв

Ця послуга забезпечує повернення КС у відомий захищений стан після відмови або переривання обслуговування. Рівні даної послуги ранжируються на підставі міри автоматизації процесу відновлення.

<table>
<tr><th>ДВ-1. Ручне відновлення</th><th>ДВ-2. Автоматизоване відновлення</th><th>ДВ-3. Вибіркове відновлення</th></tr>
<tr><td colspan="3">Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов КС і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція КС</td></tr>
<tr><td>Після відмови КС або переривання обслуговування КЗЗ повинен перевести КС до стану, із якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження</td><td>Після відмови КС або переривання обслуговування КЗЗ має бути здатним визначити, чи можуть бути використані автоматизовані процедури для повернення КС до нормального функціонування безпечним чином. Якщо такі процедури можуть бути використані, то КЗЗ має бути здатним виконати їх і повернути КС до нормального функціонування</td><td>Після будь-якої відмови КС або переривання обслуговування, що не призводить до необхідності заново інсталювати КС, КЗЗ повинен бути здатним виконати необхідні процедури і безпечним чином повернути КС до нормального функціонування або, в гіршому випадку, функціонування в режимі з погіршеними характеристиками обслуговування</td></tr>
<tr><td>—</td><td colspan="2">Якщо автоматизовані процедури не можуть бути використані, то КЗЗ повинен перевести КС до стану, з якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження</td></tr>
<tr><td colspan="2">Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути КС до нормального функціонування</td><td>повернути КС з режиму з погіршеними характеристиками обслуговування в режим нормального функціонування</td></tr>
<tr><td colspan="3">НЕОБХІДНІ УМОВИ: НО-1</td></tr>
</table>

9 Критерії спостереженості

Для того, щоб КС могла бути оцінена на предмет відповідності критеріям спостереженості, КЗЗ оцінюваної КС повинен надавати послуги з забезпечення відповідальності користувача за свої дії і з підтримки спроможності КЗЗ виконувати свої функції. Спостереженість забезпечується в КС такими послугами: реєстрація (аудит), ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність КЗЗ, самотестування, ідентифікація і автентифікація при обміні, автентифікація відправника, автентифікація отримувача

9.1 Реєстрація

Реєстрація дозволяє контролювати небезпечні для КС дії. Рівні даної послуги ранжируються залежно від повноти і вибірковості контролю, складності засобів аналізу даних журналів реєстрації і спроможності вияву потенційних порушень.

<table>
<tr><th>НР-1. Зовнішній аналіз</th><th>НР-2. Захищений журнал</th><th>НР-3. Сигналізація про небезпеку</th><th>НР-4. Детальна реєстрація</th><th>НР-5. Аналіз в реальному часі</th></tr>
<tr><td colspan="5">Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються</td></tr>
<tr><td colspan="3">КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки</td><td colspan="2">КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє або непряме відношення до безпеки</td></tr>
<tr><td colspan="5">Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події</td></tr>
<tr><td>КЗЗ має бути здатним передавати журнал реєстрації в інші системи з використанням певних механізмів захисту</td><td colspan="4">КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування.
Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації</td></tr>
</table>

	—	КЗЗ має бути здатним контролювати одиничні або повторювані реєстраційні події, які можуть свідчити про прямі (істотні) порушення політики безпеки КС. КЗЗ має бути здатним негайно інформувати адміністратора про перевищення порогів безпеки і, якщо реєстраційні небезпечні події повторюються, здійснити неруйнівні дії щодо припинення повторення цих подій
	—	КЗЗ має бути здатним виявляти і аналізувати несанкціоновані дії в реальному часі
НИ-1	НЕОБХІДНІ УМОВИ: НИ-1, НО-1	

9.2 Ідентифікація і автентифікація

Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до КС. Рівні даної послуги ранжируються залежно від числа задіяних механізмів автентифікації.

<table>
<tr><th>НИ-1. Зовнішня ідентифікація і автентифікація</th><th>НИ-2. Одиночна ідентифікація і автентифікація</th><th>НИ-3. Множинна ідентифікація і автентифікація</th></tr>
<tr><td colspan="3">Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ</td></tr>
<tr><td colspan="3">Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен</td></tr>
<tr><td>з використанням захищеного механізму одержати від деякого зовнішнього джерела автентифікований ідентифікатор цього користувача</td><td>автентифікувати цього користувача з використанням захищеного механізму</td><td>автентифікувати цього користувача з використанням захищених механізмів двох або більше типів</td></tr>
<tr><td>—</td><td colspan="2">КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування</td></tr>
<tr><td>НЕОБХІДНІ УМОВИ: НЕМАЄ</td><td colspan="2">НЕОБХІДНІ УМОВИ: НК-1</td></tr>
</table>

9.3 Достовірний канал

Ця послуга дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ. Рівні даної послуги ранжируються залежно від гнучкості надання можливості КЗЗ або користувачу ініціювати захищений обмін.

НК-1. Однонаправлений достовірний канал	**НК-2. Двонаправлений достовірний канал**
Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ	
Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем	Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації та у випадках, коли необхідний прямий зв'язок користувач/КЗЗ або КЗЗ/користувач. Зв'язок з використанням даного каналу повинен ініціюватися користувачем або КЗЗ
—	Обмін з використанням достовірного каналу, що ініціює КЗЗ, повинен бути однозначно ідентифікований як такий і має відбутися тільки після позитивного підтвердження готовності до обміну з боку користувача
НЕОБХІДНІ УМОВИ: НЕМАЄ	

9.4 Розподіл обов'язків

Ця послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Рівні даної послуги ранжируються на підставі вибірковості керування можливостями користувачів і адміністраторів.

<table>
<tr><th>НО-1. Виділення адміністратора</th><th>НО-2. Розподіл обов'язків адміністраторів</th><th>НО-3. Розподіл обов'язків на підставі привілеїв</th></tr>
<tr><td colspan="3">Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції</td></tr>
<tr><td>—</td><td colspan="2">Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі</td></tr>
<tr><td colspan="2">—</td><td>Політика розподілу обов'язків повинна визначати множину ролей користувачів</td></tr>
<tr><td colspan="3">Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі</td></tr>
<tr><td colspan="3">НЕОБХІДНІ УМОВИ: НИ-1</td></tr>
</table>

9.5 Цілісність комплексу засобів захисту

Ця послуга визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

НЦ-1. КЗЗ з контролем цілісності	**НЦ-2. КЗЗ з гарантованою цілісністю**	**НЦ-3. КЗЗ з функціями диспетчера доступу**
Політика цілісності КЗЗ повинна визначати склад КЗЗ і механізми контролю цілісності компонентів, що входять до складу КЗЗ	Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів	
В разі виявлення порушення цілісності будь-якого із своїх компонентів КЗЗ повинен повідомити адміністратора і або автоматично відновити відповідність компонента еталону або перевести КС до стану, з якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження	КЗЗ повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування	
Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ		КЗЗ повинен гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ
НЕОБХІДНІ УМОВИ: НР-1, НО-1	НЕОБХІДНІ УМОВИ: НЕМАЄ	

9.6 Самотестування

Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Рівні даної послуги ранжируються на підставі можливості виконання тестів у процесі запуску або штатної роботи.

<table>
<tr><th>НТ-1. Самотестування за запитом</th><th>НТ-2. Самотестування при старті</th><th>НТ-3. Самотестування в реальному часі</th></tr>
<tr><td colspan="3">Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ</td></tr>
<tr><td colspan="3">КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження,</td></tr>
<tr><td>—</td><td>при ініціалізації КЗЗ
—</td><td>і в процесі штатного функціонування</td></tr>
<tr><td></td><td colspan="2">НЕОБХІДНІ УМОВИ:
НО-1</td></tr>
</table>

9.7 Ідентифікація і автентифікація при обміні

Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ранжируються на підставі повноти реалізації.

<table>
<tr><th>НВ-1: Автентифікація вузла</th><th>НВ-2: Автентифікація джерела даних</th><th>НВ-3: Автентифікація з підтвердженням</th></tr>
<tr><td colspan="3">Політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ
КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму
Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації</td></tr>
<tr><td>—</td><td colspan="2">КЗЗ повинен використовувати захищені механізми для встановлення джерела кожного об'єкта, що експортується та імпортується</td></tr>
<tr><td colspan="2">—</td><td>Використовуваний протокол автентифікації повинен забезпечувати можливість однозначного підтвердження джерела об'єкта незалежною третьою стороною</td></tr>
<tr><td colspan="3">НЕОБХІДНІ УМОВИ: НЕМАЄ</td></tr>
</table>

9.8 Автентифікація відправника

Ця послуга дозволяє забезпечити захист від відмови від авторства і однозначно встановити належність певного об'єкта певному користувачу, тобто той факт, що об'єкт був створений або відправлений даним користувачем. Рівні даної послуги ранжируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною.

НА-1: Базова автентифікація відправника	**НА-2: Автентифікація відправника з підтвердженням**
Політика автентифікації відправника, що реалізується КЗЗ, повинна визначати множину властивостей і атрибутів об'єкта, що передається, користувача-відправника і інтерфейсного процесу, а також процедури, які дозволяли б однозначно встановити, що даний об'єкт був відправлений (створений) певним користувачем	
—	Додатково повинні бути визначені ті властивості, атрибути і процедури, які можуть використовуватися для однозначного підтвердження належності об'єкта незалежною третьою стороною
Встановлення належності має виконуватися на підставі затвердженого протоколу автентифікації	
—	Встановлення належності має виконуватися на підставі затвердженого протоколу автентифікації
НЕОБХІДНІ УМОВИ: НИ-1	

9.9 Автентифікація отримувача

Ця послуга дозволяє забезпечити захист від відмови від одержання і дозволяє однозначно встановити факт одержання певного об'єкта певним користувачем. Рівні даної послуги ранжируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною.

НП-1: Базова автентифікація отримувача	**НП-2: Автентифікація отримувача з підтвердженням**
Політика автентифікації одержувача, що реалізується КЗЗ, повинна визначати множину властивостей і атрибутів об'єкта, що передається, користувача-одержувача і інтерфейсного процесу, а також процедури, які дозволяли б однозначно встановити, що даний об'єкт був одержаний певним користувачем	
—	Додатково повинні бути визначені ті властивості, атрибути і процедури, які можуть використовуватися незалежною третьою стороною для однозначного підтвердження факту одержання об'єкта
Встановлення одержувача має виконуватися на підставі затвердженого протоколу автентифікації	
—	Використовуваний протокол автентифікації повинен забезпечувати можливість однозначного підтвердження незалежною третьою стороною факту одержання об'єкта
НЕОБХІДНІ УМОВИ: НИ-1	

10 Критерії гарантій

Критерії гарантій включають вимоги до архітектури КЗЗ, середовища розробки, послідовності розробки, середовища функціонування, документації і випробувань КЗЗ. В цих критеріях вводиться сім рівнів гарантій, які є ієрархічними. Вимоги викладаються за розділами. Для того, щоб КС одержала певний рівень гарантій (якщо вона не може одержати більш високий), повинні бути задоволені всі вимоги, визначені для даного рівня в кожному з розділів.

10.1 Архітектура

Вимоги до архітектури забезпечують гарантії того, що КЗЗ у змозі повністю реалізувати політику безпеки.

Вимоги	**Г-1**	**Г-2**	**Г-3**	**Г-4**	**Г-5**	**Г-6**	**Г-7**
КЗЗ повинен реалізовувати політику безпеки. Всі його компоненти повинні бути чітко визначені	+	=	=	=	=	=	=
КЗЗ повинен складатися з добре визначених і максимально незалежних компонентів. Кожний з компонентів повинен бути спроектований відповідно до принципу мінімуму повноважень	-	-	+	=	=	=	=
Критичні для безпеки компоненти КЗЗ повинні бути захищені від не критичних для безпеки за рахунок використання механізмів захисту, які надаються програмно-апаратними засобами більш низького рівня	-	-	-	+	=	=	=
З боку Розробника мають бути вжиті зусилля, спрямовані на виключення з КЗЗ компонентів, що не є критичними для безпеки. Мають бути наведені підстави для включення до КЗЗ будь-якого елемента, який не має відношення до захисту	-	-	-	-	+	=	=

Розробка ПЗ переважно має бути спрямована на мінімізацію складності КЗЗ. КЗЗ має бути спроектований і структурований так, щоб використовувати повний і концептуально простий механізм захисту з точно визначеною семантикою. Цей механізм повинен відігравати центральну роль в реалізації внутрішньої структури КЗЗ. Під час розробки КЗЗ значною мірою повинні бути задіяні такі підходи як модульність побудови і приховання (локалізація) даних	- - - -	+	=	=

* В таблицях використовуються такі позначення: “-” – вимога відсутня; “+” – вимога з'являється; “=“ – вимога зберігається.

10.2 Середовище розробки

Вимоги до середовища розробки забезпечують гарантії того, що процеси розробки і супроводження оцінюваної КС є повністю керованими з боку Розробника.

Вимоги	**Г-1**	**Г-2**	**Г-3**	**Г-4**	**Г-5**	**Г-6**	**Г-7**
Процес розробки							
Розробник повинен визначити всі стадії життєвого циклу КС, розробити, запровадити і підтримувати в робочому стані документально оформлені методики своєї діяльності на кожній стадії. Мають бути документовані всі етапи кожної стадії життєвого циклу і їх граничні вимоги	+	=	=	=	=	=	=
Розробник повинен описати стандарти кодування, яким необхідно додержуватися в процесі реалізації, і повинен гарантувати, що всі вихідні коди компілюються відповідно до цих стандартів. Будь-яка з використовуваних під час реалізації мов програмування має бути добре визначена. Всі залежні від реалізації параметри мов програмування або компіляторів повинні бути документовані	-	-	+	=	=	=	=
Розробник повинен розробити, запровадити і підтримувати в робочому стані документально оформлені методики забезпечення фізичної, технічної, організаційної і кадрової безпеки	-	-	-	+	=	=	=

Керування конфігурацією							
Розробник повинен розробити, запровадити і підтримувати в робочому стані документовані методики щодо керування конфігурацією КС на всіх стадіях її життєвого циклу. Система керування конфігурацією повинна забезпечувати керування внесенням змін в апаратне забезпечення, програми ПЗП, вихідні тексти, об'єктні коди, тестове покриття і документацію. Система керування конфігурацією повинна гарантувати постійну відповідність між всією документацією і реалізацією поточної версії КЗЗ	+	=	=	+ *	=	=	=
Система керування конфігурацією також повинна використовуватися для генерації КЗЗ з вихідного коду і обліку всіх змін з появою нових версій	-	-	-	+	=	=	=
Система керування конфігурацією повинна бути здатна видавати звіти про стан елементів конфігурації	-	-	-	+	=	=	=
Повинна використовуватися система заходів технічної, фізичної, організаційної і кадрової безпеки, спрямованих на захист усіх засобів і матеріалів, використовуваних для генерації КЗЗ, від несанкціонованої модифікації або руйнування	-	-	-	-	-	+	=

* Починаючи з рівня Г-4 система керування конфігурацією повинна базуватися на автоматизованих засобах.

10.3 Послідовність розробки

Вимоги до процесу проектування (послідовності розробки) забезпечують гарантії того, що на кожній стадії розробки (проектування) існує точний опис КС і реалізація КС точно відповідає вихідним вимогам (політиці безпеки).

<table>
<tr><th>Вимоги</th><th>Г-1</th><th>Г-2</th><th>Г-3</th><th>Г-4</th><th>Г-5</th><th>Г-6</th><th>Г-7</th></tr>
<tr><td colspan="8">Функціональні специфікації (політика безпеки)</td></tr>
<tr><td>На стадії розробки технічного завдання Розробник повинен розробити функціональні специфікації КС. Представлені функціональні специфікації повинні включати неформалізований опис політики безпеки, що реалізується КЗЗ. Політика безпеки повинна містити перелік і опис послуг безпеки, що надаються КЗЗ</td><td>+</td><td>=</td><td>=</td><td>=</td><td>=</td><td>=</td><td>=</td></tr>
<tr><td colspan="8">Функціональні специфікації (модель політики безпеки)</td></tr>
<tr><td>Відповідність політиці безпеки</td><td>-</td><td colspan="2">Показ</td><td colspan="4">Демонстрація</td></tr>
<tr><td>Функціональні специфікації повинні включати модель політики безпеки</td><td>-</td><td>+</td><td>=</td><td>=</td><td>=</td><td>=</td><td>=</td></tr>
<tr><td rowspan="3">Стиль специфікації:
неформалізована
частково формалізована
формалізована</td><td>-</td><td></td><td></td><td colspan="4" rowspan="2"></td></tr>
<tr><td>-</td><td></td><td></td></tr>
<tr><td>-</td><td></td><td></td><td colspan="4"></td></tr>
<tr><td colspan="8">Проект архітектури</td></tr>
<tr><td>Відповідність моделі політики безпеки</td><td>-</td><td colspan="3">Показ</td><td>Демонстрація</td><td colspan="2">Доказ</td></tr>
<tr><td>На стадії розробки ескізного проекту Розробник повинен розробити проект архітектури КЗЗ. Представлений проект повинен містити перелік і опис компонентів КЗЗ і функцій, що реалізуються ними. Повинні бути описані будь-які використовувані зовнішні послуги безпеки. Зовнішні інтерфейси КЗЗ повинні бути описані в термінах винятків, повідомлень про помилки і кодів повернення</td><td>+</td><td>=</td><td>=</td><td>=</td><td>=</td><td>=</td><td>=</td></tr>
</table>

Стиль специфікації: неформалізована							
частково формалізована							
формалізована							
Детальний проект							
Відповідність проекту архітектури	-	Показ				Демонстрація	Доказ
На стадіях розробки технічного проекту або робочого проекту Розробник повинен розробити детальний проект КЗЗ. Представлений детальний проект повинен містити перелік всіх компонентів КЗЗ і точний опис функціонування кожного механізму. Повинні бути описані призначення і параметри інтерфейсів компонентів КЗЗ	+	=	=	=	=	=	=
Стиль специфікації: неформалізована		Весь КЗЗ *					
частково формалізована							
формалізована							
Реалізація							
Відповідність детальному проекту	-	-	Показ				Демонстрація
Розробник повинен подати вихідний код: частини КЗЗ	-	-	+	=	=	=	=
всього КЗЗ	-	-	-	-	+	=	=
всіх бібліотек часу виконання	-	-	-	-	-	-	+

* Для рівня Г-1 вимагається детальний проект компонентів КЗЗ, що мають безпосереднє відношення до безпеки.

10.4 Середовище функціонування

Вимоги до середовища функціонування забезпечують гарантії того, що КС поставляється Замовнику без несанкціонованих модифікацій, а також інсталюється і ініціюється Замовником так, як це передбачається Розробником.

Вимоги	**Г-1**	**Г-2**	**Г-3**	**Г-4**	**Г-5**	**Г-6**	**Г-7**
Розробник повинен представити засоби інсталяції, генерації і запуску КС, які гарантують, що експлуатація КС починається з безпечного стану. Розробник повинен представити перелік усіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації і запуску	+	=	=	=	=	=	=
Повинна існувати система технічних, організаційних і фізичних заходів безпеки, яка гарантує, що програмне і програмно-апаратне забезпечення КЗЗ, яке поставляється Замовнику, точно відповідає еталонній копії	-	-	+	=	=	=	=
Для підтримки відповідності між КЗЗ, що поставляється Замовнику, і еталонною копією повинна існувати система керування розповсюдженням захищеної КС	-	-	-	-	-	+	=

10.5 Документація

Вимоги до документації є загальними для всіх рівнів гарантій.

У вигляді окремих документів або розділів (підрозділів) інших документів Розробник повинен подати опис послуг безпеки, що реалізуються КЗЗ, настанови адміністратору щодо послуг безпеки, настанови користувача щодо послуг безпеки.

В описі функцій безпеки повинні бути викладені основні, необхідні для правильного використання послуг безпеки, принципи політики безпеки, що реалізується КЗЗ оцінюваної КС, а також самі послуги.

Настанови адміністратору щодо послуг безпеки мають містити опис засобів інсталяції, генерації і запуску КС, опис всіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації і запуску КС, опис властивостей КС, які можуть бути використані для періодичної оцінки правильності функціонування КЗЗ, а також інструкції щодо використання адміністратором послуг безпеки для підтримки політики безпеки, прийнятої в організації, що експлуатує КС.

Настанови користувачу щодо послуг безпеки мають містити інструкції щодо використання функцій безпеки звичайним користувачем (не адміністратором).

Назва документів (розділів) не регламентується. Опис послуг безпеки може відрізнятися для користувача і адміністратора. Настанови адміністратору і настанови користувачу можуть бути об'єднані в настанови з установлення і експлуатації.

10.6 Випробування комплексу засобів захисту

Вимоги	**Г-1**	**Г-2**	**Г-3**	**Г-4**	**Г-5**	**Г-6**	**Г-7**
Розробник повинен подати для перевірки програму і методику випробувань, процедури випробувань усіх механізмів, що реалізують послуги безпеки. Мають бути представлені аргументи для підтвердження достатності тестового покриття	+	=	=	=	=	=	=
Розробник повинен подати докази тестування у вигляді детального переліку результатів тестів і відповідних процедур тестування, з тим, щоб отримані результати могли бути перевірені шляхом повторення тестування	+	=	=	=	=	=	=
Розробник повинен усунути або нейтралізувати всі знайдені “слабкі місця” і виконати повторне тестування КЗЗ для підтвердження того, що виявлені недоліки були усунені і не з'явилися нові “слабкі місця ”	-	+	=	=	=	=	=
Розробник повинен виконати тести з подолання механізмів захисту і довести, що КЗЗ відносно або абсолютно стійкий до такого роду атак з боку Розробника	-	-	-	+	=	+	=

А.12. Закон України «Про доступ до публічної інформації»

Цей Закон визначає порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом, та інформації, що становить суспільний інтерес, та складається з наступних розділів і статей.

Розділ I. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Публічна інформація

Стаття 2. Мета і сфера дії Закону

Стаття 3. Гарантії забезпечення права на доступ до публічної інформації

Стаття 4. Принципи забезпечення доступу до публічної інформації

Розділ II. ПОРЯДОК ДОСТУПУ ДО ІНФОРМАЦІЇ

Стаття 5. Забезпечення доступу до інформації

Стаття 6. Публічна інформація з обмеженим доступом

Стаття 7. Конфіденційна інформація

Стаття 8. Таємна інформація

Стаття 9. Службова інформація

Стаття 10. Доступ до інформації про особу

Стаття 10. Публічна інформація у формі відкритих даних

Стаття 11. Захист особи, яка оприлюднює інформацію

Розділ III. СУБ'ЄКТИ ВІДНОСИН У СФЕРІ ДОСТУПУ ДО ПУБЛІЧНОЇ ІНФОРМАЦІЇ

Стаття 12. Визначення та перелік суб'єктів

Стаття 13. Розпорядники інформації

Стаття 14. Обов'язки розпорядників інформації

Стаття 15. Оприлюднення інформації розпорядниками

Стаття 16. Відповідальні особи з питань доступу до публічної інформації

Стаття 17. Контроль за забезпеченням доступу до публічної інформації

Стаття 18. Реєстрація документів розпорядника інформації

Розділ IV. РЕАЛІЗАЦІЯ ПРАВА НА ДОСТУП ДО ІНФОРМАЦІЇ ЗА ІНФОРМАЦІЙНИМ ЗАПИТОМ

Стаття 19. Оформлення запитів на інформацію

Стаття 20. Строк розгляду запитів на інформацію

Стаття 21. Плата за надання інформації

Стаття 22. Відмова та відстрочка в задоволенні запиту на інформацію

Розділ V. ОСКАРЖЕННЯ РІШЕНЬ, ДІЙ ЧИ БЕЗДІЯЛЬНОСТІ РОЗПОРЯДНИКІВ ІНФОРМАЦІЇ

Стаття 23. Право на оскарження рішень, дій чи бездіяльності розпорядників інформації

Стаття 24. Відповідальність за порушення законодавства про доступ до публічної інформації

Розділ І. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Публічна інформація

1. Публічна інформація – це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом.

2. Публічна інформація є відкритою, крім випадків, встановлених законом.

Стаття 2. Мета і сфера дії Закону

1. Метою цього Закону є забезпечення прозорості та відкритості суб'єктів владних повноважень і створення механізмів реалізації права кожного на доступ до публічної інформації.

2. Цей Закон не поширюється на відносини щодо отримання інформації суб'єктами владних повноважень при здійсненні ними своїх функцій, а також на відносини у сфері звернень громадян, які регулюються спеціальним законом.

Стаття 3. Гарантії забезпечення права на доступ до публічної інформації

1. Право на доступ до публічної інформації гарантується:

– обов'язком розпорядників інформації надавати та оприлюднювати інформацію, крім випадків, передбачених законом;

– визначенням розпорядником інформації спеціальних структурних підрозділів або посадових осіб, які організовують у встановленому порядку доступ до публічної інформації, якою він володіє;

– максимальним спрощенням процедури подання запиту та отримання інформації;

– доступом до засідань колегіальних суб'єктів владних повноважень, крім випадків, передбачених законодавством;

– здійсненням парламентського, громадського та державного контролю за дотриманням прав на доступ до публічної інформації;

– юридичною відповідальністю за порушення законодавства про доступ до публічної інформації.

Стаття 4. Принципи забезпечення доступу до публічної інформації

1. Доступ до публічної інформації відповідно до цього Закону здійснюється на принципах:

– прозорості та відкритості діяльності суб'єктів владних повноважень;

– вільного отримання, поширення та будь-якого іншого використання інформації, що була надана або оприлюднена відповідно до цього Закону, крім обмежень, встановлених законом;

– рівноправності, незалежно від ознак раси, політичних, релігійних та інших переконань, статі, етнічного та соціального походження, майнового стану, місця проживання, мовних або інших ознак.

Розділ ІІ. ПОРЯДОК ДОСТУПУ ДО ІНФОРМАЦІЇ

Стаття 5. Забезпечення доступу до інформації

1. Доступ до інформації забезпечується шляхом:

1) систематичного та оперативного оприлюднення інформації:

– в офіційних друкованих виданнях;

– на офіційних веб-сайтах в мережі Інтернет;

– на єдиному державному веб-порталі відкритих даних;

– на інформаційних стендах;

– будь-яким іншим способом;

2) надання інформації за запитами на інформацію.

Стаття 6. Публічна інформація з обмеженим доступом

1. Інформацією з обмеженим доступом є:

– конфіденційна інформація;

– таємна інформація;

– службова інформація.

2. Обмеження доступу до інформації здійснюється відповідно до закону при дотриманні сукупності таких вимог:

– виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи кримінальним правопорушенням, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя;

– розголошення інформації може завдати істотної шкоди цим інтересам;

– шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

3. Інформація з обмеженим доступом має надаватися розпорядником інформації, якщо він правомірно оприлюднив її раніше.

4. Інформація з обмеженим доступом має надаватися розпорядником інформації, якщо немає законних підстав для обмеження у доступі до такої інформації, які існували раніше.

5. Не може бути обмежено доступ до інформації про складання, розгляд і затвердження бюджетів, кошторисів розпорядників бюджетних коштів та плани використання бюджетних коштів одержувачів бюджетних коштів, а також їх виконання за розписами, бюджетними програмами та видатками (крім таємних видатків відповідно до статті 31 Бюджетного кодексу України), взяття розпорядниками та одержувачами бюджетних коштів бюджетних зобов’язань або здійснення розпорядження бюджетними коштами у будь-який інший спосіб, планування, формування, здійснення та виконання закупівлі товарів, робіт і послуг за бюджетні кошти, у тому числі оборонних закупівель (крім випадків, якщо окрема інформація про закупівлі товарів, робіт і послуг становить державну таємницю відповідно до Закону України "Про державну таємницю"), володіння, користування чи розпорядження державним, комунальним майном, у тому числі до копій відповідних документів, умови отримання цих коштів чи майна, прізвища, імена, по батькові фізичних осіб та найменування юридичних осіб, які отримали ці кошти або майно (крім випадків, передбачених частиною

другою статті 23 Закону України "Про основи національного спротиву"). Не може бути також обмежено доступ до інформації про наявність у фізичних осіб податкового боргу. Не підлягає обмеженню також доступ до інформації про стан і результати перевірок та службових розслідувань фактів порушень, допущених у сферах діяльності, зазначених у цій частині. Доступ до зазначеної інформації забезпечується розпорядниками інформації відповідно до положень статті 5 цього Закону.

6. Не належать до інформації з обмеженим доступом відомості, зазначені у декларації особи, уповноваженої на виконання функцій держави або місцевого самоврядування, поданій відповідно до Закону України "Про запобігання корупції", крім випадків, визначених зазначеним Законом.

7. Не належить до інформації з обмеженим доступом інформація про структуру, принципи формування та розмір оплати праці, винагороди, додаткового блага керівника, заступника керівника юридичної особи публічного права, керівника, заступника керівника, члена наглядової ради державного чи комунального підприємства або державної чи комунальної організації, що має на меті одержання прибутку, особи, яка постійно або тимчасово обіймає посаду члена виконавчого органу чи входить до складу наглядової ради господарського товариства, у статутному капіталі якого більше 50 відсотків акцій (часток, паїв) прямо чи опосередковано належать державі та/або територіальній громаді.

8. Обмеженню доступу підлягає інформація, а не документ. Якщо документ містить інформацію з обмеженим доступом, для ознайомлення надається інформація, доступ до якої необмежений.

Стаття 7. Конфіденційна інформація

1. Конфіденційна інформація – інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов. Не може бути віднесена до конфіденційної інформація, зазначена в частині першій і другій статті 13 цього Закону.

2. Розпорядники інформації, визначені частиною першою статті 13 цього Закону, які володіють конфіденційною інформацією, можуть поширювати її лише за згодою осіб, які обмежили доступ до інформації, а за відсутності такої згоди – лише в інтересах національної безпеки, економічного добробуту та прав людини.

Стаття 8. Таємна інформація

1. Таємна інформація – інформація, доступ до якої обмежується відповідно до частини другої статті 6 цього Закону, розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську, розвідувальну таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю.

2. Порядок доступу до таємної інформації регулюється цим Законом та спеціальними законами.

Стаття 9. Службова інформація

1. Відповідно до вимог частини другої статті 6 цього Закону до службової може належати така інформація:

– що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

– зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

2. Документам, що містять інформацію, яка становить службову інформацію, присвоюється гриф "для службового користування". Доступ до таких документів надається відповідно до частини другої статті 6 цього Закону.

3. Перелік відомостей, що становлять службову інформацію, який складається органами державної влади, органами місцевого самоврядування, іншими суб'єктами владних повноважень, у тому числі на виконання делегованих повноважень, не може бути обмеженим у доступі.

Стаття 10. Доступ до інформації про особу

1. Кожна особа має право:

– знати у період збирання інформації, але до початку її використання, які відомості про неї та з якою метою збираються, як, ким і з якою метою вони використовуються, передаються чи поширюються, крім випадків, встановлених законом;

– доступу до інформації про неї, яка збирається та зберігається;

– вимагати виправлення неточної, неповної, застарілої інформації про себе, знищення інформації про себе, збирання, використання чи зберігання якої здійснюється з порушенням вимог закону;

– на ознайомлення за рішенням суду з інформацією про інших осіб, якщо це необхідно для реалізації та захисту прав та законних інтересів;

– на відшкодування шкоди у разі розкриття інформації про цю особу з порушенням вимог, визначених законом.

2. Обсяг інформації про особу, що збирається, зберігається і використовується розпорядниками інформації, має бути максимально обмеженим і використовуватися лише з метою та у спосіб, визначений законом.

3. Розпорядники інформації, які володіють інформацією про особу, зобов'язані:

– надавати її безперешкодно і безкоштовно на вимогу осіб, яких вона стосується, крім випадків, передбачених законом;

– використовувати її лише з метою та у спосіб, визначений законом;

– вживати заходів щодо унеможливлення несанкціонованого доступу до неї інших осіб;

4) виправляти неточну та застарілу інформацію про особу самостійно або на вимогу осіб, яких вона стосується.

4. Зберігання інформації про особу не повинно тривати довше, ніж це необхідно для досягнення мети, задля якої ця інформація збиралася.

5. Відмова особі в доступі до інформації про неї, приховування, незаконне збирання, використання, зберігання чи поширення інформації можуть бути оскаржені.

Стаття 10. Публічна інформація у формі відкритих даних

1. Публічна інформація у формі відкритих даних – це публічна інформація у форматі, що дозволяє її автоматизоване оброблення електронними засобами, вільний та безоплатний доступ до неї, а також її подальше використання.

Розпорядники інформації зобов'язані надавати публічну інформацію у формі відкритих даних на запит, оприлюднювати і регулярно оновлювати її на єдиному державному веб-порталі відкритих даних та на своїх веб-сайтах.

2. Публічна інформація у формі відкритих даних є дозволеною для її подальшого вільного використання та поширення.

Будь-яка особа може вільно копіювати, публікувати, поширювати, використовувати, у тому числі в комерційних цілях, у поєднанні з іншою інформацією або шляхом включення до складу власного продукту, публічну інформацію у формі відкритих даних з обов'язковим посиланням на джерело отримання такої інформації.

3. Публічна інформація, що містить персональні дані фізичної особи, оприлюднюється та надається на запит у формі відкритих даних у разі додержання однієї з таких умов:

– персональні дані знеособлені та захищені відповідно до Закону України "Про захист персональних даних";

– фізичні особи (суб'єкти даних), персональні дані яких містяться в інформації у формі відкритих даних, надали свою згоду на поширення таких даних відповідно до Закону України "Про захист персональних даних";

– надання чи оприлюднення такої інформації передбачено законом;

– обмеження доступу до такої інформації (віднесення її до інформації з обмеженим доступом) заборонено законом.

4. Перелік наборів даних, що підлягають оприлюдненню у формі відкритих даних, вимоги до формату і структури таких наборів даних, періодичність їх оновлення визначаються Кабінетом Міністрів України. При цьому до такого переліку Кабінет Міністрів України обов'язково включає інформацію, доступ до якої у формі відкритих даних передбачено законом.

Створення та забезпечення функціонування єдиного державного веб-порталу відкритих даних здійснюється центральним органом виконавчої влади, що реалізує державну політику у сфері електронного урядування.

Стаття 11. Захист особи, яка оприлюднює інформацію

1. Посадові та службові особи не підлягають юридичній відповідальності, незважаючи на порушення своїх обов'язків, за розголошення інформації про правопорушення або відомостей, що стосуються серйозної загрози здоров'ю чи безпеці громадян, довкіллю, якщо особа при цьому керувалася добрими намірами та мала обґрунтоване переконання, що інформація є достовірною, а

також містить докази правопорушення або стосується істотної загрози здоров'ю чи безпеці громадян, довкіллю.

Розділ ІІІ. СУБ'ЄКТИ ВІДНОСИН У СФЕРІ ДОСТУПУ ДО ПУБЛІЧНОЇ ІНФОРМАЦІЇ

Стаття 12. Визначення та перелік суб'єктів

1. Суб'єктами відносин у сфері доступу до публічної інформації є:

– запитувачі інформації – фізичні, юридичні особи, об'єднання громадян без статусу юридичної особи, крім суб'єктів владних повноважень;

– розпорядники інформації – суб'єкти, визначені у статті 13 цього Закону;

– структурний підрозділ або відповідальна особа з питань доступу до публічної інформації розпорядників інформації.

Стаття 13. Розпорядники інформації

1. Розпорядниками інформації для цілей цього Закону визнаються:

– суб'єкти владних повноважень – органи державної влади, інші державні органи, органи місцевого самоврядування, органи влади Автономної Республіки Крим, інші суб'єкти, що здійснюють владні управлінські функції відповідно до законодавства та рішення яких є обов'язковими для виконання;

– юридичні особи, що фінансуються з державного, місцевих бюджетів, бюджету Автономної Республіки Крим, – стосовно інформації щодо використання бюджетних коштів;

– особи, якщо вони виконують делеговані повноваження суб'єктів владних повноважень згідно із законом чи договором, включаючи надання освітніх, оздоровчих, соціальних або інших державних послуг, – стосовно інформації, пов'язаної з виконанням їхніх обов'язків;

– суб'єкти господарювання, які займають домінуюче становище на ринку або наділені спеціальними чи виключними правами, або є природними монополіями, – стосовно інформації щодо умов постачання товарів, послуг та цін на них;

– юридичні особи публічного права, державні/комунальні підприємства або державні/комунальні організації, що мають на меті одержання прибутку, господарські товариства, у статутному капіталі яких більше 50 відсотків акцій (часток, паїв) прямо чи опосередковано належать державі та/або територіальній громаді, – щодо інформації про структуру, принципи формування та розмір оплати праці, винагороди, додаткового блага їх керівника, заступника керівника, особи, яка постійно або тимчасово обіймає посаду члена виконавчого органу чи входить до складу наглядової ради.

2. До розпорядників інформації, зобов'язаних оприлюднювати та надавати за запитами інформацію, визначену в цій статті, у порядку, передбаченому цим Законом, прирівнюються суб'єкти господарювання, які володіють:

– інформацією про стан довкілля;

– інформацією про якість харчових продуктів і предметів побуту;

– інформацією про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, що сталися або можуть статися і загрожують здоров'ю та безпеці громадян;

– іншою інформацією, що становить суспільний інтерес (суспільно необхідною інформацією).

3. На розпорядників інформації, визначених у пунктах 2, 3, 4 частини першої та в частині другій цієї статті, юридичних осіб публічного права з числа розпорядників інформації, визначених у пункті 5 частини першої цієї статті, вимоги цього Закону поширюються лише в частині надання відповідної інформації за запитами.

4. Усі розпорядники інформації незалежно від нормативно-правового акта, на підставі якого вони діють, при вирішенні питань щодо доступу до інформації мають керуватися цим Законом.

Стаття 14. Обов'язки розпорядників інформації

1. Розпорядники інформації зобов'язані:

– оприлюднювати інформацію, передбачену цим та іншими законами;

– систематично вести облік документів, що знаходяться в їхньому володінні;

– вести облік запитів на інформацію;

– визначати спеціальні місця для роботи запитувачів з документами чи їх копіями, а також надавати право запитувачам робити виписки з них, фотографувати, копіювати, сканувати їх, записувати на будь-які носії інформації тощо;

– мати спеціальні структурні підрозділи або призначати відповідальних осіб для забезпечення доступу запитувачів до інформації та оприлюднення інформації;

– надавати та оприлюднювати достовірну, точну та повну інформацію, а також у разі потреби перевіряти правильність та об’єктивність наданої інформації і оновлювати оприлюднену інформацію.

Стаття 15. Оприлюднення інформації розпорядниками

1. Розпорядники інформації зобов'язані оприлюднювати:

– інформацію про організаційну структуру, місію, функції, повноваження, основні завдання, напрями діяльності та фінансові ресурси (структуру та обсяг бюджетних коштів, порядок та механізм їх витрачання, структуру, принципи формування та розмір оплати праці, винагороди, додаткового блага керівника, заступника керівника юридичної особи публічного права, керівника, заступника керівника, члена наглядової ради державного чи комунального підприємства або державної чи комунальної організації, що має на меті одержання прибутку, особи, яка постійно або тимчасово обіймає посаду члена виконавчого органу чи входить до складу наглядової ради господарського товариства, у статутному капіталі якого більше 50 відсотків акцій (часток, паїв) прямо чи опосередковано належать державі та/або територіальній громаді, тощо), а також інформацію, зазначену в частині п’ятій статті 6 цього Закону;

– нормативно-правові акти, акти індивідуальної дії (крім внутрішньоорганізаційних), прийняті розпорядником, проекти рішень, що підлягають обговоренню, інформацію про нормативно-правові засади діяльності;

– перелік та умови отримання послуг, що надаються цими органами, форми і зразки документів, правила їх заповнення;

– порядок складання, подання запиту на інформацію, оскарження рішень розпорядників інформації, дій чи бездіяльності;

– інформацію про систему обліку, види інформації, яку зберігає розпорядник;

– перелік наборів даних, що оприлюднюються у формі відкритих даних;

– інформацію про механізми чи процедури, за допомогою яких громадськість може представляти свої інтереси або в інший спосіб впливати на реалізацію повноважень розпорядника інформації;

– плани проведення та порядок денний своїх відкритих засідань;

– розташування місць, де надаються необхідні запитувачам форми і бланки установи;

– загальні правила роботи установи, правила внутрішнього трудового розпорядку;

– звіти, в тому числі щодо задоволення запитів на інформацію;

– інформацію про діяльність суб'єктів владних повноважень, а саме про:

– їхні місцезнаходження, поштову адресу, номери засобів зв'язку, адреси офіційного веб-сайту та електронної пошти;

– прізвище, ім'я та по батькові, службові номери засобів зв'язку, адреси електронної пошти керівника органу та його заступників, а також керівників структурних та регіональних підрозділів, основні функції структурних та регіональних підрозділів, крім випадків, коли ці відомості належать до інформації з обмеженим доступом;

– розклад роботи та графік прийому громадян;

– вакансії, порядок та умови проходження конкурсу на заміщення вакантних посад;

– перелік та умови надання послуг, форми і зразки документів, необхідних для надання послуг, правила їх оформлення;

– перелік і службові номери засобів зв'язку підприємств, установ та організацій, що належать до сфери їх управління, та їх керівників, крім підприємств, установ та організацій, створених з метою конспірації, оперативно-розшукової або контррозвідувальної діяльності;

– порядок складання, подання запиту на інформацію, оскарження рішень суб'єктів владних повноважень, їх дій чи бездіяльності;

– систему обліку, види інформації, якою володіє суб'єкт владних повноважень;

– іншу інформацію про діяльність суб'єктів владних повноважень, порядок обов'язкового оприлюднення якої встановлений законом.

2. Інформація, передбачена частиною першою цієї статті, підлягає обов’язковому оприлюдненню невідкладно, але не пізніше п’яти робочих днів з дня затвердження документа, крім випадків, передбачених частиною третьою цієї статті. У разі наявності у розпорядника інформації офіційного веб-сайту така інформація оприлюднюється на веб-сайті із зазначенням дати оприлюднення документа і дати оновлення інформації.

3. Визначені у пункті 5 частини першої статті 13 цього Закону державні чи комунальні підприємства, державні чи комунальні організації, що мають на меті одержання прибутку, господарські товариства, у статутному капіталі яких більше 50 відсотків акцій (часток, паїв) прямо чи опосередковано належать державі та/або територіальній громаді, щомісяця (не пізніше 5 числа наступного місяця) та за підсумками року (не пізніше 1 лютого наступного року) оприлюднюють на своєму офіційному веб-сайті інформацію про структуру, принципи формування та розмір оплати праці, винагороди, додаткового блага їх керівника, заступника керівника, особи, яка постійно або тимчасово обіймає посаду члена виконавчого органу чи входить до складу наглядової ради, із зазначенням дати оприлюднення і оновлення такої інформації.

4. Проекти нормативно-правових актів, рішень органів місцевого самоврядування, розроблені відповідними розпорядниками, оприлюднюються ними не пізніш як за 10 робочих днів до дати їх розгляду з метою прийняття.

Вимоги цієї частини щодо строку оприлюднення не застосовуються до проектів рішень органів місцевого самоврядування, спрямованих на надання адміністративних послуг, якщо це призведе до порушення встановленого законом строку надання відповідної адміністративної послуги.

5. Невідкладному оприлюдненню підлягає будь-яка інформація про факти, що загрожують життю, здоров'ю та/або майну осіб, і про заходи, які застосовуються у зв'язку з цим.

Стаття 16. Відповідальні особи з питань доступу до публічної інформації

1. Розпорядник інформації відповідає за визначення завдань та забезпечення діяльності структурного підрозділу або відповідальної особи з питань доступу до публічної інформації розпорядників інформації, відповідальних за опрацювання, систематизацію, аналіз та контроль щодо задоволення запиту на інформацію, надання консультацій під час оформлення запиту, а також за оприлюднення інформації, передбаченої цим Законом.

2. Запит, що пройшов реєстрацію в установленому розпорядником інформації порядку, обробляється відповідальними особами з питань доступу до публічної інформації.

Стаття 17. Контроль за забезпеченням доступу до публічної інформації

1. Парламентський контроль за дотриманням права людини на доступ до інформації здійснюється Уповноваженим Верховної Ради України з прав людини, тимчасовими слідчими комісіями Верховної Ради України, народними депутатами України.

2. Громадський контроль за забезпеченням розпорядниками інформації доступу до публічної інформації здійснюється депутатами місцевих рад, громадськими організаціями, громадськими радами, громадянами особисто шляхом проведення відповідних громадських слухань, громадської експертизи тощо.

3. Державний контроль за забезпеченням розпорядниками інформації доступу до інформації здійснюється відповідно до закону.

Стаття 18. Реєстрація документів розпорядника інформації

1. Для забезпечення збереження та доступу до публічної інформації документи, що знаходяться у суб'єктів владних повноважень, підлягають обов'язковій реєстрації в системі обліку, що має містити:

– назву документа;

– дату створення документа;

– дату надходження документа;

– джерело інформації (автор, відповідний підрозділ);

– передбачену законом підставу віднесення інформації до категорії з обмеженим доступом;

– строк обмеження доступу до інформації, у разі якщо вона віднесена до інформації з обмеженим доступом;

– галузь;

– ключові слова;

– тип, носій (текстовий документ, електронний документ, плівки, відеозаписи, аудіозаписи тощо);

– вид (нормативні акти, угоди, рішення, протоколи, звіти, прес-релізи);

– проекти рішень (доповідні записки, звернення, заяви, подання, пропозиції, листи тощо);

– форму та місце зберігання документа тощо.

2. Доступ до системи обліку, що містить інформацію про документ, що знаходиться у суб'єкта владних повноважень, забезпечується шляхом:

– оприлюднення на офіційних веб-сайтах суб'єктів владних повноважень такої інформації, а в разі їх відсутності – в інший прийнятний спосіб;

– надання доступу до системи за запитами.

3. Система обліку публічної інформації не може бути віднесена до категорії інформації з обмеженим доступом.

4. Розпорядники інформації несуть відповідальність за забезпечення доступу до системи обліку відповідно до закону.

Розділ IV. РЕАЛІЗАЦІЯ ПРАВА НА ДОСТУП ДО ІНФОРМАЦІЇ ЗА ІНФОРМАЦІЙНИМ ЗАПИТОМ

Стаття 19. Оформлення запитів на інформацію

1. Запит на інформацію – це прохання особи до розпорядника інформації надати публічну інформацію, що знаходиться у його володінні.

2. Запитувач має право звернутися до розпорядника інформації із запитом на інформацію незалежно від того, стосується ця інформація його особисто чи ні, без пояснення причини подання запиту.

3. Запит на інформацію може бути індивідуальним або колективним. Запити можуть подаватися в усній, письмовій чи іншій формі (поштою, факсом, телефоном, електронною поштою) на вибір запитувача.

4. Письмовий запит подається в довільній формі.

5. Запит на інформацію має містити:

– ім'я (найменування) запитувача, поштову адресу або адресу електронної пошти, а також номер засобу зв'язку, якщо такий є;

– загальний опис інформації або вид, назву, реквізити чи зміст документа, щодо якого зроблено запит, якщо запитувачу це відомо;

– підпис і дату за умови подання запиту в письмовій формі.

6. З метою спрощення процедури оформлення письмових запитів на інформацію особа може подавати запит шляхом заповнення відповідних форм запитів на інформацію, які можна отримати в розпорядника інформації та на офіційному веб-сайті відповідного розпорядника. Зазначені форми мають містити стислу інструкцію щодо процедури подання запиту на інформацію, її отримання тощо.

7. У разі якщо з поважних причин (інвалідність, обмежені фізичні можливості тощо) особа не може подати письмовий запит, його має оформити відповідальна особа з питань доступу до публічної інформації, обов'язково зазначивши в запиті своє ім'я, контактний телефон, та надати копію запиту особі, яка його подала.

Стаття 20. Строк розгляду запитів на інформацію

1. Розпорядник інформації має надати відповідь на запит на інформацію не пізніше п'яти робочих днів з дня отримання запиту.

2. У разі якщо запит на інформацію стосується інформації, необхідної для захисту життя чи свободи особи, щодо стану довкілля, якості харчових продуктів і предметів побуту, аварій, катастроф, небезпечних природних явищ та інших надзвичайних подій, що сталися або можуть статись і загрожують безпеці громадян, відповідь має бути надана не пізніше 48 годин з дня отримання запиту.

3. Клопотання про термінове опрацювання запиту має бути обґрунтованим.

4. У разі якщо запит стосується надання великого обсягу інформації або потребує пошуку інформації серед значної кількості даних, розпорядник інформації може продовжити строк розгляду запиту до 20 робочих днів з обґрунтуванням такого продовження. Про продовження строку розпорядник інформації повідомляє запитувача в письмовій формі не пізніше п'яти робочих днів з дня отримання запиту.

Стаття 21. Плата за надання інформації

1. Інформація на запит надається безкоштовно.

2. У разі якщо задоволення запиту на інформацію передбачає виготовлення копій документів обсягом більш як 10 сторінок, запитувач зобов'язаний відшкодувати фактичні витрати на копіювання та друк.

3. Розмір фактичних витрат визначається відповідним розпорядником на копіювання та друк в межах граничних норм, встановлених Кабінетом Міністрів України. У разі якщо розпорядник інформації не встановив розміру плати за копіювання або друк, інформація надається безкоштовно.

4. При наданні особі інформації про себе та інформації, що становить суспільний інтерес, плата за копіювання та друк не стягується.

Стаття 22. Відмова та відстрочка в задоволенні запиту на інформацію

1. Розпорядник інформації має право відмовити в задоволенні запиту в таких випадках:

1) розпорядник інформації не володіє і не зобов'язаний відповідно до його компетенції, передбаченої законодавством, володіти інформацією, щодо якої зроблено запит;

2) інформація, що запитується, належить до категорії інформації з обмеженим доступом відповідно до частини другої статті 6 цього Закону;

3) особа, яка подала запит на інформацію, не оплатила передбачені статтею 21 цього Закону фактичні витрати, пов'язані з копіюванням або друком;

4) не дотримано вимог до запиту на інформацію, передбачених частиною п'ятою статті 19 цього Закону.

2. Відповідь розпорядника інформації про те, що інформація може бути одержана запитувачем із загальнодоступних джерел, або відповідь не за суттю запиту вважається неправомірною відмовою в наданні інформації.

3. Розпорядник інформації, який не володіє запитуваною інформацією, але якому за статусом або характером діяльності відомо або має бути відомо, хто нею володіє, зобов'язаний направити цей запит належному розпоряднику з одночасним повідомленням про це запитувача. У такому разі відлік строку розгляду запиту на інформацію починається з дня отримання запиту належним розпорядником.

4. У відмові в задоволенні запиту на інформацію має бути зазначено:

– прізвище, ім'я, по батькові та посаду особи, відповідальної за розгляд запиту розпорядником інформації;

– дату відмови;

– мотивовану підставу відмови;

– порядок оскарження відмови;

– підпис.

5. Відмова в задоволенні запиту на інформацію надається в письмовій формі.

6. Відстрочка в задоволенні запиту на інформацію допускається в разі, якщо запитувана інформація не може бути надана для ознайомлення в передбачені цим Законом строки у разі настання обставин непереборної сили. Рішення про відстрочку доводиться до відома запитувача у письмовій формі з роз'ясненням порядку оскарження прийнятого рішення.

7. У рішенні про відстрочку в задоволенні запиту на інформацію має бути зазначено:

– прізвище, ім'я, по батькові та посаду особи, відповідальної за розгляд запиту розпорядником інформації;

– дату надсилання або вручення повідомлення про відстрочку;

– причини, у зв'язку з якими запит на інформацію не може бути задоволений у встановлений цим Законом строк;

– строк, у який буде задоволено запит;

– підпис.

Розділ V. ОСКАРЖЕННЯ РІШЕНЬ, ДІЙ ЧИ БЕЗДІЯЛЬНОСТІ РОЗПОРЯДНИКІВ ІНФОРМАЦІЇ

Стаття 23. Право на оскарження рішень, дій чи бездіяльності розпорядників інформації

1. Рішення, дії чи бездіяльність розпорядників інформації можуть бути оскаржені до керівника розпорядника, вищого органу або суду.

2. Запитувач має право оскаржити:

– відмову в задоволенні запиту на інформацію;

– відстрочку задоволення запиту на інформацію;

– ненадання відповіді на запит на інформацію;

– надання недостовірної або неповної інформації;

– несвоєчасне надання інформації;

– невиконання розпорядниками обов'язку оприлюднювати інформацію відповідно до статті 15 цього Закону;

– інші рішення, дії чи бездіяльність розпорядників інформації, що порушили законні права та інтереси запитувача.

3. Оскарження рішень, дій чи бездіяльності розпорядників інформації до суду здійснюється відповідно до Кодексу адміністративного судочинства України.

Стаття 24. Відповідальність за порушення законодавства про доступ до публічної інформації

1. Відповідальність за порушення законодавства про доступ до публічної інформації несуть особи, винні у вчиненні таких порушень:

– ненадання відповіді на запит;

– ненадання інформації на запит;

– безпідставна відмова у задоволенні запиту на інформацію;

– неоприлюднення інформації відповідно до статті 15 цього Закону;

– надання або оприлюднення недостовірної, неточної або неповної інформації;

– несвоєчасне надання інформації;

– необґрунтоване віднесення інформації до інформації з обмеженим доступом;

– нездійснення реєстрації документів;

– навмисне приховування або знищення інформації чи документів.

2. Особи, на думку яких їхні права та законні інтереси порушені розпорядниками інформації, мають право на відшкодування матеріальної та моральної шкоди в порядку, визначеному законом.

Додаток Б. Розширена нормативно-правова база щодо захисту інформації в Україні та стандарти у галузі захисту інформації

Б.1 Нормативно-правова база щодо захисту інформації в Україні.

Б.2. Статі Кримінального кодексу, які передбачують покарання за розголошення таємниці.

Б.3. Нормативно-правові акти, що регламентують діяльність Держспецзв'язку за сферами.

Б.4. Стандарти у галузі захисту інформації

Б.1. Нормативно-правова база щодо захисту інформації в Україні

Нормативно-правова база складається з:

- Законів України
- Указів Президента України
- Розпоряджень Президента України
- Постанови Кабінету Міністрів України
- Розпоряджень Кабінету Міністрів України
- Державних стандартів
- Концепцій
- Наказів Адміністрації Держспецзв'язку
- Нормативних документів Державної служби спеціального зв'язку та захисту інформації України
- Відповідних статей Кримінального кодексу України.

До основних законів відносяться:

1. Закон України «Про інформацію».
2. Закон України «Про науково-технічну інформацію».
3. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».
4. Закон України «Про доступ до публічної інформації».
5. Закон України «Про захист персональних даних».
6. Закон України «Про державну таємницю».
7. Закон України «Про основні засади забезпечення кібербезпеки України».
8. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України».
9. Закон України «Про критичну інфраструктуру».
10. Закон України «Про Національну систему конфіденційного зв'язку».
11. Закон України «Про радіочастотний ресурс України».
12. Закон України «Про телекомунікації».
13. Закон України «Про електронні комунікації»

14. Закон України «Про електронні документи та електронний документообіг».

15. Закон України «Про електронні довірчі послуги», на зміну Закону України «Про електронний цифровий підпис».

16. Закон України «Про оборону України».

17. Закон України «Про правовий режим воєнного стану».

18. Закон України «Про національну безпеку України».

19. Закон України «Про ліцензування певних видів господарської діяльності»

20. Стратегія кібербезпеки України.

21. Постанова Кабінету Міністрів України від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури.

22. Постанова Кабінету Міністрів України від 23 грудня 2020 року №1295 «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки».

23. Постанова Кабінету Міністрів України від 8 лютого 2021 р. №94 «Про реалізацію експериментального проєкту щодо функціонування Національного центру резервування державних інформаційних ресурсів».

24. Постанова Кабінету Міністрів України від 23 грудня 2020 року №1363 «Про реалізацію експериментального проєкту щодо запровадження комплексу організаційно-технічних заходів з виявлення вразливостей і недоліків у налаштуванні інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, в яких обробляються державні інформаційні ресурси»

25. Розпорядження Кабінету Міністрів України від 2 грудня 2020 №1566-р щодо питання штучного інтелекту.

26. Положення про Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України у новій редакції, затверджене наказом Адміністрації Держспецзв'язку від 26 жовтня 2020 року № 686.

27. Указ Президента України №544/2021 «Про рішення Ради національної безпеки і оборони України від 22 жовтня 2021 року «Про Концепцію реформування Державної служби спеціального зв'язку та захисту інформації України»

28. Указ Президента України №151/2022 від 19 березня 2022 р. «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану»

29. Указ Президента України №151/2022 від 19 березня 2022 р. та «Про нейтралізацію загроз інформаційній безпеці держави».

Захистом інформації в Україні займаються:

Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язок) утворена на виконання ухваленого 23 лютого 2006 року Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» і є спеціалізованим органом центральної виконавчої влади в галузі спеціального зв'язку та захисту інформації, суб'єктом сектору оборони і

безпеки, основним суб'єктом національної системи кібербезпеки, що здійснює координацію діяльності суб’єктів забезпечення кібербезпеки в галузі кіберзахисту, та адміністратором зв'язку. Держспецзв'язок виконує 93 завдання й функції та формує державну політику в 16 сферах (згідно із Законом України «Про Державну службу спеціального зв'язку та захисту України»).

Крім цієї структури захистом інформації, тобто розробкою та впровадженням криптографічних і технічних засобів захисту інформації мають право ті структури, які ліцензовані **Державною Службою спеціального зв’язку та захисту інформації України**. До них відносяться:

– ПрАТ «Інститут інформаційних технологій» (код ЄДРПОУ 22723472).

– ТОВ «САЙФЕР БІС» (код ЄДРПОУ 33349855).

– ТОВ «АВЕСТ-УКРАЇНА» (код ЄДРПОУ 37963188).

– ТОВ «АТМНІС» (код ЄДРПОУ 34964079).

– ТОВ «Ілайф» (код ЄДРПОУ 36049014).

– ТОВ «НОКК СОФТ» (код ЄДРПОУ 38265927).

– ТОВ «Науково-виробничий центр «Безпека інформаційних технологій і систем» (код ЄДРПОУ 31028324).

– ТОВ «ДБО Софт» (код ЄДРПОУ 37619243).

– ТОВ «ІТ ІНЖИНІРІНГ» (код ЄДРПОУ 41215845).

– ТОВ «Техноконсалтинг» (код ЄДРПОУ 25284317).

– ТОВ «Український спеціальний оператор» (код ЄДРПОУ 36002112).

– ТОВ «СИСТЕМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ «КРИПТОСОФТ» (код ЄДРПОУ 37727303).

– ТОВ «ДОЛЯ І КО. ЛТД» (код ЄДРПОУ 01043342).

– ТОВ «УНІВЕРСАЛЬНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ» (код ЄДРПОУ 34891802).

– ТОВ «АЛЬТАЇР-775» (код ЄДРПОУ 25197618).

– ТОВ «Безпека та інновації інформаційних систем» (код ЄДРПОУ 41449076).

– ТОВ «ЗАХИСТ.ЮЕЙ» (код ЄДРПОУ 42292899).

– ТОВ «ДІСІЕНСІ» (код ЄДРПОУ 41564452).

– Мале підприємство «ДИНА» у формі товариства з обмеженою відповідальністю (код ЄДРПОУ 13683319).

– ТОВ «АВТОР» (код ЄДРПОУ 32248356).

– Приватне акціонерне товариство «Науково-дослідний інститут прикладних інформаційних технологій» (код ЄДРПОУ 30674051).

– ТОВ «С.І.Т» (код ЄДРПОУ 3873869).

– ТОВ»АЙ-ДЖИ-ЕМ» (код ЄДРПОУ 38777968).

– ТОВ «НВП «СМАРТ СОЛЮШЕНС» (код ЄДРПОУ 42687163).

– ТОВ «АЛЛІС ЛТД» (код ЄДРПОУ 41065991).

– ТОВ «ОРГПРОМСИСТЕМИ» (код ЄДРПОУ 24376313).

– ТОВ «М.С.Л» (код ЄДРПОУ 30109292).

– ТОВ «Інновейшн девелопмент ХАБ» (код ЄДРПОУ 39665878).

– ТОВ «САЙБЕР ЛАБ» (код ЄДРПОУ 43927493).

– Адміністрація Державної служби спеціального зв'язку та захисту інформації України (код ЄДРПОУ 34620942).

Б.2. Статі Кримінального кодексу, які передбачують покарання за розголошення таємниці

У Кримінальному кодексу є ряд статей, які передбачують покарання за розголошення таємниці. До них відносяться:

Стаття 114. Шпигунство, карається позбавленням волі на строк від восьми до п'ятнадцяти років

Стаття 145. Незаконне розголошення лікарської таємниці, карається штрафом до п'ятдесяти неоподатковуваних мінімумів доходів громадян або громадськими роботами на строк до двохсот сорока годин, або позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років, або виправними роботами на строк до двох років.

Стаття 159. Порушення таємниці голосування, карається штрафом від ста до трьохсот неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або обмеженням волі на строк до трьох років.

Стаття 163. Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер.

Ч.1 караються штрафом від п'ятдесяти до ста неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або обмеженням волі до трьох років.

Ч.2 караються позбавленням волі на строк від трьох до семи років.

Стаття 168. Розголошення таємниці усиновлення (удочеріння) виправними роботами на строк до двох років.

Стаття 189. Вимагання, в частині яка торкається розголошення відомостей, які потерпілий чи його близькі родичі бажають зберегти в таємниці (вимагання), – караються обмеженням волі на строк до п'яти років або позбавленням волі на той самий строк.

Стаття 231. Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю – позбавленням волі на строк до трьох років.

Стаття 232. Розголошення комерційної або банківської таємниці – виправними роботами на строк до двох років, або позбавленням волі на той самий строк.

Стаття 232-1. Розголошення або використання неоприлюдненої інформації про емітента або його цінні папери – карається обмеженням волі на строк до трьох років.

Розділ XIV ЗЛОЧИНИ У СФЕРІ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ, НЕДОТОРКАННОСТІ ДЕРЖАВНИХ КОРДОНІВ, ЗАБЕЗПЕЧЕННЯ ПРИЗОВУ ТА МОБІЛІЗАЦІЇ.

Стаття 328. Розголошення державної таємниці – карається позбавленням волі на строк від п'яти до восьми років.

Стаття 329. Втрата документів, що містять державну таємницю – від двох до п'яти років.

Стаття 330. Передача або збирання відомостей, що становлять конфіденційну інформацію, яка є власністю держави – від чотирьох до восьми років.

Б.3. Нормативно-правові акти, що регламентують діяльність Держспецзв'язку за сферами

Перелік актів законодавства у сфері криптографічного захисту інформації

Закони України

– Закон України «Про Державну службу спеціального зв'язку та захисту інформації України»;

– Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»;

– Закон України «Про електронні довірчі послуги» (набрання чинності з 07.11.2018).

Нормативно-правові акти Президента України

– Указ Президента України від 27.09.1999 № 1229 «Про Положення про технічний захист інформації в Україні»;

– Указ Президента України від 22.05.1998 № 505 «Про Положення про порядок здійснення криптографічного захисту інформації в Україні».

Нормативно-правові акти Кабінету Міністрів України

– Постанова Кабінету Міністрів України від 16.12.2015 № 1057 «Про визначення сфер діяльності, в яких центральні органи виконавчої влади здійснюють функції технічного регулювання»;

– Постанова Кабінету Міністрів України від 03.09.2014 № 411 «Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України»;

– Постанова Кабінету Міністрів України від 29.03.2006 № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах».

Нормативно-правові акти Адміністрації Держспецзв'язку

– Наказ Міністерства юстиції України та Адміністрації Держспецзв'язку від 27.12.2013 № 2782/5/689 «Про затвердження вимог до алгоритмів, форматів та інтерфейсів, що реалізуються у засобах шифрування та надійних засобах електронного цифрового підпису», зареєстрований в Міністерстві юстиції України 27.12.2013 за № 2227/24759;

– Наказ Адміністрації Держспецзв'язку від 18.12.2012 № 739 «Про затвердження Вимог до форматів криптографічних повідомлень», зареєстрований в Міністерстві юстиції України 14.01.2013 за № 108/22640;

– Наказ Міністерства юстиції України та Адміністрації Держспецзв'язку від 20.08.2012 № 1236/5/453 «Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису», зареєстрований в Міністерстві юстиції України 20.08.2012 за №1398/21710;

– Наказ Адміністрації Держспецзв'язку від 29.11.2008 № 200 «Про затвердження Стандарту надання адміністративної послуги з організації державної експертизи у сфері криптографічного захисту інформації»;

– Наказ Адміністрації Держспецзв'язку від 23.06.2008 № 100 «Про затвердження Положення про державну експертизу в сфері криптографічного захисту інформації», зареєстрований в Міністерстві юстиції України 16.07.2008 за № 651/15342;

– Наказ Адміністрації Держспецзв'язку від 12.06.2007 № 114 «Про затвердження Інструкції про порядок постачання і використання ключів до засобів криптографічного захисту інформації», зареєстрований в Міністерстві юстиції України 25.06.2007 за № 729/13996;

– Наказ Адміністрації Держспецзв'язку від 20.07.2007 № 141 «Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації», зареєстрований в Міністерстві юстиції України 30.07.2007 за № 862/14129.

Перелік актів законодавства у сфері технічного захисту інформації

Закони України

– Закон України «Про Державну службу спеціального зв'язку та захисту інформації України»;

– Закон України «Про інформацію»;

– Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»;

– Закон України «Про державну таємницю»;

– Закон України «Про захист персональних даних»;

– Закон України «Про доступ до публічної інформації»;

– Закон України «Про національну безпеку України»;

– Закон України «Про ліцензування видів господарської діяльності»;

– Закон України «Про основні засади державного нагляду (контролю) у сфері господарської діяльності»;

– Закон України «Про акредитацію органів з оцінки відповідності»;

– Закон України «Про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання»;

– Закон України «Про наукову і науково-технічну експертизу»;

– Закон України «Про метрологію та метрологічну діяльність»;

– Закон України «Про основні засади забезпечення кібербезпеки України».

Нормативно-правові акти Президента України

– Указ Президента України від 27.09.1999 № 1229 «Про Положення про технічний захист інформації в Україні».

Нормативно-правові акти Кабінету Міністрів України

– Постанова Кабінету Міністрів України від 27.01.2016 № 96 «Про затвердження Порядку видачі або відмови у видачі рішення про призначення, його переоформлення та видачі його дубліката, розширення та обмеження сфери призначення, тимчасового припинення і поновлення дії рішення про призначення та анулювання такого рішення та визнання такими, що втратили чинність, деяких постанов Кабінету Міністрів України»;

– Постанова Кабінету Міністрів України від 16.12.2015 № 1057 «Про визначення сфер діяльності, в яких центральні органи виконавчої влади здійснюють функції технічного регулювання»;

– Постанова Кабінету Міністрів України від 03.09.2014 № 411 «Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України»;

– Постанова Кабінету Міністрів України від 29.03.2006 № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»;

– Постанова Кабінету Міністрів України від 28.01.2004 № 86 «Про затвердження Порядку здійснення державного контролю за міжнародними передачами товарів подвійного використання»;

– Постанова Кабінету Міністрів України від 20.11.2003 № 1807 «Про затвердження Порядку здійснення державного контролю за міжнародними передачами товарів військового призначення»;

– Постанова Кабінету Міністрів України від 16.11.2002 № 1772 «Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах»;

– Постанова Кабінету Міністрів України від 12.04.2002 № 522 «Про затвердження Порядку підключення до глобальних мереж передачі даних»;

– Постанова Кабінету Міністрів України від 13.03.2002 № 281 «Про деякі питання захисту інформації, охорона якої забезпечується державою»;

– Постанова Кабінету Міністрів України від 08.06.1998 № 838 «Про затвердження Положення про порядок надання суб'єктам господарювання діяльності повноважень на право здійснення експорту, імпорту товарів військового призначення та товарів, які містять відомості, що становлять державну таємницю»;

– Постанова Кабінету Міністрів України від 16.02.1998 № 180 «Про затвердження Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в інформаційно-телекомунікаційних та інформаційних системах»;

– Постанова Кабінету Міністрів України від 04.02.1998 № 121 «Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації засобів інформатизації»;

– Постанова Кабінету Міністрів України від 08.10.1997 № 1126 «Про затвердження Концепції технічного захисту інформації в Україні»;

Нормативно-правові акти Адміністрації Держспецзв'язку

– Наказ Адміністрації Держспецзв'язку від 02.12.2014 № 660 «Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», зареєстрований в Міністерстві юстиції України 28.01.2015 за № 90/26535;

– Наказ Адміністрації Держспецзв'язку від 11.03.2011 № 53 «Про затвердження Порядку надання висновків і погодження експорту та тимчасового вивезення товарів військового призначення і подвійного використання, які належать до криптографічних систем, засобів криптографічного та технічного захисту інформації або містять у своєму складі такі засоби», зареєстрований в Міністерстві юстиції України 01.04.2011 за № 437/19175;

– Наказ Адміністрації Держспецзв'язку від 10.06.2008 № 94 «Про затвердження Порядку координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», зареєстрований в Міністерстві юстиції України 07.07.2008 за № 603/15294;

– Наказ Адміністрації Держспецзв'язку від 16.04.2008 № 64 «Про затвердження Порядку формування Реєстру організаторів державної експертизи у сфері технічного захисту інформації та Реєстру експертів з питань технічного захисту інформації»;

– Наказ Адміністрації Держспецзв'язку від 29.05.2007 № 100 «Про затвердження Інструкції про порядок оформлення та складання Державною службою спеціального зв'язку та захисту інформації України матеріалів про адміністративні правопорушення», зареєстрований в Міністерстві юстиції України 12.06.2007 за № 618/13885;

– Наказ Адміністрації Держспецзв'язку від 16.05.2007 № 93 «Про затвердження Положення про державну експертизу в сфері технічного захисту інформації», зареєстрований в Міністерстві юстиції України 16.07.2007 за № 820/14087;

– Наказ Адміністрації Держспецзв'язку від 16.05.2007 № 87 «Про затвердження Положення про державний контроль за станом технічного захисту інформації», зареєстрований в Міністерстві юстиції України 10.07.2007 за № 785/14052;

– Наказ Адміністрації Держспецзв'язку від 16.05.2007 № 86 «Про затвердження Положення про державний контроль за станом технічного захисту інформації під час діяльності на території України іноземних інспекційних груп», зареєстрований в Міністерстві юстиції України 04.06.2007 за № 577/13844;

– Наказ Адміністрації Держспецзв'язку від 26.03.2007 № 45 «Про затвердження Порядку оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації», зареєстрований в Міністерстві юстиції України 10.04.2007 за № 320/13587;

– Наказ Адміністрації Держспецзв'язку від 22.03.2007 № 36 «Про затвердження Положення про порядок розроблення, прийняття, перегляду та скасування міжвідомчих нормативних документів системи технічного захисту

інформації», зареєстрований в Міністерстві юстиції України 04.04.2007 за № 312/13579;

– Наказ ДСТСЗІ СБ України від 23.02.2002 № 9 «Про затвердження Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб», зареєстрований в Міністерстві юстиції України 13.03.2002 за №245/6533;

Нормативні документи системи технічного захисту інформації

– НД ТЗІ 2.6-002-15 Порядок зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99, затверджений наказом Адміністрації Держспецзв'язку від 27.04.2016 № 293;

– НД ТЗІ 2.6-003-2015 Порядок зіставлення компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99, затверджений наказом Адміністрації Держспецзв'язку від 27.04.2016 № 294;

– НД ТЗІ 2.6-013-2016 Методичні вказівки з виконання зіставлення результатів оцінювання засобів захисту інформації від несанкціонованого доступу на відповідність вимогам ISO/IEC 15408 з вимогами НД ТЗІ 2.5-004-99, затверджений наказом Адміністрації Держспецзв'язку від 27.04.2016 № 295;

– НД ТЗІ 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці, затверджений наказом Адміністрації Держспецзв'язку від 15.04.2013 № 215;

– НД ТЗІ 1.5-002-2012 Класифікатор засобів технічного захисту інформації, затверджений наказом Адміністрації Держспецзв'язку від 29.08.2012 № 472;

– НД ТЗІ 2.7-011-2012 Захист інформації на об'єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв, затверджений наказом Адміністрації Держспецзв'язку від 23.07.2012 № 389;

– НД ТЗІ 2.6-001-2011 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах, затверджений наказом Адміністрації Держспецзв'язку від 25.03.2011 № 65;

– НД ТЗІ 2.7-009-2009 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу, затверджений наказом Адміністрації Держспецзв'язку від 24.07.2009 № 172;

– НД ТЗІ 2.7-010-2009 Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу, затверджений наказом Адміністрації Держспецзв'язку від 24.07.2009 № 172;

– НД ТЗІ 1.4-002-2008 Радіолокатори нелінійні. Класифікація. Рекомендовані методи та засоби випробувань, затверджений наказом Адміністрації Держспецзв'язку від 14.02.2008 № 32;

– НД ТЗІ 3.7-003-2005 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі, затверджений наказом ДСТСЗІ СБ України від 08.11.2005 № 125;

– НД ТЗІ 1.6-002-2003 Правила побудови, викладення, оформлення та позначення нормативних документів системи технічного захисту інформації, затверджений наказом ДСТСЗІ СБУ від 24.04.2003 № 41;

– НД ТЗІ 2.5-010-2003 Вимоги до захисту інформації WEB – сторінки від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБУ від 02.04.2003 № 33;

– НД ТЗІ 2.5-008-2002 Вимоги із захисту службової інформації від несанкціонованого доступу під час обробки в автоматизованих системах класу 2, затверджений наказом ДСТСЗІ СБУ від 13.12.2002 № 84;

– НД ТЗІ 2.3-006-2001 Радіовиявлювачі аналізувальні. Методи та засоби випробувань, затверджений наказом ДСТСЗІ СБУ від 06.11.2001 № 64;

– НД ТЗІ 2.3-005-2001 Радіовиявлювачі панорамні. Методи та засоби випробувань, затверджений наказом ДСТСЗІ СБУ від 11.09.2001 № 54;

– НД ТЗІ 4.7-001-2001 Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби визначення наявності та віддаленості місця контактного підключення засобів технічної розвідки. Рекомендації щодо розроблення методів випробувань, затверджений наказом ДСТСЗІ СБУ від 06.04.2001 № 11;

– НД ТЗІ 2.3-002-2001 Технічний захист мовної інформації в симетричних в симетричних абонентських аналогових телефонних лініях. Засоби пасивного приховування мовної інформації. Нелінійні атенюатори та загороджувальні фільтри. Методика випробувань, затверджений наказом ДСТСЗІ СБУ від 06.04.2001 № 11;

– НД ТЗІ 2.3-003-2001 Технічний захист мовної інформації в симетричних в симетричних абонентських аналогових телефонних лініях. Засоби пасивного приховування мовної інформації. Генератори спеціальних сигналів. Методика випробувань, затверджений наказом ДСТСЗІ СБУ від 06.04.2001 № 11;

– НД ТЗІ 2.3-004-2001 Радіовиявлювачі індикаторні. Методи та засоби випробувань, затверджений наказом ДСТСЗІ СБУ від 09.04.2001 № 12;

– НД ТЗІ 2.3-001-2001 Радіовиявлювачі вимірювальні. Методи та засоби випробувань, затверджений наказом ДСТСЗІ СБУ від 27.02.2001 № 5;

– НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 20.12.2000 № 60;

– НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованих системах, затверджений наказом ДСТСЗІ СБУ від 04.12.2000 № 53;

– НД ТЗІ Р-001-2000 Засоби активного захисту інформації з акустичними та віброакустичними джерелами випромінювання. Класифікація та загальні технічні вимоги, затверджений наказом ДСТСЗІ СБУ від 04.09.2000 № 41;

– НД ТЗІ 1.5-001-2000 Радіовиявлювачі. Класифікація. Загальні технічні вимоги, затверджений наказом ДСТСЗІ СБУ від 13.06.2000 № 29;

– НД ТЗІ 2.7-002-99 Методичні вказівки з використання засобів копіювально-розмножувальної техніки, затверджений наказом ДСТСЗІ СБУ від 26.07.1999 № 34;

– НД ТЗІ 2.5-006-99 Класифікатор засобів копіювально-розмножувальної техніки, затверджений наказом ДСТСЗІ СБУ від 26.07.1999 № 34;

– НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБУ від 28.04.1999 № 22 (Зміна № 1 Наказ від 28.12.2012 № 806);

– НД ТЗІ 2.5-002-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту, затверджений наказом ДСТСЗІ СБУ від 28.05.1999 № 26;

– НД ТЗІ 2.5-003-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту, затверджений наказом ДСТСЗІ СБУ від 28.05.1999 № 26;

– НД ТЗІ 1.1-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення, затверджений наказом ДСТСЗІ СБУ від 28.05.1999 № 26;

– НД ТЗІ 2.7-001-99 Технічний захист інформації в програмно-керованих АТС загального користування. Порядок виконання робіт, затверджений наказом ДСТСЗІ СБУ від 28.05.1999 № 26;

– НД ТЗІ 3.7-002-99 Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова), затверджений наказом ДСТСЗІ СБУ від 28.05.1999 № 26;

– НД ТЗІ 2.5-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту, затверджений наказом ДСТСЗІ СБУ від 28.05.1999 № 26;

– НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБУ від 28.04.1999 № 22;

– НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБУ від 28.04.1999 № 22;

– НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблювальної інформації від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБУ від 28.04.1999 № 22;

– НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі, затверджений наказом ДСТСЗІ СБУ від 28.04.1999 № 22;

– ТР ЕОТ-95 Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від

витнку каналами побічних електромагнітних випромінювань і наводок, затверджені наказом ДСТСЗІ від 09.06.1995 № 25;

– ТР ТЗІ ПЕМВН-95 Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок, затверджені наказом ДСТСЗІ від 09.06.1995 № 25.

Перелік актів законодавства у сфері державного контролю за станом криптографічного та технічного захисту інформації

Закони України

– Закон України «Про Державну службу спеціального зв'язку та захисту інформації України»;

– Закон України «Про основні засади державного нагляду (контролю) у сфері господарської діяльності»;

– Закон України «Про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання»;

– Закон України «Про державну таємницю»;

– Закон України «Про ліцензування видів господарської діяльності»;

– Закон України «Про електронні комунікації».

Укази Президента України

– Указ Президента України від 30.03.2015 № 184/2015 «Про рішення Ради національної безпеки і оборони України від 12 березня 2015 року «Про стан подолання негативних наслідків, спричинених втратою матеріальних носіїв секретної інформації на тимчасово окупованій території України, в районі проведення антитерористичної операції в Донецькій та Луганській областях»;

– Указ Президента України від 22.05.1998 № 505/98 «Про Положення про порядок здійснення криптографічного захисту інформації в Україні».

Нормативно-правові акти Кабінету Міністрів України

– Постанова Кабінету Міністрів України від 19.10.2016 № 736 «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію»;

– Постанова Кабінету Міністрів України від 03.09.2014 № 411 «Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України»;

– Постанова Кабінету Міністрів України від 10.05.2018 № 342 «Про затвердження методик розроблення критеріїв за якими оцінюється ступінь ризику від провадження господарської діяльності та визначається періодичність проведення планових заходів державного нагляду (контролю), а також уніфікованих форм актів, що складаються за результатами проведення планових (позапланових) заходів державного нагляду (контролю)»;

– Постанова Кабінету Міністрів України від 31.10.2018 № 915 «Про затвердження критеріїв, за якими оцінюється ступінь ризику від провадження господарської діяльності, що підлягає ліцензуванню, у сфері надання послуг у галузі криптографічного захисту інформації (крім електронних довірчих послуг) та технічного захисту інформації за переліком, що визначається Кабінетом

Міністрів України, і встановлюється періодичність проведення планових заходів державного нагляду (контролю) Адміністрацією Державної служби спеціального зв'язку та захисту інформації»;

– Постанова Кабінету Міністрів України від 16.11.2018 № 821 «Деякі питання ліцензування господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України»;

– Постанова Кабінету Міністрів України від 07.11.2018 № 992 «Про затвердження вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг»;

– Постанова Кабінету Міністрів України від 19.09.2018 № 749 «Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності»;

– Постанова Кабінету Міністрів України від 21 жовтня 2020 р. № 991 «Про затвердження Технічного регламенту засобів криптографічного захисту інформації».

Нормативно-правові акти Адміністрації Держспецзв'язку

– Наказ Адміністрації Держспецзв'язку від 05.10.2017 № 547 «Про затвердження уніфікованої форми акта, складеного за результатами проведення планового (позапланового) заходу державного нагляду (контролю) щодо додержання ліцензіатом вимог ліцензійних умов у сфері провадження господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України» зареєстрований в Міністерстві юстиції України 30.10.2017 за № 1323/31191;

– Наказ Адміністрації Держспецзв'язку від 16.05.2007 № 87 «Про затвердження Положення про державний контроль за станом технічного захисту інформації», зареєстрований в Міністерстві юстиції України 10.07.2007 за № 785/14052;

– Наказ Адміністрації Держспецзв'язку від 16.05.2007 № 86 «Про затвердження Положення про державний контроль за станом технічного захисту інформації під час діяльності на території України іноземних інспекційних груп», зареєстрований в Міністерстві юстиції України 04.06.2007 за № 577/13844;

– Наказ Адміністрації Держспецзв'язку від 27.10.2020 № 687 «Про затвердження переліку стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації»;

– спільний Наказ Міністерства цифрової трансформації України та Адміністрації Держспецзв'язку 30.09.2020 № 140/614 «Про встановлення вимог до технічних засобів, процесів їх створення, використання та функціонування у складі інформаційно-телекомунікаційних систем під час надання кваліфікованих електронних довірчих послуг», зареєстрований в Міністерстві юстиції України 22 жовтня 2020 р. за № 1039/35322.

Перелік законодавчих та нормативно-правових актів, що визначають провадження ліцензованої діяльності у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації, за переліком, що визначається Кабінетом Міністрів України

– Закон України «Про Державну службу спеціального зв'язку та захисту інформації України».

– Закон України «Про ліцензування видів господарської діяльності».

– Закон України «Про основні засади державного нагляду (контролю) у сфері господарської діяльності».

– Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».

– Закон України «Про інформацію».

– Закон України «Про доступ до публічної інформації».

– Закон України «Про електронні документи та електронний документообіг».

– Закон України «Про електронні довірчі послуги».

– Постанова Кабінету Міністрів України від 05.08.2015 № 609 «Про затвердження переліку органів ліцензування та визнання такими, що втратили чинність, деяких постанов Кабінету Міністрів України».

– Постанова Кабінету Міністрів України від 16.11.2016 № 821 «Деякі питання ліцензування господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації, за переліком, що визначається Кабінетом Міністрів України».

Б.4. Стандарти у галузі захисту інформації

Роль стандартів і специфікацій. Найбільш важливі стандарти й специфікації в області інформаційної безпеки

Фахівцям в області *інформаційної безпеки* (ІБ) сьогодні майже неможливо обійтися без знань відповідних *стандартів* і *специфікацій*. На те є кілька причин.

Формальна полягає в тому, що необхідність проходження деяким *стандартам* закріплена законодавчо. Однак найбільш переконливі змістовні причини. По-перше, *стандарти* й *специфікації* – одна з форм нагромадження знань, насамперед про процедурний і програмно-технічний рівні ІБ. У них зафіксовані апробовані, високоякісні рішення й методології, розроблені найбільш кваліфікованими фахівцями. По-друге, і ті, і інші є основним засобом забезпечення взаємної сумісності апаратно-програмних систем і їхніх компонентів, причому в Internet-співтоваристві цей засіб дійсно працює, і досить ефективно.

Стандарт – документ, у якому з метою добровільного багаторазового використання встановлюються характеристики продукції, правила здійснення й

характеристики процесів виробництва, експлуатації, зберігання, перевезення, реалізації й утилізації, виконання робіт або надання послуг. *Стандарт* також може містити вимоги до термінології, символіці, упакуванню, маркуванню або етикеткам і правилам їхнього нанесення;

Стандартизація – діяльність по встановленню правил і характеристик з метою їх добровільного багаторазового використання, спрямована на досягнення впорядкованості в сферах виробництва й обігу продукції й підвищення конкурентоспроможності продукції, робіт або послуг.

Примітно також, що в число принципів *стандартизації*, входить принцип застосування міжнародного *стандарту* як основи розробки національного, за винятком випадків, якщо «таке застосування визнане неможливим внаслідок невідповідності вимог міжнародних *стандартів* кліматичним і географічним особливостям, технічним і (або) технологічним особливостям або по інших підставах, або Україна, відповідно до встановлених процедур, виступала проти прийняття міжнародного *стандарту* або окремого його положення». Із практичної точки зору, кількість *стандартів* і *специфікацій* (міжнародних, національних, галузевих і т.п.) в області *інформаційної безпеки* нескінченно.

На верхньому рівні можна виділити дві, що істотно відрізняються друг від друга, групи *стандартів* і специфікацій:

– **оціночні *стандарти***, призначені для оцінки й класифікації *інформаційних систем* і засобів захисту по вимогах безпеки;

– ***специфікації*, що** регламентують різні аспекти реалізації й використання засобів і методів захисту.

Ці групи, зрозуміло, не конфліктують, а доповнюють одна одну. **Оціночні *стандарти*** описують найважливіші, з погляду *інформаційної безпеки*, поняття й аспекти ІС, відіграючи роль організаційних і архітектурних *специфікацій*. Інші *специфікації* визначають, як саме будувати ІС запропонованої архітектури й виконувати організаційні вимоги.

Із числа **оціночних необхідно виділити** *стандарт* Міністерства оборони США «Критерії оцінки довірених комп'ютерних систем» і його інтерпретацію для мережних конфігурацій, «Гармонізовані критерії Європейських країн», міжнародний *стандарт* «Критерії оцінки безпеки інформаційних технологій», Вимоги Державної служби спеціального зв'язку та захисту інформації України. До цієї ж групи відноситься й Федеральний *стандарт* США «Вимоги безпеки для криптографічних модулів», що регламентує конкретний, але дуже важливий і складний аспект *інформаційної безпеки*.

Технічні *специфікації*, застосовні до сучасним розподілених ІС, створюються, головним чином, ***«Тематичною групою за технологією Internet» (Internet Engineering Task Force, IETF)*** і її підрозділом – робочою групою по безпеці. Ядром розглянутих технічних специфікацій ***служать документи по безпеці на IP-рівні (IPsec).*** Крім цього, аналізується *захист на* транспортному рівні ***(Transport Layer Security, TLS),*** а також ***на рівні додатків (специфікації GSS-API, Kerberos).*** Необхідно відзначити, що Internet-співтовариство приділяє належну увагу адміністративному й процедурному рівням безпеки («Посібник з

інформаційної безпеки підприємства», «Як вибирати постачальника Інтернет-Послуг», «Як реагувати на порушення інформаційної безпеки»).

У питаннях **мережної безпеки** неможливо розібратися без освоєння *специфікацій* **X.800** «Архітектура безпеки для взаємодії відкритих систем», **X.500** «Служба директорій: огляд концепцій, моделей і сервісів» і **X.509** «Служба директорій: каркаси сертифікатів відкритих ключів і атрибутів».

Британський стандарт **BS 7799** «Керування інформаційною безпекою. Практичні правила», корисний для керівників організацій і осіб, відповідальних за *інформаційну безпеку*, без скільки-небудь істотних змін відтворений у міжнародному стандарті **ISO/IEC 17799**.

Такий, на наш погляд, «стандартний мінімум», яким повинні активно володіти всі діючі фахівці в області *інформаційної безпеки*.

До стандартів які діють в Україні відносяться наступні:

Перелік стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації:

I. Стандарти, що визначають вимоги до блокових шифрів (block ciphers)

1. ДСТУ 7624:2014 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення». (Калина)
2. ДСТУ ISO/IEC 18033-3:2015 (ISO/IEC 18033-3:2010, IDT) «Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 3. Блокові шифри».
3. ДСТУ ГОСТ 28147:2009 «Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования».
4. ДСТУ ISO/IEC 10116:2019 (ISO/IEC 10116:2017, IDT) «Інформаційні технології. Методи захисту. Режими роботи n-бітних блокових шифрів».

II. Стандарти, що визначають вимоги до потокових шифрів (stream ciphers)

1. ДСТУ 8845:2019 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного потокового перетворення».
2. ДСТУ ISO/IEC 18033-4:2015 (ISO/IEC 18033-4:2011, IDT) «Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 4. Потокові шифри».

III. Стандарти, що визначають вимоги до асиметричних криптографічних алгоритмів та методів (asymmetric algorithms and techniques)

1. ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння».
2. ДСТУ ISO/IEC 9796-2:2015 (ISO/IEC 9796-2:2010, IDT) «Інформаційні технології. Методи захисту. Схеми цифрового підпису, які забезпечують

відновлення повідомлення. Частина 2. Механізми, що ґрунтуються на факторизації цілих чисел».

3. ДСТУ ISO/IEC 9796-3:2015 (ISO/IEC9796-3:2006, IDT) «Інформаційні технології. Методи захисту. Схеми цифрового підпису, які забезпечують відновлення повідомлення. Частина 3. Механізми, що ґрунтуються на дискретному логарифмі».

4. ДСТУ ISO/IEC 14888-2:2015 (ISO/IEC 14888-2:2008, IDT) «Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 2. Механізми, що ґрунтуються на факторизації цілих чисел».

5. ДСТУ ISO/IEC 14888-3:2019 (ISO/IEC 14888-3:2018, IDT) «Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 3. Механізми, що ґрунтуються на дискретному логарифмуванні».

6. ДСТУ ISO/IEC 15946-5:2019 (ISO/IEC 15946-5:2017) «Інформаційні технології. Методи захисту. Криптографічні методи на основі еліптичних кривих. Частина 5. Генерування еліптичних кривих».

7. ДСТУ ISO/IEC 18033-2:2015 (ISO/IEC 18033-2:2006, IDT) «Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 2. Асиметричні шифри».

IV. Стандарт, що визначає вимоги до кодів автентифікації повідомлень (message authentication codes)

ДСТУ ISO/IEC 9797-2:2015 (ISO/IEC 9797-2:2011, IDT) «Інформаційні технології. Методи захисту. Коди автентифікації повідомлень (MACs). Частина 2. Механізми що використовують спеціалізовану ґеш-функцію».

V. Стандарти, що визначають вимоги до ґеш-функцій (hash functions)

1. ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція ґешування». (Купина)

2. ДСТУ ISO/IEC 10118-2:2015 (ISO/IEC 10118-2:2010; Cor 1:2011, IDT) «Інформаційні технології. Методи захисту. Ґеш-функції. Частина 2. Ґеш-функції, що використовують n-бітний блоковий шифр».

3. ДСТУ ISO/IEC 10118-3:2005 (ISO/IEC 10118-3:2004; Cor 1:2011, IDT) «Інформаційні технології. Методи захисту. Ґеш-функції. Частина 3. Спеціалізовані ґеш-функції».

4. ДСТУ ISO/IEC 10118-4:2015 (ISO/IEC 10118-4:1998; Cor 1:2014; Amd 1:2014, IDT) «Інформаційні технології. Методи захисту. Ґеш-функції. Частина 4. Ґеш-функції, що використовують модульну арифметику».

5. ГОСТ 34.311-95 «Информационная технология. Криптографическая защита информации. Функция хэширования».

VI. Стандарти, що визначають вимоги до автентифікації сутності (entity authentication)

1. ДСТУ ISO/IEC 9798-2:2015 (ISO/IEC 9798-2:2008; Cor 3:2013, IDT) «Інформаційні технології. Методи захисту. Автентифікація об’єктів. Частина 2. Механізми, що використовують симетричні алгоритми шифрування».

2. ДСТУ ISO/IEC 9798-3:2002 (ISO/IEC 9798-3:1998; Cor 1:2009; Cor 2:2012) «Інформаційні технології. Методи захисту. Автентифікація суб’єктів. Частина 3. Механізми з використанням методу цифрового підпису».

3. ДСТУ ISO/IEC 9798-4:2015 (ISO/IEC 9798-4:1999; Cor 1:2009; Cor 2:2012, IDT) «Інформаційні технології. Методи захисту. Автентифікація об’єктів. Частина 4. Методи, що використовують криптографічну перевірочну функцію».

4. ДСТУ ISO/IEC 9798-5:2015 (ISO/IEC 9798-5:2009, IDT) «Інформаційні технології. Методи захисту. Автентифікація об’єктів. Частина 5. Механізми, що використовують методи нульової обізнаності».

5. ДСТУ ISO/IEC 9798-6:2015 (ISO/IEC 9798-6:2010, IDT) «Інформаційні технології. Методи захисту. Автентифікація об’єктів. Частина 6. Механізми, що використовують ручне передавання даних».

VII. Стандарти, що визначають вимоги до управління ключами (key management)

1. ДСТУ ISO/IEC 11770-2:2015 (ISO/IEC 11770-2:2008; Cor 1:2009, IDT) «Інформаційні технології. Методи захисту. Керування ключами. Частина 2. Механізми з використанням симетричних методів».

2. ДСТУ ISO/IEC 11770-3:2015 (ISO/IEC 11770-3:2008; Cor 1:2009, IDT) «Інформаційні технології. Методи захисту. Керування ключами. Частина 3. Механізми з використанням асиметричних методів».

3. ДСТУ ISO/IEC 11770-4:2015 (ISO/IEC 11770-4:2008; Cor 1:2009, IDT) «Інформаційні технології. Методи захисту. Керування ключами. Частина 4. Механізми, засновані на нестійких секретах».

4. ДСТУ ISO/IEC 11770-5:2015 (ISO/IEC 11770-5:2008, IDT) «Інформаційні технології. Методи захисту. Керування ключами. Частина 5. Керування груповими ключами».

VIII. Стандарти, що визначають вимоги до випадкової генерації біт (random bit generation)

1. ДСТУ ISO/IEC 18031:2015 (ISO/IEC 18031:2011; Cor 1:2014, IDT) «Інформаційні технології. Методи захисту. Генерування випадкових бітів».

2. ДСТУ ISO/IEC 20543 «Інформаційні технології. Методи захисту. Методи тестування та аналізу для генерування випадкових бітів».

IX. Стандарти, що визначають вимоги до методів встановлення чутливих параметрів безпеки (sensitive security parameter establishment methods)

1. ДСТУ ISO/IEC 11770-2:2015 (ISO/IEC 11770-2:2008; Cor 1:2009, IDT) «Інформаційні технології. Методи захисту. Керування ключами. Частина 2. Механізми з використанням симетричних методів».

2. ДСТУ ISO/IEC 11770-3:2015 (ISO/IEC 11770-3:2008; Cor 1:2009, IDT) «Інформаційні технології. Методи захисту. Керування ключами. Частина 3. Механізми з використанням асиметричних методів».

X. Стандарти, що визначають вимоги до тестових метрик пом'якшення неінвазійних атак (non-invasive attack mitigation test metrics)

1. ДСТУ ISO/IEC 20085-1 «Методи захисту ІТ. Вимоги до засобів тестування та методів калібрування засобів тестування для застосування у методах тестування пом'якшення неінвазійних атак на криптографічні модулі. Частина 1. Методи та засоби тестування».

2. ДСТУ ISO/IEC 20085-2 «Методи захисту ІТ. Вимоги до засобів тестування та методів калібрування засобів тестування для застосування у методах тестування пом'якшення неінвазійних атак на криптографічні модулі. Частина 2. Методи та прилади тестового калібрування».

XI. Стандарти та технічні специфікації, що визначають вимоги до форматів криптографічних повідомлень

RFC 5652 «Cryptographic Message Syntax (CMS)» з використання криптографічних алгоритмів згідно з RFC 3370 «Cryptographic Message Syntax (CMS) Algorithms» або Технічних специфікацій до RFC 5652, затверджених наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України

<u>У рамках технічного захисту</u>:

1. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.
2. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.
3. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.
4. ДБН А.2.2-2-96 ДЕРЖАВНІ БУДІВЕЛЬНІ НОРМИ УКРАЇНИ Проектування. Технічний захист інформації. Загальні вимоги до організації проектування і проектної документації для будівництва.
5. Положення про технічний захист інформації в Україні, затвердженого Указом Президента України від 27 вересня 1999 р. № 1229.
6. Правила проведення робіт із сертифікації засобів захисту інформації, затвердженими спільним наказом Адміністрації Держспецзв'язку та Держспоживстандарту України від 25.04.2007 р. № 75/91 і зареєстрованими в Міністерстві юстиції України 14.05.2007 р. за № 498/13765.

7. Положення про державну експертизу в сфері технічного захисту інформації, затвердженим наказом Адміністрації Держспецзв'язку України від 16.05.2007 р. № 93 і зареєстрованим в Міністерстві юстиції України 16.07.2007 р. за № 820/14087.

8. Нормативний документ технічного захисту інформації (НД ТЗІ) НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу, Наказ ДСТСЗІ СБУ від 28.04.99 (Зміна № 1 Наказ Адміністрації Держспецзв'язку від 28.12.2012 № 806)

9. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу, Наказ ДСТСЗІ СБУ від 28.04.99 № 22

10. НД ТЗІ 1.1-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення, Наказ ДСТСЗІ СБУ від 28.05.99 №26

11. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованих системах, Наказ ДСТСЗІ СБУ від 04.12.2000 № 53 (Зміна № 1 Наказ Адміністрації Держспецзв'язку від 28.12.2012 № 806)

12. НД ТЗІ 1.4-002-2008 Радіолокатори нелінійні. Класифікація. Рекомендовані методи та засоби випробувань, Наказ Адміністрації Держспецзв'язку від 14.02.2008 №32

13. НД ТЗІ 1.5-001-2000 Радіовиявлювачі. Класифікація. Загальні технічні вимоги, Наказ ДСТСЗІ СБУ від 13.06.2000 № 29 (Зміна № 1 Наказ ДСТСЗІ СБУ від 27.02.2001 №5)

14. НД ТЗІ 1.5-002-2012 Класифікатор засобів технічного захисту інформації, Наказ Адміністрації Держспецзв'язку від 29.08.2012 № 472

15. НД ТЗІ 1.6-002-2003 Правила побудови, викладення, оформлення та позначення нормативних документів системи технічного захисту інформації, Наказ ДСТСЗІ СБУ від 24.04.2003 № 41 (Зміна № 1, Наказ Адміністрації Держспецзв'язку від 03.11.2011 № 93 дск., зміна № 2, Наказ Адміністрації Держспецзв'язку від 17.08.2013 № 451)

16. НД ТЗІ 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці, Наказ Адміністрації Держспецзв'язку від 15.04.2013 № 215

17. НД ТЗІ 2.3-001-2001 Радіовиявлювачі вимірювальні. Методи та засоби випробувань, Наказ ДСТСЗІ СБУ від 27.02.2001 № 5

18. НД ТЗІ 2.3-002-2001 Технічний захист мовної інформації в симетричних в симетричних абонентських аналогових телефонних лініях. Засоби пасивного приховування мовної інформації. Нелінійні атенюатори та загороджувальні фільтри. Методика випробувань, Наказ ДСТСЗІ СБУ від 06.04.2001 № 11

19. НД ТЗІ 2.3-003-2001 Технічний захист мовної інформації в симетричних в симетричних абонентських аналогових телефонних лініях. Засоби пасивного приховування мовної інформації. Генератори спеціальних сигналів. Методика випробувань, Наказ ДСТСЗІ СБУ від 06.04.2001 № 11

20. НД ТЗІ 2.3-004-2001 Радіовиявлювачі індикаторні. Методи та засоби випробувань, Наказ ДСТСЗІ СБУ від 09.04.2001 № 12

21. НД ТЗІ 2.3-005-2001 Радіовиявлювачі панорамні. Методи та засоби випробувань, Наказ ДСТСЗІ СБУ від 11.09.2001 № 54

22. НД ТЗІ 2.3-006-2001 Радіовиявлювачі аналізу вальні. Методи та засоби випробувань, Наказ ДСТСЗІ СБУ від 06.11.2001 № 64

23. Р-001-2000 Засоби активного захисту мовної інформації з акустичними та віброакустичними джерелами випромінювання. Класифікація та загальні технічні вимоги. Рекомендації, Наказ ДСТСЗІ СБУ від 04.09.2000 № 41

24. ТР ЕОТ -95 Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок, Наказ Державної служби України з питань ТЗІ від 09.06.95 № 25 (Зміна № 1, Наказ Адміністрації Держспецзв'язку від 03.11.2011 № 93 дск)

25. ТР ТЗІ – ПЕМВН-95 Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок, Наказ ДСТЗІ від 09.06.95 № 25, Наказ Державної служби України з питань ТЗІ від 09.06.95 № 25

26. (Зміна № 1, Наказ Адміністрації Держспецзв'язку від 03.11.2011 № 93 дск)

27. НД ТЗІ 2.5-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту, Наказ ДСТСЗІ СБУ від 28.05.99 № 26

28. НД ТЗІ 2.5-002-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту, Наказ ДСТСЗІ СБУ від 28.05.99 № 26

29. НД ТЗІ 2.5-003-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту, Наказ ДСТСЗІ СБУ від 28.05.99 № 26

30. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, Наказ ДСТСЗІ СБУ від 28.04.99 № 22 (Зміна № 1 Наказ від 28.12.2012 № 806)

31. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблювальної інформації від несанкціонованого доступу, Наказ ДСТСЗІ СБУ від 28.04.99 № 22 (Зміна № 1 Наказ від 15.10.2008 № 172)

32. НД ТЗІ 2.5-006-99 Класифікатор засобів копіювально-розмножувальної техніки, Наказ ДСТСЗІ СБУ від 26.07.99 № 34

33. НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час обробки в автоматизованих системах класу 2, Наказ ДСТСЗІ СБУ від 13.12.2002 № 84 (Зміна № 1 Наказ Адміністрації Держспецзв'язку від 28.12.2012 № 806)

34. НД ТЗІ 2.5-010-2003 Вимоги до захисту інформації WEB – сторінки від несанкціонованого доступу, Наказ ДСТСЗІ СБУ від 02.04.2003 № 33 (Зміна № 1 Наказ від 28.12.2012 № 806)

35. НД ТЗІ 2.6-001-2011 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах, Наказ Адміністрації Держспецзв'язку від 25.03.2011 № 65

36. НД ТЗІ 2.7-001-99 Технічний захист інформації в програмно-керованих АТС загального користування. Порядок виконання робіт, Наказ ДСТСЗІ СБУ від 28.05.99 №26 (Зміна № 1 Наказ від 28.12.2012 № 806)

37. НД ТЗІ 2.7-002-99 Методичні вказівки з використання засобів копіювально-розмножувальної техніки, Наказ ДСТСЗІ СБУ від 26.07.99 № 34

38. НД ТЗІ 2.7-009-2009 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу, Наказ Адміністрації Держспецзв'язку від 24.07.2009 № 172 (Зміна № 1 Наказ від 28.12.2012 № 806)

39. НД ТЗІ 2.7-010-2009 Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу, Наказ Адміністрації Держспецзв'язку від 24.07.2009 № 172

40. НД ТЗІ 2.7-011-2012 Захист інформації на об'єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв, Наказ Адміністрації Держспецзв'язку від 23.07.2012 №389

41. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу, Наказ ДСТСЗІ СБ України від 20.12.2000 № 60

42. (Зміна № 1 Наказ Адміністрації Держспецзв'язку від 28.12.2012 № 806)

43. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі, Наказ ДСТСЗІ СБУ від 28.04.99 № 22 (Зміна № 1 Наказ ДСТСЗІ СБУ від 18.06.2002 № 37, зміна № 2 Наказ Адміністрації Держспецзв'язку від 28.12.2012 № 806)

44. НД ТЗІ 3.7-002-99 Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова), Наказ ДСТСЗІ СБУ від 28.05.99 № 26

45. НД ТЗІ 3.7-003-2005 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі, Наказ ДСТСЗІ СБ України від 08.11.2005 № 125 (Зміна № 1 Наказ Адміністрації Держспецзв'язку від 28.12.2012 № 806)

46. НД ТЗІ 4.7-001-2001 Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби визначення наявності та віддаленості місця контактного підключення засобів технічної розвідки. Рекомендації щодо розроблення методів випробувань, Наказ ДСТСЗІ СБУ від 06.04.2001 № 11

<u>У рамках сертифікації і ліцензування:</u>

1. ДСТУ 1.0-93 Державна система стандартизації України. Основні положення.
2. ДСТУ 1.3-93 Державна система стандартизації України. Порядок розроблення і побудови, викладення та оформлення технічних умов.
3. ДСТУ 1.4-93 Державна система стандартизації України. Стандарти підприємства. Основні положення.
4. ДСТУ 1.5-93 Державна система стандартизації України. Загальні вимоги до побудови. викладу, оформлення та змісту стандартів.
5. ДСТУ 1.6-97 Державна система стандартизації України. Порядок державної реєстрації галузевих стандартів, стандартів науково-технічних та інженерних товариств і спілок.
6. ДСТУ 2296-93 Національний знак відповідності. Форма, розміри, технічні вимоги та правила застосування.
7. ДСТУ 2462-94 Сертифікація. Основні поняття. Терміни та визначення.
8. ДСТУ 3410-96 Система сертифікації УкрСЕПРО. Основні положення.
9. ДСТУ 3412-96 Система сертифікації УкрСЕПРО. Вимоги до випробувальних лабораторій та порядок їх акредитації.
10. ДСТУ 3413-96 Система сертифікації УкрСЕПРО. Порядок проведення сертифікації продукції.
11. ДСТУ 3417-96 Система сертифікації УкрСЕПРО. Процедура визнання результатів сертифікації продукції, що імпортується.
12. ДСТУ 3419-96 Система сертифікації УкрСЕПРО. Сертифікація систем якості. Порядок проведення.

Огляд закордонних стандартів

Першим оціночним *стандартом*, що одержав міжнародне визнання й зробило винятково сильний вплив на наступні розробки в області *інформаційної безпеки*, став ***стандарт*** **Міністерства оборони США «Критерії оцінки довірених комп'ютерних систем»** (Department of Defense Trusted Computer System Evaliation Criteria, TCSEC), більше відомий (по кольорі обкладинки) за назвою **«Помаранчева книга»**.

Без перебільшення можна затверджувати, що в «Помаранчевій книзі» закладений понятійний базис ІБ. Досить лише перелічити поняття, що втримуються *в* ньому*: безпечна* й *довірена системи*, *політика безпеки*, *рівень гарантованості, підзвітність, довірена обчислювальна база*, *монітор обігів*, *ядро й периметр безпеки*. Винятково важливо й виділення таких аспектів *політики безпеки*, як добровільне (*дискреційне*) і *примусове (мандатне) керування доступом, безпека повторного використання об'єктів*. Останнім один по одному, але аж ніяк не за значенням варто назвати принципи *класифікації по вимогах безпеки* на основі паралельної жорсткості вимог до *політики безпеки* й *рівня гарантованості*.

Після «Помаранчевої книги» була випущена ціла **«Веселкова серія»**. З концептуальної точки зору, найбільш значимий документ у

ній – **«Інтерпретація «Помаранчевої книги» для мережних конфігурацій»** (Trusted Network Interpretation). Він складається із двох частин. Перша містить властиво інтерпретацію, у другий описуються *сервіси безпеки*, специфічні або особливо важливі для мережних конфігурацій.

Найважливіше поняття, уведене в першій частині, – мережна *довірена обчислювальна база*. Інший принциповий аспект – облік динамічності мережних конфігурацій. Серед захисних механізмів виділена *криптографія*, що допомагає підтримувати як *конфіденційність*, так і *цілісність*.

Новим для свого часу став систематичний підхід до питань *доступності*, формування архітектурних принципів її забезпечення.

Згадаємо також достатню умову коректності *фрагментуваня монітора обігів*, що є теоретичною основою декомпозиції розподіленої ІС в об'єктно-орієнтованому стилі в сполученні із криптографічним захистом комунікацій.

Переходячи до знайомства з **«Гармонізованими критеріями Європейських країн»**, відзначимо відсутність у них апріорних вимог до умов, у яких повинна працювати *інформаційна система*. Передбачається, що спочатку формулюється *мета оцінки*, потім орган сертифікації визначає, наскільки повно вона досягається, тобто якою мірою коректні й ефективна архітектура й реалізація *механізмів безпеки* в конкретній ситуації. Щоб полегшити формулювання мети оцінки, *стандарт* містить опис десяти зразкових класів функціональності, типових для урядових і комерційних систем.

В «Гармонізованих критеріях» підкреслюється розходження між системами й продуктами інформаційних технологій, але для уніфікації вимог вводиться єдине поняття – *об'єкт оцінки*.

Важлива вказівка й на розходження між *функціями (сервісами) безпеки* і їхніх механізмів, що реалізують, а також виділення двох аспектів гарантованості – ефективності *й* коректності засобів безпеки.

Серед технічних *специфікацій* на перше місце, безумовно, варто поставити документ **X.800** «Архітектура безпеки для взаємодії відкритих систем». Тут виділені найважливіші *мережні сервіси безпеки*: *автентифікація, керування доступом*, забезпечення *конфіденційності* й/або *цілісності* даних, а також *неможливість відмовитися* від зроблених дій. Для реалізації сервісів передбачені наступні мережні *механізми безпеки* і їхньої комбінації: *шифрування*, *електронний цифровий підпис (ЕЦП)*, *керування доступом*, контроль *цілісності даних*, *автентифікація*, *доповнення трафика*, *керування маршрутизацією*, *нотаризація*. Обрано рівні еталонної семирівневої моделі, на яких можуть бути реалізовані *сервіси* й *механізми безпеки*. Нарешті, детально розглянуті питання адміністрування засобів безпеки для розподілених конфігурацій.

Специфікація Internet-співтовариства **RFC 1510** «Мережний сервіс автентифікації Kerberos (V5)» відноситься до більше приватної, але досить важливої і актуальної проблеми – *автентифікації в різнорідному розподіленому середовищі з підтримкою* ***концепції єдиного входу в мережу***. *Сервер автентифікації Kerberos* являє собою довірену третю сторону, що володіє секретними ключами суб'єктів, що обслуговуються, і яка допомагає їм у

попарній перевірці дійсності. Про вагомість даної *специфікації* свідчить той факт, що клієнтські компоненти Kerberos присутні в більшості сучасних операційних систем.

«Гармонізовані критерії Європейських країн» стали досить передовим документом для свого часу, вони підготували появу міжнародного *стандарту* **ISO/IEC 15408:2017** «Критерії оцінки безпеки інформаційних технологій» (Evaluation criteria for IT security), у україномовній літературі звичайно (але не зовсім вірно) іменованого *«Загальними критеріями»* (ЗК).

На сьогоднішній день ***«Загальні критерії»*** – самий повний і сучасний оцінний *стандарт*. Насправді, це метастандарт, що визначає інструменти оцінки безпеки ІС і порядок їхнього використання; він не містить визначених класів безпеки. Такі класи можна будувати, опираючись на задані вимоги.

ЗК містять два основних види вимог безпеки:

– *функціональні*, відповідні активному аспекту захисту, запропоновані до *функцій (сервісам) безпеки* і їхніх механізмів, що реалізують;

– *вимоги довіри*, що відповідають пасивному аспекту; вони пред'являються до технології й процесу розробки й експлуатації.

Вимоги безпеки формулюються, і їхнє виконання перевіряється для певного *об'єкта оцінки* – апаратно-програмного продукту або *інформаційної системи*.

Підкреслимо, що безпека в ЗК розглядається не статично, а відповідно до життєвого циклу *об'єкта оцінки*. Крім того, останній з'являється в контексті середовища безпеки, що характеризується певними умовами й погрозами.

«Загальні критерії» сприяють формуванню двох базових видів використовуваних на практиці нормативних документів – це *профіль захисту* й *завдання по безпеці*.

– ***Профіль захисту*** являє собою типовий набір вимог, яким повинні задовольняти продукти й/або системи певного класу.

– ***Завдання по безпеці*** містить сукупність вимог до конкретної розробки, їхнє виконання дозволить вирішити поставлені завдання по забезпеченню безпеки.

Криптографія – область специфічна, але загальне подання про її місце в *архітектурі безпеки* й про вимоги до криптографічних компонентів мати необхідно. Для цього доцільно ознайомитися з Федеральним стандартом США **FIPS 140-2** «Вимоги безпеки для криптографічних модулів» (Security Requirements for Cryptographic Modules). Він виконує організуючу функцію, описуючи зовнішній інтерфейс *криптографічного модуля*, загальні вимоги до подібних модулів і їхнього оточення. Наявність такого *стандарту* спрощує розробку *сервісів безпеки* й *профілів захисту* для них.

Криптографія як засіб реалізації *сервісів безпеки* має дві сторони: алгоритмічну й інтерфейсну. Розглянемо запропоновану в рамках Internet-співтовариства технічну *специфікацію* «Узагальнений прикладний програмний інтерфейс служби безпеки» (Generic Security Service Application Program Interface, **GSS-API**).

Інтерфейс безпеки **GSS-API** призначений для захисту комунікацій між компонентами програмних систем, побудованих в архітектурі *клієнт/сервер*. Він створює умови для взаємної *автентифікації* партнерів, що спілкуються, *контролює* цілісність повідомлень, що пересилаються, і є гарантією *їхньої* конфіденційності. Користувачами інтерфейсу безпеки GSS-API є комунікаційні протоколи (звичайно прикладного рівня) або інші програмні системи, що самостійно виконують пересилання даних.

Технічні *специфікації* IPsec [IPsec] мають, без перебільшення, фундаментальне значення, описуючи повний набір засобів забезпечення *конфіденційності* й *цілісності* на *мережному рівні*. Для домінуючого, в сучасний час, протоколу IP версії 4 вони носять факультативний характер; у перспективній версії IPv6 їхня реалізація обов'язкова. На основі IPsec будуються захисні механізми протоколів більше високого рівня, аж до прикладного, а також закінчені засобу безпеки, у тому числі *віртуальні приватні мережі*. Зрозуміло, IPsec істотно опирається на криптографічні механізми й ключову інфраструктуру.

Точно так само характеризуються й засоби безпеки ***транспортного рівня* (Transport Layer Security, TLS).** *Специфікація* TLS розвиває й уточнює популярний протокол Secure Socket Layer (SSL), використовуваний у великій кількості програмних продуктів самого різного призначення.

У згаданому вище інфраструктурному плані дуже важливі рекомендації **X.500 «Служба директорій: огляд концепцій, моделей і сервісів»** (The Directory: Overview of concepts, models and services) і **X.509 «Служба директорій: каркаси сертифікатів відкритих ключів і атрибутів»** (The Directory: Public-key and attribute certificate frameworks). У рекомендаціях X.509 описаний формат сертифікатів відкритих ключів і атрибутів – базових елементів інфраструктур відкритих ключів і керування привілеями.

Як відомо, забезпечення *інформаційної безпеки* – проблема комплексна, потребуюча погодженого вживання заходів на законодавчому, адміністративному, процедурному й програмно-технічному рівнях. При розробці й реалізації базового документа адміністративного рівня – *політики безпеки* організації – відмінною підмогою може стати рекомендація Internet-співтовариства **«Посібник з інформаційної безпеки підприємства»** (Site Security Handbook). У ньому висвітлюються практичні аспекти формування *політики* й *процедур безпеки*, пояснюються основні поняття адміністративного й процедурного рівнів, утримується мотивування дій, що рекомендуються, зачіпаються теми аналізу ризиків*, реакції на порушення* ІБ і дій після ліквідації порушення. Більш докладно останні питання розглянуті в рекомендації **«Як реагувати на порушення інформаційної безпеки»** (Expectations for Computer Security Incident Response). У цьому документі можна знайти й посилання на корисні інформаційні ресурси, і практичні ради процедурного рівня.

При розвитку й реорганізації корпоративних *інформаційних систем*, безсумнівно, виявиться корисною рекомендація «Як вибирати постачальника Internet-Послуг» (Site Security Handbook Addendum for ISPs). У першу чергу її положень необхідно дотримуватися в ході формування

організаційної й архітектурної безпеки, на якій базуються інші міри процедурного й програмно-технічного рівнів.

Для практичного створення й підтримки режиму *інформаційної безпеки* за допомогою регуляторів адміністративного й процедурного рівнів придасться знайомство із британським *стандартом* **BS 7799 «Керування інформаційною безпекою. Практичні правила»** (Code of practice for information security management) і його другою частиною **BS 7799-2:2002 «Системи керування інформаційною безпекою –** специфікація з посібником з використання» (Information security management systems – Specification with guidance for use). У ньому роз'ясняються такі поняття й процедури, як *політика безпеки*, загальні принципи організації захисту, *класифікація ресурсів* і керування ними, *безпека персоналу, фізична безпека*, принципи адміністрування систем і мереж, *керування доступом,* розробка й супровід ІС, планування безперебійної роботи організації.