Тема 1. Предмет та об'єкт захисту у інформаційній безпеці

У теорії захисту інформації у якості ***предмету захисту інформації*** розглядають ***інформацію,*** яка циркулює, накопичується та обробляється в сучасних комп'ютерних системах. Ця інформація відрізняється двоїстим поданням, високим ступенем обробки та передачі та концентрації інформації. У якості ***об'єкту захисту інформації***, при цьому, розглядається комп'ютерна система. У практиці інформаційної безпеки об'єкт захисту інформації розглядають у більш широкому розумінні, ніж комп'ютерна система. До цієї системи додаються приміщення, будівлі, а також територія, що межує з ними.

1.1. Класифікація інформаційних систем, визначення поняття інформаційно-комунікаційної системи

На поточний час в професійному середовищі циркулює низка термінів, яks визначають поняття систем, в яких інформація накопичується, обробляється та передається. До таких термінів можна віднести:

- *комп'ютерні (обчислювальні) системи;*
- *автоматизовані системи;*
- *комп'ютерні систем і мережі;*
- *інформаційно-телекомунікаційні системи;*
- *інформаційні і комунікаційні системи;*
- *інформаційно-комунікаційні системи.*

Обчислювальна система. Під обчислювальною системою розуміють сукупність програмних і апаратних засобів, призначених для обробки інформації. Обчислювальна система поєднує в собі технічні засоби обробки і передачі даних (засоби обчислювальної техніки і зв'язку), а також методи і алгоритми обробки даних, що реалізовані у вигляді відповідного програмного забезпечення (ПЗ).

Комп'ютерна система. За логікою, має визначення синоніму обчислювальної системи. Але у вітчизняних нормативних документах його тлумачення досить специфічне. Згідно НД ТЗІ 1.1-003-99 "Термінологія в

області захисту інформації в комп'ютерних системах від несанкціонованого доступу", комп'ютерна система – це сукупність програмно-апаратних засобів, яка подана для оцінки. Під оцінкою тут розуміють експертну оцінку захищеності інформації в цій системі, як складову експертизи або сертифікації на відповідність чинним нормативним документам і стандартам.

На практиці цей термін також використовується як синонім для *обчислювальних систем, автоматизованих систем та інформаційних систем*. Ми будемо використовувати термін "комп'ютерна система" як синонім терміну "обчислювальна система".

Автоматизована система (АС). Термін "Автоматизована система" вживається по відношенню до систем автоматизованої обробки інформації, що побудовані на основі обчислювальної техніки. Цей термін використовується не лише в контексті захисту оброблюваної інформації, з ним пов'язані численні стандарти, як, наприклад, ГОСТ серії 34 (Інформаційна технологія. Комплекс стандартів на автоматизовані системи).

Існують різні тлумачення терміну "Автоматизована система". В подальшому ми будемо дотримуватись визначення з НД ТЗІ 1.1-003-99: ***автоматизована система*** – це організаційно-технічна система, що реалізує інформаційну технологію і об'єднує (див. рис.):

- обчислювальну систему;
- фізичне середовище;
- персонал;
- інформацію, яка обробляється.

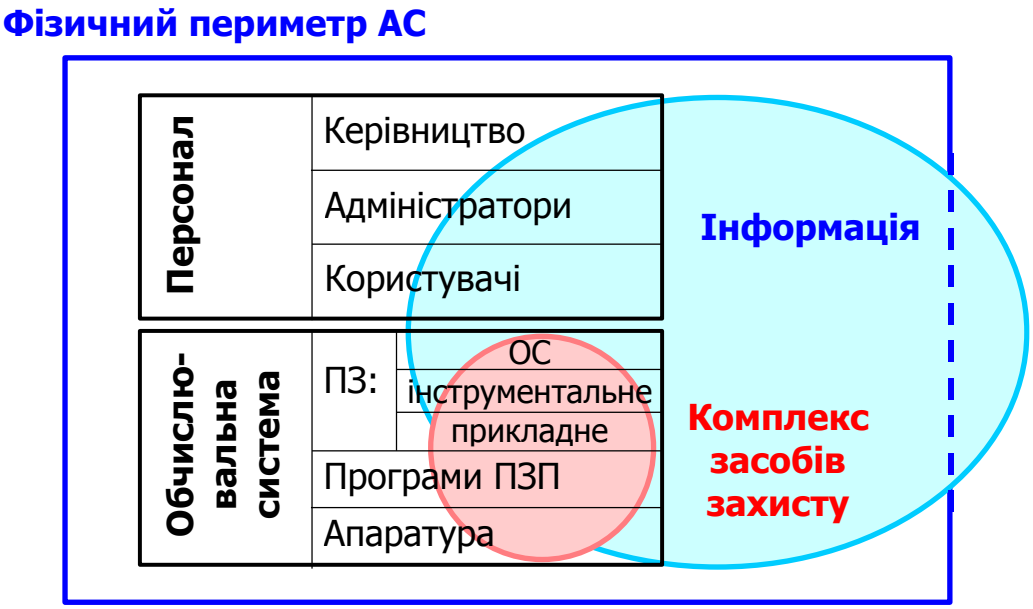


Рис. Автоматизована система

Для АС обчислювальна система, персонал, інформація з технологією її обробки і фізичне середовище розглядаються як складові. Також їх часто згадують як середовища функціонування системи.

Інформаційно-телекомунікаційна система (ІТС). Інформаційно-телекомунікаційною системою називають організаційно-технічну систему, яка включає функції ***інформаційної системи***, тобто організаційно-технічної системи, що реалізує певну технологію (або сукупність технологій) обробки інформації, та/або ***телекомунікаційної системи***, тобто технічної системи, що реалізує певну технологію (або сукупність технологій) передачі даних шляхом їх кодування у формі фізичних сигналів.

Закон «Про захист інформації в інформаційно-телекомунікаційних системах» від 31.05.05 (вступив у дію 1.01.06 р.) визначає інформаційно-телекомунікаційну систему як сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле.

В документі НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» підтверджується наведене вище визначення інформаційно-телекомунікаційної системи, але введено новий вид автоматизованої системи - ***інтегрованої системи***.

Інтегрована система – це сукупність двох або кількох взаємопов'язаних інформаційних та (або) телекомунікаційних систем, в якій функціонування однієї (кількох) з них залежить від результатів функціонування іншої (інших) таким чином, що цю сукупність у процесі взаємодії можна розглядати як єдину систему. Ця система вважається також інформаційно-телекомунікаційною системою.

Інформаційно – комунікаційні системи (ІКС) - це системи, які побудовано з використанням сучасних інформаційно – комунікаційних технологій (ІКТ).

Інформаційно–комунікаційні технології (ІКТ) – це сукупність обчислювальної техніки та обчислювальних мереж разом, що накопичують, обробляють та передають інформацію, подану у формі даних, голосових повідомлень та відео зображень, які базуються на сучасних комунікаційних технологіях (мобільний та супутниковий широкосмуговий зв'язок), новітніх сучасних матеріалах (оптоволокно) та програмному забезпеченні для нових, більш ефективних і розповсюджених видів застосування цих новітніх технологій і можливостей.

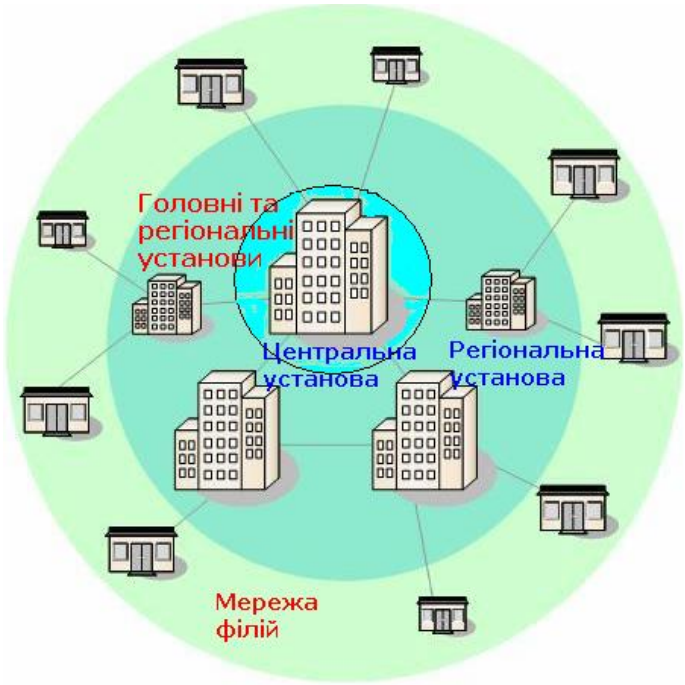
Треба зазичити, що загальноприйнятим терміном в Україні в галузі захисту інформації до поточного часу є «інформаційно-телекомунікаційні системи», саме він переважно використовується у законодавстві України щодо захисту інформації.

Терміни «інформаційно-телекомунікаційна система», «інтегрована система», «інформаційна і комунікаційна система», «інформаційно-комунікаційна система», «автоматизована система» у подальшому будемо використовувати як синоніми.

1.2. Приклади сучасних систем обробки інформації

Сучасні інформаційні системи різного призначення, розміру, форми власності можуть мати спільні риси і, навидь, схожу структуру. Наведемо приклад організації (компанії) з позиції обробки інформації (наприклад, страхової компанії, виробничого об'єднання, органу державної влади, тощо)

(рис). Інформація такої організації обробляється з використанням інформаційно-комунікаційної системи, приклад структурної схеми якої наведемо на наступному рисунки.



Центральна установа забезпечує накопичення та аналітичну обробку інформації, централізовану підтримку служб, а також реалізацію стратегій масштабу організації

Регіональні установа

Рис. Приклад організації (компанії) з позиції обробки інформації

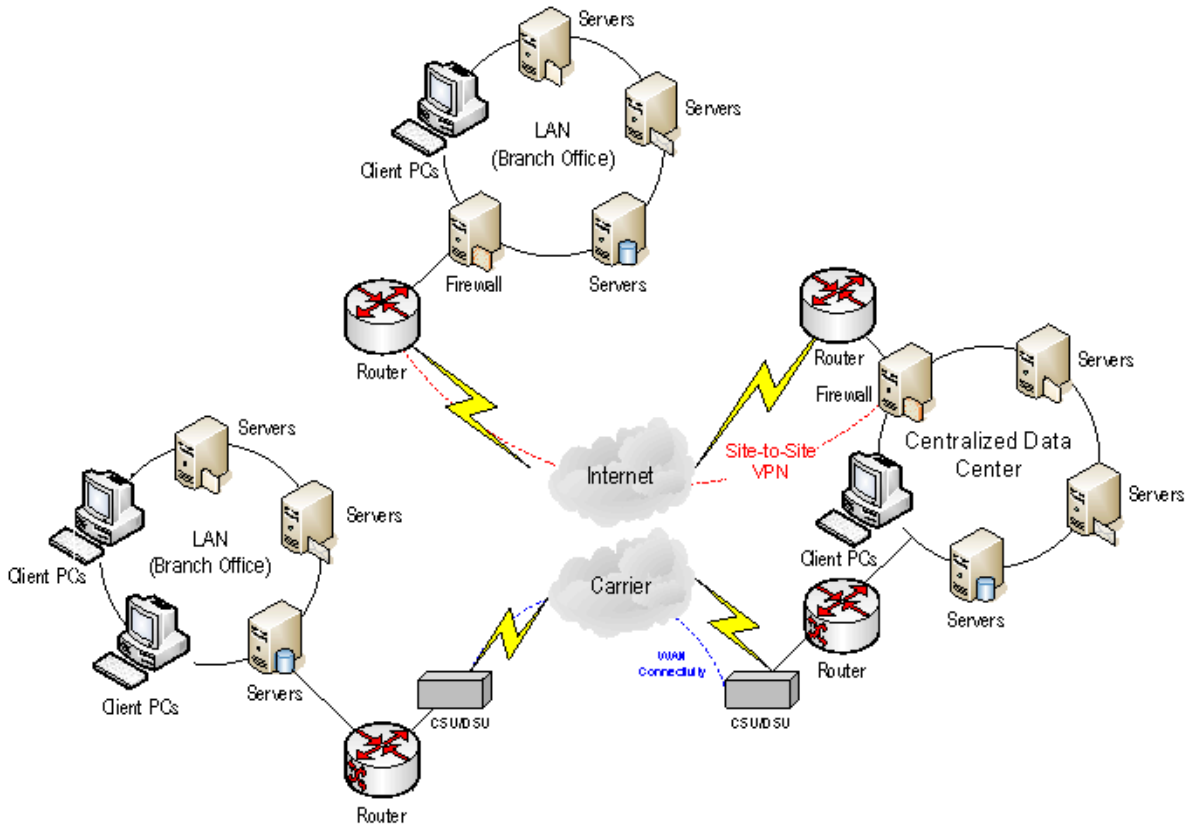


Рис. Структурна схема ІКС

При детальному порівнянні різних систем можна виділити спільні риси. В будь-якій ІКС можна виділити типові рівні, на яких вирішуються задачі, спільні для всіх систем. Як правило, виділяють 4 рівня (рис.).

Рис. Типові рівні ІКС

Розглянемо типові рівні ІКС знизу вверх:

- ***Рівень мережі*** – відповідає за взаємодію вузлів ІКС. Елементами ІКС, що відносяться до цього рівня, є модулі, які реалізують стеки протоколів мережевої взаємодії, наприклад, TCP/IP. Також на цьому рівні функціонує специфічна апаратура – мережеве обладнання.
- ***Рівень операційних систем*** (ОС) – відповідає за обслуговування програмного забезпечення, яке реалізує більш високі рівні, і його взаємодію з обладнанням. В якості типових елементів цього рівня можна назвати такі поширені ОС, як Microsoft Windows, Sun Solaris, Linux.
- ***Рівень систем керування базами даних*** (СКБД) – відповідає за зберігання та обробку даних. В якості типових елементів цього рівня можна назвати СКБД Oracle і MS SQL Server. Іноді СКБД є центральним елементом ІС (наприклад, облік товарів на складі), а іноді СКБД функціонує прозоро для користувачів і виконує допоміжні функції, зокрема для зберігання технологічної інформації самої ІС. Так, наприклад, система підтримки конфіденційного документообігу OPTiMA WorkFlow базується на СКБД MS SQL Server.
- ***Рівень прикладного ПЗ*** (застосувань) - найвищий рівень. Розрізняють прикладний компонент і компонент подання (рос. – *представления*), які є

складовими прикладного рівня. Прикладний компонент забезпечує виконання специфічних функцій ІС. Компонент подання відповідає за взаємодію з користувачем і подання даних у необхідній формі. На рівні прикладного ПЗ функціонують, наприклад, офісні застосування, такі як популярні Microsoft Office, Star Office або Open Office, бухгалтерські програми, спеціально розроблені для кожної окремої ІС програмні засоби, що реалізують специфічні для неї функції, і будь-які інші прикладні програми.

Тема 2. Загрози безпеці інформації

2.1. Поняття загрози інформації

Визначимо поняття загрози інформації та низку суміжних понять.

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***– 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*** (– 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".

2.2.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 яки загрози націлені;

• за характером впливу;

• за розміщенням джерела загроз.

2.2.1. Класифікація загроз інформаційної безпеки за її складовими

Класифікація загроз інформаційної безпеки за її складовими полягає у визначенні загроз (загрози), яки безпосередньо направлені на таки складові інформаційної безпеки, як ***цілісність, доступність, конфіденційність***. Усі загрози, що класифікуються за іншими ознаками можуть впливати на усі складові інформаційної безпеки.

2.2.2. Класифікація загроз інформаційної безпеки за компонентами інформаційних систем, на яки вони націлені

Класифікація загроз інформаційної безпеки за компонентами інформаційних систем, на яки загрози націлені полягає у визначенні загроз (загрози), яки 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.

2.2.3. Класифікація загроз інформаційної безпеки за характером впливу

Загрози інформаційної безпеці за характером впливу класифікують як ***випадкові та навмисні*** дії природного або техногенного характеру (див. рис.).

2.2.3.1. Випадкові загрози

Випадкові загрози – це загрози, яки 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***.

Рис. Загрози безпеці інформації

2.2.3.2. 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». 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 десятков километрів 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, яки 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) мікророботів візуального спостереження.

Інші методи «спеціальних впливів» характеризувати не будемо.

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, яки 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 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. Зображення електронопроміневого монітору комп'ютера може бути відтворено за допомогою звичайного телевізору, який має бути оснащений простим додатковим обладнанням синхронізації сигналів. 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. 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. 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, яки 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, яки 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.

2.2.4. 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***.

2.3. Поняття порушника інформаційної безпеки

В подальшому будемо використовувати терміни ***"порушник" і "зловмисник"*** у тих значеннях, які було наведено в підрозділі 3.1. «Поняття загрози інформації».

Нагадаємо, що ***порушниками*** називають особи, яки 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 ***“зломщик”*** (рос. – *“взломщик”*).

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.

2.4. Поняття про модель загроз та модель порушника

Результатом аналізу можливих загроз є ***модель загроз*** – абстрактний структурований опис загроз.

Нормативними документами України («Типове положення про службу захисту інформації в автоматизованій системі») рекомендовано таку структуру опису загрози:

На порушення яких властивостей інформації або АС спрямована загроза:

- порушення конфіденційності,
- порушення цілісності,
- порушення доступності інформації,
- порушення спостереженості та керованості АС.

Джерела виникнення загрози:

які суб’єкти АС або суб’єкти, зовнішні по відношенню до неї, можуть ініціювати загрозу (див. далі 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.

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 АС:

- 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.

2.5. Приклади дій порушника та типові атаки на інформаційній ресурс

Наведемо спрощену класифікацію, яка відображає найбільш типові атаки на розподілені автоматизовані системи. Ця класифікація запропонована Питером Меллом (Peter Mell):

- ***Віддалене проникнення*** *(remote penetration)*. Атаки, які дозволяють реалізувати віддалене керування комп'ютером через мережу.
- ***Локальне проникнення*** *(local penetration)*. Атака, що приводить до отримання несанкціонованого доступу до вузла, на якому вона ініційована.
- ***Віддалена відмова в обслуговуванні*** *(remote denial of service)*. Атаки, що дозволяють порушити функціонування системи або перезавантажити комп'ютер через мережу (в тому числі через Інтернет).
- ***Локальна відмова в обслуговуванні*** *(local denial of service)*. Атаки, що дозволяють порушити функціонування системи або перезавантажити комп'ютер, на якому вони ініційовані. Приклади атак цього типу: аплет, що перезавантажує процесор (наприклад, відкриттям великої кількості

вікон великого розміру), що приводить до неможливості обробки запитів інших програм.

- ***Сканування мережі*** *(network scanning)*. Аналіз топології мережі і активних сервісів, що доступні для атаки. Атака може здійснюватись за допомогою службового програмного забезпечення.
- ***Використання сканерів вразливостей*** *(vulnerability scanning)*. Сканери вразливостей призначені для пошуку вразливостей на локальному або віддаленому комп'ютері. Вони в першу чергу призначені служити діагностичним інструментом системних адміністраторів, але можуть бути використані і як зброя для розвідки й атаки. Найвідоміші з таких програмних засобів: SATAN, SystemScanner, Xspider, nessus.
- ***Злом паролів*** *(password cracking)*. Для цього використовуються програмні засоби, що підбирають паролі користувачів. В залежності від надійності системи зберігання паролів, можуть використовуватись методи зламу або підбору пароля за словником.
- ***Аналіз протоколів*** *(sniffing* - прослуховування трафіку*)*. Пасивна атака, яка спрямована на розкриття конфіденційних даних, зокрема, ідентифікаторів і паролів доступу.

До цієї класифікації не потрапили численні атаки, що спрямовані на введення в оману протоколів пошуку в мережі. На наш погляд, слід додати такий пункт:

- ***Підміна об'єкта*** *(spoofing)*. Типові приклади: несправжній DNS-сервер, підміна IP-адреси джерела (IP spoofing), несправжній ARP-запит (ARP spoofing).

Неважко помітити, що запропонована класифікація є не цілком послідовною. Перші чотири класи атак розрізняються здебільшого по кінцевому результату (або меті реалізації), а наступні – по способу їх здійснення.

ТЕМА 3. ОСНОВНІ СКЛАДОВІ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. ПРАВОВЕ ТА ЗАКОНОДАВЧЕ РЕГУЛЮВАННЯ

3.1. Характеристика системи регулювання інформаційної безпеки в Україні

Захист інформації як на рівні держави в цілому, так і на рівні організацій та окремих громадян має забезпечити держава. В Конституції України (стаття 17) визначається, що «захист суверенітету і територіальної цілісності України, забезпечення її економічної та ***інформаційної безпеки*** є найважливішими функціями держави, справою всього Українського народу».

Для реалізації цієї мети держава має:

• виробити політику в галузі інформаційної безпеки;

• законодавчо встановити статус, володарів та користувачів інформації, систем обробки та захисту інформації та інше;

• створити ієрархічну систему державних органів, яки створюють та впроваджують у життя політику інформаційної безпеки;

• створити систему стандартизації, ліцензування та сертифікації в галузі захисту інформації;

• підвищувати рівень освіти громадян в галузі інформаційної безпеки;

• встановити та дотримувати відповідальність громадян за порушення законодавства в галузі інформаційної безпеки.

Політика в галузі інформатизації та інформаційної безпеки

Політику в галузі інформаційної безпеки визначає Закон України «Про основи національної безпеки України».

Стаття 8 Закону України «Про основи національної безпеки України» визначає, що основними напрямами державної політики з питань ***національної безпеки в інформаційній сфери*** є:

- забезпечення інформаційного суверенітету України;
- вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для

розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері;

- наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;
- активне залучення засобів масової інформації до боротьби з корупцією, зловживаннями службовим становищем, іншими явищами, які загрожують національній безпеці України;
- забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції;
- вжиття комплексних заходів щодо ***захисту національного інформаційного простору*** та протидії монополізації інформаційної сфери України.

Законодавче оформлення статусу, володарів та користувачів інформації, систем обробки та захисту інформації

Законодавче оформлення статусу, володарів та користувачів інформації, систем обробки та захисту інформації визначають Закон України «Про інформатизацію», Закон України “Про державну таємницю”, Закон України “Про захист інформації в інформаційно-телекомунікаційних системах”, Закон України “Про захист персональних даних”. Основні положення цих законів будуть проаналізовані нижче у розділі «Класифікація інформації та інформаційних систем за законодавством України».

Система державних органів, які створюють та впроваджують у життя політику інформаційної безпеки

Політику в галузі інформаційної безпеки, підготовку законодавчих актів и нормативних документів, а також здійснення її виконання в Україні здійснює система державних органів - Президент України та Рада Національної безпеки

України, Кабінет Міністрів України, Верховна рада України та Служба спеціального зв'язку та захисту інформації України (Держспецзв'язку України) - уповноважений орган регулювання відносин в галузі інформаційної безпеки в Україні.

Система стандартизації, ліцензування та сертифікації в галузі захисту інформації

Система стандартизації, ліцензування та сертифікації в галузі захисту інформації в України регулює відносини у зазначених напрямках діяльності. Основу цієї системи створюють Закон України «Про сертифікацію», «Порядок проведення робіт із сертифікації засобів забезпечення технічного захисту інформації загального призначення – Введено в дію Наказом ДСТСЗІ СБ України і Держстандарту України від 09.07.2001р. № 329/32», «Положення про державну експертизу в сфері технічного захисту інформації – Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 29 грудня 1999 р. № 62» та інші.

Підвищення рівня освіти та відповідальності громадян за порушення законодавства в галузі інформаційної безпеки

В Україні створена та функціонує система вищої освіти в галузі інформаційної безпеки. Основу її складають 3 навчальних напрямки «Безпека інформаційних і комунікаційних систем», «Системи технічного захисту інформації», «Управління інформаційною безпекою», які об'єднанні у галузь знань «Національна безпека».

Відповідальність громадян за порушення законодавства в галузі інформаційної безпеки визначаються статтями 361 – 363 розділу XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Кримінального кодексу України.

3.2. Загальна характеристика нормативно-правової бази України з захисту інформації

Нормативно-правову базу у галузі захисту інформації в Україні складають низка законів, стандартів та нормативно-правових документів. Наведемо основні з них:

1. Закон України “Про інформацію” № 2657-XII від 02.10.1992. – ВВР, 1992, N 48, ст.650.
2. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах”, від 05.07.1994 № 80/94-ВР (Із змінами, внесеними згідно із Законом N 1703-IV від 11.05.2004, в редакції Закону N 2594-IV від 31.05.2005, ВВР, 2005, N 26, ст.347).
3. Закон України “Про державну таємницю” N 3855-XII від 21.01.1994, ВВР, 1994, N 16, ст.93 (остання редакція N 1519-IV від 19.02.2004).
4. Закон України “Про електронний цифровий підпис” N 852-IV від 22.05.2003, ВВР, 2003, N 36, ст.276.
5. Закон України “Про електронні документи і електронний документообіг”, N 851-IV від 22.05.2003, ВВР, 2003, N 36, ст.275 (Із змінами, внесеними згідно із Законом N 2599-IV від 31.05.2005, ВВР, 2005, N 26, ст.349).
6. Закон України “Про телекомунікації” N 1280-IV, ВВР, 2004, N 12, ст.155 (остання редакція від 01.02.2007).
7. Закон України “Про Державну службу спеціального зв’язку та захисту інформації України” від 23 лютого 2006 року № 3475-IV – ВВР, 2006, N 30, ст.258.
8. Концепція технічного захисту інформації в Україні, Затверджено постановою Кабінету Міністрів України від 08.10.1997 р. N 1126.
9. Положення про технічний захист інформації в Україні. – Затверджено Указом Президента України від 27.09.99р. № 1229.
10. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.
11. НД ТЗІ 1.1-002-99: Загальні положення по захисту інформації в комп'ютерних системах від несанкціонованого доступу, Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 р. № 22

12. НД ТЗІ 1.1-003-99: Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу, Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 р. № 22.
13. НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 р. № 22
14. НД ТЗІ 2.5-005-99: Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу, Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 р. № 22
15. НД ТЗІ 1.4-001-2000: Типове положення про службу захисту інформації в автоматизованій системі, Затверджено наказом ДСТСЗІ СБ України від 04.12.2000 р. № 53
16. НД ТЗІ 3.7-001-99: Методичні вказівки по розробці технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі, Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 р. № 22.
17. 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, Затверджено наказом ДСТСЗІ СБ України від 20.12.2000 р. № 60.
18. НД ТЗІ 2.1-001-01: Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення. Затверджено наказом ДСТСЗІ СБ України від 09.02.2001 р. № 2.
19. НД ТЗІ 2.5-008-02: Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2, Затверджено наказом ДСТСЗІ СБ України від 13.12.2002 р. № 84.
20. НД ТЗІ 2.5-010-03: Вимоги до захисту інформації WEB – сторінки від несанкціонованого доступу, Затверджено наказом ДСТСЗІ СБ України від 02.04.2003 р. № 33.

21. НД ТЗІ 3.7-003-05: Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі, Затверджено наказом ДСТСЗІ СБ України від 08.11.2005 р. №125.
22. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. – Затверджено наказом Держстандарту України від 19.12.96 р. № 511.
23. Положення про державну експертизу в сфері технічного захисту інформації – Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 29 грудня 1999 р. № 62, Зареєстровано в Міністерстві юстиції України 24 січня 2000 р. за № 40/4261.
24. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ЕОТ-95). – Затверджені наказом ДСТЗІ від 09.06.95р. № 25.
25. Тимчасові рекомендації з технічного захисту інформації вид витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ТЗІ-ПЕМВН-95). – Затверджені наказом ДСТЗІ від 09.06.95р. № 25.
26. Порядок проведення робіт із сертифікації засобів забезпечення технічного захисту інформації загального призначення – Введено в дію Наказом ДСТСЗІ СБ України і Держстандарту України від 09.07.2001 р. № 329/32. Зареєстровано в Міністерстві юстиції України від 26 липня 2001 р. за № 640/5831.
27. Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах. – Затверджено постановою Кабінету Міністрів України від 16.02.98р. № 180.
28. ГОСТ 34.201-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначения документов при создании автоматизированных систем (Взамен ГОСТ 24.101-80, ГОСТ 24.102-80)

29. ГОСТ 34.601-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания. (Взамен ГОСТ 24.601-86, ГОСТ 24.602-86)
30. ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы (Взамен ГОСТ 24.201-85)
31. ГОСТ 34.603-92 Информационная технология. Виды испытаний автоматизированных систем (Взамен ГОСТ 24.104-85 в части разд. 3.)
32. РД 50-34.698-90. Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы – требования к содержанию документов.
33. Закон України "Про захист персональних даних"

Додатково до вітчізнянних, визначимо низьку міжнародних стандартів та нормативно-правових документів, які на території України мають рекомендаційний характер:

1. Common Criteria for Information Technology Security Evaluation: Version 2.1. CCIMB-99-031. August 1999.
2. Common Methodology for Information Technology Security Evaluation: Version 2.3. CCMB-2005-08-004. August 2005.
3. ISO/IEC 10745:1995, Information technology – Open Systems Interconnection – Upper layers security model.
4. ISO/IEC 13594:1995, Information technology – Lower layers security.
5. ISO/IEC 10181-1:1996, Information technology – Security frameworks for open systems: Overview.
6. ISO/IEC 10181-2:1996, Information technology – Security frameworks for open systems: Authentication framework.
7. ISO/IEC 10181-3:1996, Information technology – Security frameworks for open systems: Access control framework.
8. ISO/IEC 10181-4:1996, Information technology – Security frameworks for open systems: Non-repudiation framework.

9. ISO/IEC 10181-5:1996, Information technology – Security frameworks for open systems: Confidentiality framework.
10. ISO/IEC 10181-6:1996, Information technology – Security frameworks for open systems: Integrity framework.
11. ISO/IEC 10181-7:1996, Information technology – Security frameworks for open systems: Security audit framework.
12. ISO/IEC 18045:2005. Information technology – Security techniques – Methodology for IT security evaluation
13. ISO/IEC 7498-1:1994, Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model.
14. ISO/IEC 9545:1994, Information technology – Open Systems Interconnection – Application Layer Structure.
15. ISO/IEC 8822:1994, Information technology – Open Systems Interconnection – Presentation Service Definition.
16. ISO/IEC 8326:1996, Information technology – Open Systems Interconnection – Session Service Definition.
17. ISO/IEC 8072:1996, Information technology – Open Systems Interconnection – Transport Service Definition.
18. ISO/IEC 8348:2002, Information technology – Open Systems Interconnection – Network Service Definition.
19. ISO/IEC 8886:1996, Information technology – Open Systems Interconnection – Data Link Service Definition.
20. ISO/IEC 10022:1996, Information technology – Open Systems Interconnection – Physical Service Definition.
21. ISO/IEC 7498-2:1989, Information processing systems – Open Systems Interconnection - Basic Reference Model – Part 2: Security Architecture.
22. IT Baseline Protection Manual. – BSI (Federal Agency for Security in Information Technology) – October 2000.
23. Security Architecture for Open Systems Interconnection for CCITT Applications. Recommendation X.800 – CCITT, Geneva, 1991.

24. ISO/IEC 17799:2000, Information technology – Code of practice for Information security management. International Standard.
25. ISO/IEC 15408-1:2005, Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model
26. ISO/IEC 15408-2:2005, Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements
27. ISO/IEC 15408-3:2005, Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements
28. ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements
29. ISO/IEC 27002:2005, Information technology – Security techniques – Code of practice for information security management
30. IEEE802.10B. IEEE Standards for Interoperable Local Area Network (LAN) Security (SILS): Part B - Secure Date Exchange. – April 1992.

3.3. Визначення поняття про інформаційну безпеку та суміжних понять в законодавстві України

В законодавстві України поняття інформаційної безпеки використовується, але у його частині, яка регулює відносини інженерно-технічної складової інформаційної безпеки, її визначення відсутнє. Там це поняття замінюється на поняття ***захисту інформації***.

Зазначимо, що англійський термін ***Information Security*** може бути перекладеним як ***інформаційна безпека***, ***безпека інформації***, інколи перекладається як ***захист інформації***. Якщо термінам безпека інформації і захист інформації можна надати однакове визначення як стану захищеності інформації, то зміст терміну інформаційна безпека визначає одночасно як стан захищеності інформації від загроз так і стан захищеності суб'єктів інформаційних відносин (людини, суспільства) від руйнуючої інформації (деструктивні, руйнуючи інформаційні впливи, пропаганда насильства, інформаційні війни та ін.). Таким чином, існує поняття ***захисту від інформації***.

В НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу» від 01.07.99 р. (підрозділ 5.1 – загальні положення) надано наступне визначення ***захисту інформації.***

Захист інформації, що обробляється в АС, полягає в створенні і підтримці в дієздатному стані системи заходів, як технічних (інженерних, програмно-апаратних), так і не технічних (правових, організаційних), що дозволяють запобігти або ускладнити можливість реалізації ***загроз***, а також знизити потенційні збитки. Іншими словами, захист інформації спрямовано на забезпечення безпеки оброблюваної інформації і АС в цілому, тобто такого стану, який забезпечує збереження заданих властивостей інформації і АС, що її обробляє.

Система зазначених заходів, що забезпечує захист інформації в АС, називається ***комплексною системою захисту інформації*** (далі - ***КСЗІ***).

Загроза інформації – це потенційно можливий несприятливий вплив. Несприятливими впливами називаються впливи, які призводять до зниження цінності інформаційних ресурсів.

В НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» від 28.04.99 р. (підрозділ 4.1 - Терміни і визначення) надано наступне визначення захисту інформації та суміжних термінів.

3.1.6. ***Безпека інформації*** (information security) — стан інформації, в якому забезпечується збереження визначених ***політикою безпеки*** властивостей інформації.

3.1.7. ***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.

3.1.8. ***Комплексна система захисту інформації (***далі – ***КСЗІ)*** — сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС.

3.1.9. ***Комплекс засобів захисту*** (далі - ***КЗЗ)*** (trusted computing base) — сукупність програмно-апаратних засобів, які забезпечують реалізацію політики безпеки інформації.

3.1.4. ***Політика безпеки інформації*** (information security policy) — сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок обробки інформації.

Закон «Про захист інформації в інформаційно-телекомунікаційних системах» (від 31.05.05, вступив у дію 1.01.06 р.) в статті 1 - Визначення термінів надає наступну редакцію захисту інформації в системі та технічного захисту інформації.

Захист інформації в системі - діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі.

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.

3.4. Класифікація інформації та інформаційних систем за законодавством України

Класифікація інформації. В законодавстві України, зокрема, Законі України «Про інформацію» (стаття 28) за режимом доступу інформація поділяється ***на відкриту інформацію та інформацію з обмеженим доступом***. Контроль за режимом доступу до інформації здійснює держава.

Стаття 30 Закону України «Про інформацію» визначає, що інформація з обмеженим доступом за своїм правовим режимом поділяється на ***конфіденційну і таємну***.

Конфіденційна інформація - це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов.

Стосовно інформації, що є власністю держави і знаходиться в користуванні органів державної влади чи органів місцевого самоврядування, підприємств, установ та організацій усіх форм власності, з метою її збереження може бути відповідно до закону встановлено обмежений доступ - надано статус ***конфіденційної*** *(інколи використовують термін* ***ДСК – для службового користування)***. Порядок обліку, зберігання і використання документів та інших носіїв інформації, що містять зазначену інформацію, визначається Кабінетом Міністрів України.

Громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлюють для неї систему (способи) захисту.

Таємна інформація - це інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі.

Закон України «Про державну таємницю» (стаття 1) визначає що ***державна таємниця*** - вид таємної інформації, що охоплює відомості у сфері оборони, економіки, зовнішніх відносин, державної безпеки і охорони правопорядку, розголошення яких може завдати шкоди життєво важливим інтересам України і які визнані у порядку, встановленому цим Законом, державною таємницею та підлягають охороні з боку держави. ***Ступінь секретності*** - категорія, яка характеризує важливість такої інформації, можливу шкоду внаслідок її розголошення, ступінь обмеження доступу до неї та рівень її охорони державою. Критерії визначення ступеня секретності інформації встановлює Державний комітет України з питань державних секретів.

Віднесення інформації до категорії таємних відомостей, які становлять державну таємницю, і доступ до неї громадян здійснюється відповідно до статті 7 Закону України «Про державну таємницю». Порядок обігу таємної інформації та її захисту визначається відповідними державними органами за умови додержання вимог, встановлених цим Законом.

Відповідно до Закону України "Про державну таємницю" ***Звід відомостей, що становлять державну таємницю (далі - ЗВДТ)***, є єдиною формою реєстрації цих відомостей в Україні. З моменту опублікування ЗВДТ держава забезпечує захист і правову охорону відомостей, які зареєстровані в ньому. ЗВДТ формується Службою безпеки України на підставі рішень ***державних експертів з питань таємниць*** про віднесення інформації до державної таємниці та висновків державних експертів про скасування раніше прийнятих рішень, а у випадках, передбачених статтею 12 Закону України "Про державну таємницю" - на виконання рішень суду.

Класифікація інформаційних систем. Класифікацію інформаційних систем надано в НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу». В цьому документі за сукупністю характеристик АС (конфігурація апаратних засобів ОС і їх фізичне розміщення, кількість різноманітних категорій оброблюваної інформації, кількість користувачів і категорій користувачів) виділено три ієрархічні класи АС, вимоги до функціонального складу КЗЗ яких істотно відрізняються:

- ***АС-1*** (клас «1») — ***одномашинний однокористувачевий комплекс***, який обробляє інформацію однієї або кількох категорій конфіденційності. Істотні особливості: в кожний момент часу з комплексом може працювати тільки один користувач, хоч у загальному випадку осіб, що мають доступ до комплексу, може бути декілька, але всі вони повинні мати однакові повноваження (права) щодо доступу до інформації, яка оброблюється. Приклад - автономна персональна обчислювальна машина, доступ до якої контролюється з використанням організаційних заходів;

- ***АС-2*** (клас «2») — ***локалізований багатомашинний багатокористувачевий комплекс***, який обробляє інформацію різних категорій конфіденційності. Істотна відміна від попереднього класу — наявність користувачів з різними повноваженнями по доступу і/або технічних засобів, які можуть одночасно здійснювати обробку інформації різних категорій конфіденційності. Приклад – локальна мережа;
- ***АС-3*** (клас «3») — ***розподілений багатомашинний багатокористувачевий комплекс***, який обробляє інформацію різних категорій конфіденційності. Істотна відміна від попереднього класу — необхідність передачі інформації через незахищене середовище або, в загальному випадку, наявність вузлів, що реалізують різну політику безпеки. Приклад — глобальна мережа Інтернет.

3.5. Порядок та умови доступу та обробки інформації за визначенням законодавством України

Закон «Про захист інформації в інформаційно-телекомунікаційних системах» (від 31.05.05, вступив у дію 1.01.06 р.) встановлює наступні ***порядок та умови доступу та обробки інформації***.

В статті 4 - Доступ до інформації в системі цього закону, ***порядок доступу до інформації***, перелік користувачів та їх повноваження стосовно цієї інформації ***визначаються власником інформації***. Порядок доступу до інформації, яка є власністю держави, 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 власника в порядку, встановленому законом.

В Статті 8 - Умови обробки інформації в системі цього закону, ***умови обробки інформації*** в системі визначаються ***власником системи*** відповідно до договору з власником інформації, якщо інше не передбачено законодавством.

Інформація, яка є власністю держави, або інформація з обмеженим доступом, вимоги щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням ***комплексної системи захисту інформації (КСЗІ)*** з

підтвердженою відповідністю. ***Підтвердження відповідності*** здійснюється за результатами ***державної експертизи*** в порядку, встановленому законодавством.

Для створення комплексної системи захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають ***сертифікат відповідності*** або ***позитивний експертний висновок за результатами державної експертизи*** у сфері технічного та/або криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюються в порядку, встановленому законодавством.

В Статті 9 - Забезпечення захисту інформації в системі цього закону, відповідальність за забезпечення захисту інформації в системі ***покладається на власника системи***. Власник системи, в якій обробляється інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює ***службу захисту інформації (СЗІ)*** або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним. Про спроби та/або факти несанкціонованих дій у системі щодо інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, власник системи повідомляє уповноважений орган у сфері захисту інформації.

Порядок створення, завдання, функції, структура та повноваження якої визначено в НД 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі».

Тема 4. Основні методи захисту інформації в комп'ютерних системах

4.1. Основі теоретичні положення захисту інформації в комп'ютерних системах

Захист інформації – галузь знань, яка має відповідну теорію, що складає її фундаментальне підґрунтя. ***Теорія захисту інформації*** – це наука про загальні принципи та методи побудови захищених інформаційно-комунікаційних систем.

Теорія захисту інформації – природнича наука, яка має відповідні аксіоматику, понятійний та формальний апарат. Основним методологічним інструментом теорії захисту інформації, яка оперує складними системами, є методи системного аналізу для вивчення систем і теорії прийняття рішень для розв'язання задач синтезу систем захисту інформації. Всі положення теорії захисту інформації мають базуватися на доказовому підході та відповідати вимогам ***несуперечності, повноти і розв'язаності***.

Несуперечність – властивість теорії, коли перетворення формул не ведуть до виникнення двох і більше результатів, які спростовують один одне. ***Повнота*** – властивість теорії, в якій не виникають твердження, що не вдається ні довести ані спростувати. ***Розв'язаність*** – властивість теорії, в якій існує єдиний механізм (алгоритм) для визначення істинності або фальшивості будь якого твердження в цієї теорії.

На поточний час в теорії захисту інформації використовуються два підходи для аналізу та синтезу систем безпеки – формальний та неформальний (описовий).

Традиційно ***формальний підхід теорії захисту інформації*** складають етапи визначення сукупності політики безпеки, критерію безпеки та моделі безпеки ІКС у формальному вигляді. Важливим етапом формального підходу є проведення доказу відповідності системи безпеки критерію безпеки при дотриманні встановлених правил та обмежень. За умови виконання останнього етапу у теорії захисту інформації говорять про "гарантованість" захисту інформації. Зазначимо, що у теорії захисту інформації також існують розділи, яки не оперують поняттям гарантованості таки як методи оптимального проектування систем захисту інформації, аналіз ризиків, моделювання окремих процесів захисту та інші.

На поточний час найбільш розвинутими формальними розділами теорії захисту інформації є ***математичні методи криптографії та моделювання політик безпеки.*** Сучасний формальний базис теорії захисту інформації у великої мірі сформувався під впливом криптографії, яка почала формуватись значно раніше. Формальний підхід теорії захисту інформації знаходиться у стадії

становлення і не може задовольнити всіх завдань, які виникають при дослідженні та створенні систем захисту інформації. Тому, цій підхід доповнюється традиційним неформальним (описовим) підходом.

Неформальний (описовий) підхід теорії захисту інформації носить характер опису методів і механізмів, які використовуються для захисту інформації в автоматизованих системах.

Цій підхід використовується у випадку, якщо формальні методи з будь-яких причин не можуть бути використані при аналізі і синтезі систем захисту інформації, чи взагалі не розроблені.

Треба зазначити, що теорія захисту інформації до цього часу залишається відносно замкнутою науковою дисципліною у частині розробки та впровадження формальних методів. Розвиток цих методів не завжди є синхронізованим із досягненнями як класичних, так і сучасних наук. Цим пояснюється дуже розповсюджені ілюзії користувачів інформаційних технологій про те, що якість захисту інформації визначається виключно кількістю і надійністю механізмів захисту, а формальний підхід мало що дає.

Теорія захисту інформації як наука, що знаходиться на стадії розвитку, зіткнулась з колом проблем. Частина з цих проблем вже є розв’язаною, інші очікують розв’язання. Розглянемо декілька базових проблем теорії захисту інформації, які на поточний час розв’язані.

Важливою проблемою теорії захисту інформації є проблема ***складності задачі вивчення (аналізу) систем захисту інформації***. У сучасній теорії захисту інформації цю проблему розв’язують, застосовуючи метод ієрархічної декомпозиції складних систем. З використанням цього методу, загальну складну систему розкладають на низьку рівнів ієрархії. При цьому, верхній рівень ієрархії складає політика безпеки, другий рівень – системи підтримки політики безпеки, третій рівень – механізми захисту, четвертий рівень – реалізація механізмів безпеки. Вивчення цих підсистем проводять із застосуванням специфічних для кожного рівня ієрархії методів аналізу.

Наступною проблемою теорії захисту інформації є проблема ***побудови (синтезу) “гарантовано захищеної системи”***. Проблема полягає у протиріччі

між вимогами до гарантованості і принциповою неможливістю побудувати "гарантовано захищену систему" у класі відкритих систем. В теорії відкритих систем проблему гарантованої безпеки відносять до ***алгоритмічно нерозв'язних проблем***.

Алгоритмічно нерозв'язною проблемою є клас задач, для якого не можна запропонувати ніякого єдиного алгоритму, який розв'язував би усі задачі з указаного класу.

Доказове обґрунтування відсутності гарантованої безпеки у відкритих системах надає, наприклад, теорема про неможливість розв'язати задачу забезпечення безпеки довільної системи у загальному випадку за умови загального завдання на доступ, сформульована в роботі М.Харрісона, В.Руззо, Дж.Ульмана. Рішення цієї проблеми проводиться шляхом декомпозиції загальної вихідної проблеми гарантованого захисту інформації у комп'ютерних системах на сукупність двох задач. Перша з цих задач полягає у коректному формулюванні політики безпеки, а друга – у побудові (синтезі) системи захисту інформації, яка гарантовано підтримує політику безпеки.

Наведені вище підходи до розв'язання проблем аналізу і синтезу систем захисту інформації вперше були впроваджені у Критеріях оцінки захищених комп'ютерних систем Міністерства оборони США (англ. – Trusted Computer System Evaluation Criteria, TCSEC), відомих також як "Оранжева книга", у 80-х роках минулого сторіччя та складають теоретичний базис багатьох сучасних стандартів захисту інформації.

Основні типи політик безпеки

При побудові систем захисту інформації необхідно сформулювати мету, головні умови та ресурси щодо захисту та розподілу інформації. Це завдання визначають як побудову політики безпеки.

У критеріях захищеності комп'ютерних систем TCSEC надано наступне визначення ***політики безпеки***. ***Політика*** **безпеки** – це набір норм, правил і практичних прийомів, які регулюють управління, захист і розподіл цінної інформації.

Наведене визначення політики дозволяє використовувати певний апарат для її реалізації. Наявність політики безпеки та її формального опису у вигляді моделі безпеки за умови дотримання системою визначених правил та обмежень, дозволяє провести формальне доведення відповідності системи визначеному критерію безпеки.

У загальному випадку визначене завдання є багатоальтернативним, не має єдиного розв'язку, часто несе в собі протиріччя. Так, наприклад, між вимогами до ефективності функціонування системи захисту інформації та забезпеченням ефективності функціонування інформаційної системи існує протиріччя.

Поняття політики безпеки, на відміну від поняття ***несанкціонованого доступу (НСД)***, є більш широким. Політика безпеки разом з поняттям дозволених доступів, оперує поняттям недозволених доступів. Виконання політики безпеки забезпечує необхідні, а інколи і достатні умови безпеки системи.

У сучасній теорії захисту інформації розглядають такі політики безпеки: дискреційна (розмежувальна), мандатна (багаторівнева), ролевого розмежування доступів, ізольованого програмного середовища, безпеки інформаційних потоків та інші.

Дискреційна політика безпеки

Дискреційна політика безпеки - за іншими перекладами – розмежувальна, – політика, яка базується на ***дискреційному керуванні доступом*** (рос. – *дискреционное управление доступом, избирательное управление доступом, произвольное управление доступом*, англ. – *discretionary access control*).

Дискреційна політика безпеки передбачає, що права доступу суб'єктів до кожного окремого об'єкта системи можуть бути довільним чином обмежені на основі деякого зовнішнього по відношенню до системи правила. Також дискреційна політика безпеки вимагає ідентифікованості всіх суб'єктів та об'єктів системи.

Основний елемент дискреційного розмежування доступу ***є матриця доступу. Матриця доступу*** – матриця D розміром $|S|\times|O|$, рядки якої

відповідають суб'єктам, а стовпчики – об'єктам. Кожний елемент матриці доступу $D[s,o] \subseteq R$ визначає права доступу суб'єкта s до об'єкта o, де R – множина прав доступу.

Суб'єкти s є активними сутностями, здебільшого це користувачі або процеси. Об'єкти o є пасивними сутностями, що потребують захисту. Це можуть бути, наприклад, файли, записи баз даних, сегменти оперативної пам'яті. У деяких операціях доступу суб'єкти можуть виступати як пасивні сутності, до яких здійснюють доступ інші суб'єкти, тому множини S та O знаходяться у відповідності $S \subset O$.

У матриці доступу D кожен рядок відповідає певному суб'єктові s, а кожен стовпчик – об'єктові o (рис.). Елементом матриці $D[s,o]$ є множина прав доступу, або повноважень суб'єкта s стосовно об'єкта o. Ці права, власне, і визначають, що може робити суб'єкт з об'єктом.

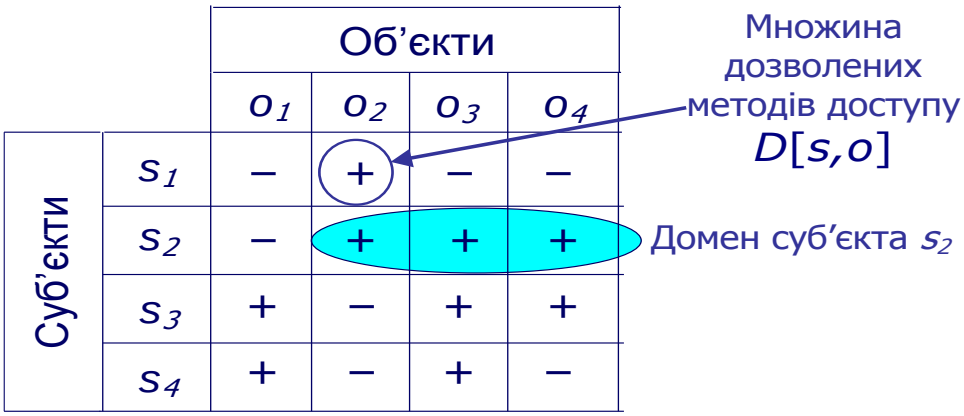


Рис. Матриця доступу *D*

Підмножина об'єктів, до яких визначений суб'єкт має певні права доступу, називається ***доменом*** цього суб'єкта.

Матриця доступу дуже розріджена і неефективна з точки зору використання пам'яті. Тому, замість неї у реальних системах використовуються ***списки доступу та списки повноважень***. ***Список доступу*** асоціюється з кожним захищеним об'єктом в системі і містить в собі ідентифікатори різних суб'єктів разом з їхніми правами доступу до даного об'єкту (список доступу, таким чином, описує стовпчик матриці доступу). На відміну від списку доступу, ***список повноважень*** асоціюється з кожним суб'єктом в системі і містить в собі ідентифікатори об'єктів разом з повноваженнями цього суб'єкта стосовно цих

об’єктів. Список повноважень, таким чином, відповідає рядкові матриці доступу.

При використанні матричної моделі безпеки політика безпеки інформації містить не лише саму матрицю доступу, яка описує правила розмежування доступу, але й обмеження, що накладаються на спосіб модифікації матриці доступу. Так, у випадку довірчого керування доступом всі права на зміну прав доступу до об’єкта надаються (довіряються) суб’єктові, що є власником цього об’єкта. Тобто, якщо список прав доступу суб’єкта *s* до об’єкта *o* містить право власника, то суб’єкт *s* отримує повний контроль над стовпчиком матриці доступу, що відповідає *o*. У випадку адміністративного керування доступом система захисту визначає можливість доступу суб’єктів до об’єктів, базуючись на мітках або атрибутах доступу, які може встановлювати або змінювати лише спеціально призначений адміністратор.

Перевагою дискреційної політики безпеки є проста реалізація системи розмежування доступу і, як наслідок, її широка розповсюдженість на практиці. Разом з цим ця політика вважається недосконалою із-за низки суттєвих недоліків.

Недоліками цієї політики є статичність правил розмежування доступу, яки не враховують динаміку змін стану комп’ютерної системи. Також, у випадку використання дискреційної політики безпеки, при доступі суб’єкта до об’єкта кожного разу необхідно визначати права доступу та аналізувати їх вплив на безпеку системи, що знижує її прозорість. У загальному випадку для систем дискреційного політики задача перевірки безпеки є алгоритмічно нерозв’язною. Доведення того факту, що система, у якій реалізовано дискреційну політику, є захищеною у заданому стані, має бути проведено для кожної конкретної системи и для кожного стану цієї системи.

Широковідомою практичною проблемою систем дискреційної політики є проблема їх нечутливості до впливу троянських програм (“троянських коней”).

Мандатна політика безпеки

Мандатна політика безпеки, за іншими перекладами – нормативна, примусова, або багаторівнева – політика, яка базується на *мандатному керуванні доступом* (рос. – *мандатное управление доступом*, *нормативное управление доступом*, *полномочное управление доступом*, *принудительное управление доступом*, англ. – *mandatory access control*).

Мандатна політика безпеки передбачає існування наступних умов: визначеності решітки конфіденційності інформації; надання кожному об'єкту системи рівня конфіденційності, який визначає цінність інформації, яка містися в ньому; задоволення вимоги ідентифікованості всіх суб'єктів та об'єктів системи.

Головне завдання мандатної політики безпеки – запобігання витоку інформації від об'єктів з високим рівнем доступу до об'єктів з низьким рівнем доступу.

Найбільш розповсюдженим описом мандатної політики безпеки є модель Белла – ЛаПадула. Ця модель гарантує, що суб'єкт може ознайомитись з інформацією лише тоді, коли має на це достатні повноваження, і будь-який суб'єкт (крім адміністратора, якому надано повноваження встановлювати рівні конфіденційності об'єктів) ніяким чином не зможе здійснити перенесення даних з об'єкта з вищим рівнем конфіденційності у об'єкт з більш низьким рівнем конфіденційності. Отже, це – модель конфіденційності.

Мандатна політика реалізується з використанням адміністративного керування доступом.

Перевагами мандатної політики безпеки є те, що її правила більш прозорі і зрозумілі у порівняні з правилами дискреційної політики. Системи, що побудовані на цієї політиці безпеки також більш надійні у порівнянні із системами, які побудовані на дискреційної політиці безпеки.

У загальному випадку для систем мандатної політики задача перевірки безпеки є алгоритмічно розв'язною і безпека систем мандатної політики є доведеною.

Недоліками мандатної політики безпеки є значні вимоги до обчислювальних ресурсів та складність у практичної реалізації.

Математичні моделі безпеки

Формальне визначення політики безпеки називають ***математичною моделлю безпеки.***

Згідно з 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. Серед моделей безпеки найбільше розповсюдження отримали моделі Харрісона-Руззо-Ульмана, Take-Grant, Белла-ЛаПадула та інші.

4.2. Захист від апаратних та програмних закладок, впроваджених на етапах розробки та виробництва

Несанкціонована зміна проектних рішень, зокрема зміна алгоритмічної, програмної, або технічної структури комп'ютерної (інформаційної) системи може відбутися на етапах її розробки та експлуатації. ***Несанкціоновану зміну структури (НЗС)***, яка була здійснена на етапах розробки чи модернізації комп'ютерної (інформаційної) системи називають ***закладками***.

Для захисту від даних загроз на різних етапах життєвого циклу комп'ютерних систем вирішуються різні задачі. На ***етапах розробки чи модернізації*** комп'ютерної системи необхідно максимально виключити наявність ***помилок та закладок***, на ***етапі експлуатації*** крім контролю та виключення помилок та закладок необхідно забезпечувати ***цілісність та незмінність структур системи***.

Для того, щоб запобігти несанкціонованої зміні проектних рішень на рівнях алгоритмічної, програмної, або технічної структури комп'ютерної системи необхідно дотримуватись низькі ***основних принципів:***

● залучати до розробки висококваліфікованих фахівців;

● при розробці використовувати ієрархічні структури, стандартні конструкції та блоки, сучасні технології програмування;

● автоматизувати процес розробки;

● проводити ретельний контроль процесу розробки;

● сертифікувати кінцевий продукт та інші.

4.3. Захист від несанкціонованої зміни структур на рівні апаратних та програмних засобів у процесі експлуатації

З метою захисту від ***несанкціонованої зміни структури програмних і апаратних засобів комп'ютерної системи у процесі експлуатації*** необхідно виконувати наступні заходи:

● охорона приміщень;

● розмежування доступу до обладнання;

● протидія несанкціонованому підключенню обладнання;

● захист засобів управління і комутації, а також внутрішнього монтажу від несанкціонованого втручання;

● протидія впровадженню шкідливих програм.

4.4. Захист комп'ютерних систем від несанкціонованого доступу

Несанкціонований доступ (НСД) до інформації в комп'ютерних системах є найнебезпечнішою загрозою інформації. Як правило НСД до інформації здійснюється з використанням:

● знання комп'ютерної системи і вміння працювати на неї;

● відомостей про систему захисту інформації;

● вад програмних і апаратних засобів;

● помилки та необачливість обслуговуючого персоналу та користувачів та інші.

З метою захисту інформації від НСД створюється ***система розмежування доступу (СРД)*** до інформації. СРД є одним з дієвих механізмів комплексних систем захисту інформації.

Одним з механізмів зловмисника для дослідження СРД з метою несанкціонованого доступу до інформації є ***дослідження і копіювання інформації*** про систему захисту інформації (СЗІ). Для протидії цієї загрозі інформації використовується комплекс засобів і заходів і створюється ***система захисту від дослідження і копіювання інформації (СЗДК).*** Таким чином, СРД та СЗДК є підсистемами системи захисту інформації від НСД.

В основі функціонування СРД знаходиться певна модель політики безпеки. Найбільше розповсюдження ***мають дискреційна та мандатна політики безпеки, які були розглянуті у підрозділі 4.1.***

Основними елементами, які складають СРД є блок ідентифікації та автентифікації суб'єктів доступу, диспетчер доступу, блок криптографічного перетворення інформації при її збереженні та передачі, блок очистки пам'яті.

4.5. Поняття про методи криптографічного захисту інформації

Історична довідка з криптографії

Криптографія, як наука, має велику історію. Історію криптографії поправу визначають як історію розвитку науки захисту інформації. Тому перед тим, як розглянути основні криптографічні методи захисту інформації, наведемо історичну довідку з розвитку криптографії.

Криптографічні методи захисту інформації з'явились більш ніж п'ять тисяч років тому, практично одночасно з зародженням письменності. Історія криптографії має окремі факти використання шифрованих повідомлень у древніх цивілізаціях Єгипту, Месопотамії та Індії.

В державах давньої Греції у V-VI сторіччях до нашої ери криптографія активно розвивалася та використовувалася. В працях грека Полібія того часу наводиться опис системи шифрування "квадрат Полібія", в древній Спарті були створені та використовувалися прилади для шифрування – таблиця Енея та низка інших. У Давньому Римі також використовували криптографію – відомою є

праця Юлія Цезаря, де є опис шифру. Внесок в розвиток криптографії зробили видатні мислителі того часу – Аристотель, Піфагор, Платон.

Подальший розвиток криптографія набула у VIII-IX сторіччях нашої ери в країнах арабського світу. Сучасні математика та криптографія зобов'язані арабському світу того часу арабським цифрам та арабським системам шифрів, в тому числі шифрів із застосуванням декількох шифроабеток.

У часи епохи Відродження в XIV-XVI сторіччях криптографія продовжувала розвиватися, з'явилися шифри – "Міланський ключ", "Єврейський шифр", код з перешифруванням Л. Альберті, роботи з криптографії Д. Кардано, Б. Виженера. У ті часи були отримані результати з алгебри Л. Фібоначчі, Н. Оремом, Ф. Вієтом та іншими, які надали підґрунтя для подальшого розвитку криптографії.

У XVII—XIX сторіччях сформувався та набув подальший розвиток криптоаналіз – наука, яка займається дешифруванням. Розвиток криптоаналізу був стимульований спеціальними службами провідних країн світу того часу, яки створили дешифрувальні служби. Становлення дешифрувальної справи того часу пов'язують з іменами математиків та фахівців Д. Валлисом в Англії, А. Россиньолем та Ч. Беббиджем у Франції, графом Гронсфельдом в Германії, Х. Гольбахом, Ф. Епінусом в Росії та іншими. У ці часи також продовжився розвиток криптографії.

Історія криптографії XX сторіччя пов'язана з винаходом та активним використанням під час другої світової війни електромеханічних шифраторів. Лідирували шифратори двох типів: на комутаційних дисках чи роторах та на цевочних дисках. Широковідома німецька шифрувальна машина "Энігма" використовувала перший тип комутаційних дисків, а американська шифрувальна машина М-209 – другий. В ті часи на розвиток криптографії працюють такі всесвітньо відомі математики як К. Шеннон та С. Куллбак в Сполучених Штатах Америки, В. Котельников, А. Марков та А. Гельфонд в Радянському Союзі, та інші.

В наші часи криптографія остаточно оформилась як математична наука, вона орієнтована на сучасні засоби обчислювальної техніки та телекомунікацій.

Основні поняття криптографії

Криптографія (англ. – *Cryptography*) – це наука, яка займається вивченням та розробкою методів, способів та засобів перетворення інформації у вигляд, який ускладнює чи робить неможливим несанкціоновані дії з нею. Криптографія базується на методах (алгоритмах) шифрування та дешифрування.

Шифрування (англ. – *Encryption*) – це процес криптографічного перетворення даних, за допомогою якого відкритий текст перетворюється в шифротекст з метою захисту від несанкціонованого доступу. ***Дешифрування*** (англ. – *Decryption*) – це процес, зворотній шифруванню. ***Алгоритм шифрування***, криптографічний алгоритм або криптоалгоритм (англ. – *Encryption algorithm*) – це алгоритм, згідно якого здійснюється криптографічне перетворення інформації. Криптографія разом з ***криптоаналізом*** та, за деякими визначеннями, ***стеганографією***, є складовою науки – ***криптології.***

Криптоаналіз (англ. – *Cryptanalysis*) – це складова криптології, наука, що займається вивченням та розробкою методів способів та засобів розкриття шифрів. ***Криптологія*** (англ. – *Cryptology*) – це наука, складовими якої є *криптографія, криптоаналіз* та, за деякими визначеннями, ***стеганографія. Стеганографія*** (англ. – *Stegonography*) – складова криптології, наука організації передачі інформації таким чином, що приховується сама наявність такої передачі.

Криптографічні методи (криптографічні алгоритми, алгоритми шифрування), тобто методи або алгоритми, згідно яким здійснюється криптографічне перетворення інформації, є найбільш потужним механізмом захисту інформації.

Сучасна криптографія застосовується для ***шифрування та дешифрування інформації*** – даних користувача, а також для розв’язання задач пов’язаних із забезпеченням захищеності систем захисту інформації, таких як ***автентифікація користувачів, контроль цілісності інформації, незаперечність причетності до авторства чи до одержання документа або повідомлення.*** Визначимо автентифікацію як процедуру перевірки належності учаснику процесу обміну інформацією ідентифікатора, який був їм

пред'явлений. Ідентифікатор – це послідовність латинських літер і цифр, яка починається з літери. Цілісність інформації – це властивість інформації, яке полягає в тому, що вона не може бути модифікована неавторизованим користувачем і/чи процесом.

Незаперечність причетності до авторства – це поняття, зворотне поняттю відмови від авторства, тобто заперечення причетності до утворення або передавання якого-небудь документа чи повідомлення. В свою чергу, незаперечність причетності до одержання документа, або повідомлення – поняття, зворотне поняттю відмови від причетності до утворення або передавання якого-небудь документа чи повідомлення.

Важливим поняттям криптографії є ***криптоаналітична атака*** (англ. – *cryptoanalytic attack*) – це загальна назва методу, яким криптоаналітик намагається зламати криптосистему. У залежності від якості та кількості інформації, якою володіє криптоаналітик, криптоаналітичні атаки поділяють на атаки лише із криптотекстом, атака з відомим відкритим текстом, атака з вибраним відкритим текстом, атака з вибраним криптотекстом, атака з вибраним ключем.

У криптографії використовують поняття ***стійкість криптографічних алгоритмів*** (англ. – *cipher strength*). Це поняття характеризує рівень стійкості криптоалгоритму до розшифрування, який визначається часом та обчислювальними ресурсами, необхідними для розшифрування. Розрізняють поняття абсолютної та практичної крипостійкості. ***Абсолютна стійкість криптоалгоритмів*** (англ. – *perfect secrecy*) за Шеноном означає статистичну незалежність відкритого та зашифрованого тексту і досягається лише тоді, якщо довжина ключа є не меншою від довжини відкритого тексту та ключ обирається з ключового простору дійсно випадково. ***Практична стійкість криптоалгоритмів*** (англ. – *computationally secure*) – це поняття стійкості алгоритмів, які не є ідеальні, тобто можуть бути дешифрованими за скінчений час.

В сучасній криптографії криптографічні методи не використовуються самостійно. Вони складають основу, базову частину більш загальної

криптографічної системи. ***Криптографічна система,*** **або** ***криптосистема*** (англ. – *cryptosystem*) – це сукупність програмних, апаратних, програмно-апаратних засобів, криптографічних алгоритмів або криптографічних схем, поєднаних в єдиній системі з метою розв'язання конкретної задачі захисту інформації.

Історія криптографії починалась із використання криптоалгоритмів, які користувачі мали тримати в таємниці. Розкриття цих алгоритмів третій стороні автоматично приводило до розкриття шифротексту. Такі криптоалгоритми з часом отримали назву тайнопису. ***Тайнопис*** (англ. – *cryptographic writing*) – це методи кодування, особливістю яких є обов'язкове збереження в таємниці криптографічного алгоритму від третьої сторони. Вони були обмеженими за функціональними можливостями і в сучасній криптографії не використовуються.

Наприкінці XIX сторіччя криптографія починає відмовлятися від тайнопису і переходити до криптоалгоритмів з ключем. Такі зміни пов'язують з ідеями французького математика Огюста Кергоффса, сформульованими в роботі "Військова криптографія", яка вийшла в світ у 1883 році. В цій роботі О.Кергоффс вперше відокремлює проблеми таємності криптоалгоритму и таємності ключа. Він пропонує використовувати криптоалгоритми, для яких пріоритетним є таємність ключа і не є важливою, власне, таємність криптоалгоритму.

Сучасна криптографія базується на криптоалгоритмах шифрування з ключем. ***Шифрування з ключем*** (англ. – *key coding*) – це методи кодування, особливістю яких є обов'язкове збереження ключа в таємниці від третьої сторони, збереження криптографічного алгоритму при цьому не обов'язково.

Криптоалгоритми шифрування з ключем

Серед криптоалгоритмів шифрування з ключем розрізняють дві великі групи таких криптоалгоритмів – ***симетричні та асиметричні***. ***Симетричне шифрування*** (англ. – *symmetric coding*) – це метод шифрування, у якому ключі зашифровування і розшифровування або однакові, або легко виводяться один з

одного, забезпечуючи таким чином спільний ключ. ***Асиметричне шифрування*** (англ. – *asymmetric coding*) – це група методів криптографічного шифрування, у яких використовуються два ключі – секретний (приватний) і відкритий, причому жоден із ключів не може бути обчислений з іншого за певний час. Інша назва методу – ***шифрування з відкритим ключем*** (англ. – *public key coding*).

Симетричне та асиметричне шифрування є домінуючими криптографічними методами на поточний час. Історія криптографії із симетричними криптоалгоритмами почалась наприкінці XIX сторіччя з виходом в світ роботи О. Кергоффса "Військова криптографія". Криптографія з асиметричними криптоалгоритмами значно молодше. Її початок пов'язують з роботами американських вчених В.Діффі і М.Хеллмана, які вийшли в світ у 70-х роках минулого сторіччя.

Симетричні та асиметричні криптоалгоритми мають переваги та недоліки. Симетричні криптоалгоритми в порівнянні з асиметричними мають більшу швидкодію та меншу довжину ключа. Асиметричні криптоалгоритми, в свою чергу, можуть застосовуватися у таких випадках організації криптосистем, де використання симетричних алгоритмів є неможливим. Порівняння характеристик цих криптоалгоритмів, в цілому, не є коректним, тому що вони створені для розв'язання різних завдань шифрування.

Сфери застосування асиметричних криптоалгоритмів шифрування

Асиметричні криптоалгоритми, як і симетричні, застосовуються для шифрування масивів даних, але їх швидкість значно поступається швидкості останніх. Основне призначення асиметричних криптоалгоритмів – забезпечення ефективного функціонування сучасних криптосистем. Ці криптоалгоритми складають основу задач автентифікації користувачів, контролю цілісності інформації, незаперечності причетності до авторства чи до одержання документа або повідомлення та інших.

Важливе практичне застосування асиметричних криптоалгоритмів – в основі підсистем електронно-цифрового підпису (ЕЦП) криптографічних систем. *Електронно-цифровий підпис* (англ. – *electronic digital signature*) – цифрова

послідовність, що додається до повідомлення (даних) для забезпечення цілісності та підтвердження авторства і формується із застосуванням асиметричних криптосистем. У електронно-цифровому підписі для шифрування повідомлень використовується закритий, а для розшифрування – відкритий ключ.

4.6. Захист комп'ютерних систем від вірусів та спаму

Класичні ***комп'ютерні віруси*** – це програмні засоби, які здатні самостійно відтворюватись, тобто розмножуватись, і які використовують в якості носія інший програмний код, який вони модифікують таким чином, щоби впровадити в нього свою копію. В результаті замість програмного коду, запущеного користувачем на виконання, починає виконуватись код вірусу.

Комп'ютерні віруси розрізняються між собою за такими ознаками:

- середовище існування – системні області комп'ютера, ОС, прикладні програми, у визначенні компоненти яких впроваджується код вірусу:
  - файлові;
  - завантажувальні (boot);
  - макро;
  - скриптові.
- спосіб зараження – різні методи впровадження вірусного коду в об'єкти, які він заражає.

В залежності від середовища існування віруси використовують різні способи зараження, тому універсальної класифікації за другою ознакою немає.

Віруси також класифікують (або надають їм додаткові ознаки) за тими технологіями, які віруси використовують для ускладнення їх виявлення і ліквідації. Деякі з них розглянемо в розділі, присвяченому захисту від вірусів.

Файлові віруси

Файлові віруси для свого розповсюдження використовують файлову систему. Найпоширеніший тип файлових вірусів використовує в якості носія виконувані

файли. За способом зараження з них виділяють так звані ***віруси, що перезаписують*** **(*overwriting*) і *паразитичні віруси* (*parasitic*)**. Перші з них заміняють собою оригінальний файл, знищуючи його, так що в результаті їх діяльності і прикладні програми, і ОС дуже швидко перестають функціонувати. Другі – значно більш витончені, вони модифікують оригінальний файл, зберігаючи його функціональність. Цей тип файлових вірусів є найпоширенішим, і його ми в подальшому розглянемо детальніше. Існують також так звані ***компаньйон-віруси***, які створюють файли-двійники, так звані *link-віруси*, які використовують особливості організації файлової системи.

Завантажувальні віруси

Завантажувальні, або бутові (англ. *boot* – початкове завантаження, специфічний комп'ютерний термін, скорочення від *bootstrap*), віруси активуються в момент завантаження системи. Для цього вони повинні розташувати частину свого коду в службових структурах носія, з якого відбувається завантаження – жорсткого диску або дискети. Зараження дискети здійснюється шляхом записування свого коду замість оригінального коду boot-сектора дискети. Зараження жорсткого диска – одним з трьох способів: вірус записує себе або замість коду MBR (Master Boot Record – системного завантажувача жорсткого диску), або замість коду boot-сектора завантажувального диска (у Windows – зазвичай диска C:), або модифікує адресу активного boot-сектора в таблиці розділів диска (Disk Partition Table), що знаходиться в MBR.

Завантаження з дискети вже давно стало великою екзотикою, тому що сучасні операційні системи вимагають більші об'єми носіїв для розміщення свого коду. Саме втрата актуальності дискети як носія для завантаження ОС стала причиною того, що бутові віруси в наш час втратили поширення.

На жорсткому диску бутові віруси можуть вельми спокійно існувати і завдавати величезної шкоди інформаційним ресурсам. Також вони можуть дуже ефективно протидіяти антивірусним засобам, оскільки фактично саме віруси стартують першими, ще до запуску операційної системи, і тому вони здатні

залишити за собою керування критичними для їх існування ресурсами комп'ютера, зокрема, файловою системою. З іншого боку, для цього потрібно фактично утворити для ОС віртуальну машину, що для сучасних систем хоча й є цілком можливим (адже для цього існують спеціальні програмні засоби, наприклад, vmware), але потребує великого обсягу програмного коду, що не дуже прийнятно для вірусу.

Макро-віруси

Макро-віруси – це віруси, які використовують програмний код, прихований в файлах документів – так звані макроси. Ідея макросів полягає в тому, що під час роботи з документами досить часто виникає необхідність багаторазово повторювати рутинні операції редагування, або виконання деяких процедур вимагає виконання певної, завжди однакової, послідовності дій. Цілком природно для виконання таких дій визначити процедуру, яка буде виконувати визначену послідовність операцій автоматично. В якості елементарних операцій в макросі мають бути припустимими окремі команди з множини тих команд, що передбачені в програмі обробки документа, або спеціально розроблені макро-команди. Свої макро-мови для автоматизації мають різні табличні і графічні редактори, системи проектування, текстові процесори.

Макро-віруси – це програми на макро-мовах. Передумовою появи макро-вірусів стали можливості, які з'явились в удосконалених системах, що використовують макроси: по-перше, можливість зберігання макросів в файлі документа, а по-друге – суттєве розширення функцій, доступних для макрокоманд.

Скриптові віруси

Програмний код може впроваджуватись і в інші види документів, наприклад, в HTML-сторінки, що завантажуються з мережі або локально і подаються на екрані програмою-браузером. При цьому також автоматично виконується програмний код сценаріїв ("скриптів" від англ. *script* – сценарій) або інших елементів (ActiveX, Java). Програмний код сценаріїв може існувати і окремо, в

спеціальних файлах. Деякі мови сценаріїв дуже розвинені, їх можна вважати повноцінними мовами програмування. Наприклад, в операційній системі UNIX/Linux сценарії в якості системних команд використовуються на рівних правах з бінарними виконуваними файлами, далеко не всі користувачі знають, що саме вони запускають – скомпільовану програму чи сценарій. Сценарії можуть мати встановлений атрибут SUID. Не дивно, що в їх середовищі також можуть існувати віруси.

Скриптові віруси розглядають як підгрупу файлових вірусів. Такі віруси можуть бути написаними на різних мовах сценаріїв (VBS, JS, BAT, PHP і т.д.). Вони можуть заражати інші програми-сценарії (командні і службові файли Windows або UNIX), можуть бути компонентами багатокомпонентних вірусів, можуть заражати файли інших форматів (як, наприклад, згаданий вище HTML), якщо в них можливе виконання сценаріїв.

Крім розглянутих нами, іноді в класифікаціях згадують "поштові віруси", які поширюються електронною поштою. В наш час переважна більшість небезпечних руйнівних програмних засобів дійсно надходить з мережі, в тому числі й електронною поштою. Однак практично всі такі засоби не є специфічними "поштовими вірусами". Як правило, це звичайні файлові віруси, якими заражені файли, що пересилаються поштою у вигляді вкладень. Ще частіше, такі руйнівні засоби – це типові "троянські коні". А в окремих випадках (такі випадки є найнебезпечнішими) – це мережеві хробаки.

Технології виявлення комп'ютерних вірусів

Основними ***технологіями виявлення вірусів*** (і інших шкідливих програмних засобів) є:

- пошук сигнатур;
- евристичний аналіз;
- контроль незмінності об'єктів.

Однією з основних технологій виявлення вірусів був і залишається пошук характерних ознак відомих вірусів (так званих ***сигнатур*)** у файлах і оперативній пам'яті комп'ютера. Деякий час великі надії покладали на так званий

“евристичний аналіз”, коли впровадження шкідливого коду визначалось (точніше, “підозрювалось”) за наявністю “підозрілих операцій” (як, наприклад, відкриття для модифікації виконуваних файлів, перехоплення переривань, тощо). Також деякі засоби контролювали *незмінність файлів*, здебільшого виконуваних, що гарантувало неможливість впровадження в них коду вірусу. Сучасні антивірусні засоби поєднують в собі всі ці можливості, причому для виявлення відомих вірусів (а також хробаків, “троянських коней” і інших небезпечних програмних засобів) найефективнішим залишається саме пошук їхніх сигнатур.

За режимом дії з-проміж антивірусних засобів виділяють:

- антивірусні сканери (АВС);
- антивірусні монітори (АВМ);
- антивірусні фільтри (АВФ).

Антивірусні сканери періодично або за запитом здійснюють повне сканування файлової системи комп’ютера або вибіркове сканування заданих файлів або каталогів. Обсяг файлової системи сучасних комп’ютерів і кількість сигнатур в базі сучасних антивірусних засобів такий, що повне сканування комп’ютера з рутинної операції перетворилось на авральну процедуру, яка на кілька годин паралізує будь-яку діяльність на комп’ютері. Тому, незважаючи на переконливі вимоги антивірусних засобів провести повне сканування файлової системи, на практиці таке сканування проводять дуже нечасто (є можливість проводити такі сканування вночі, але реально так роблять здебільшого в корпоративних мережах).

Антивірусні монітори працюють неперервно, але вони здійснюють лише вибіркову перевірку, і тому, як правило, не дуже сильно уповільнюють роботу комп’ютера. Обов’язково перевіряються всі файли, з якими проводяться будь-які операції (відкривання, зчитування, записування, переміщення файлу, запуск на виконання), а якщо таких операцій відбувається мало, іде повільне вибіркове сканування файлової системи. Слід зазначити, що в момент відкривання файлу, особливо великих файлів і архівів, перевірка займає помітний проміжок часу, так що антивірусний монітор дійсно помітно уповільнює деякі види операцій, а

саме: запуск великих програм, відкриття великих документів і, особливо, архівів, що містять документи, а також пакетні операції оброблення великої кількості файлів (наприклад, переміщення великого каталогу з документами WinWord).

Антивірусні фільтри призначені для роботи з потоками даних, головним чином – тими, що надходять з мережі. Вони ефективні для перевірки електронної пошти, повідомлень з каналів IRC, P2P-мереж і інших. Також вони ефективні проти так званих *безтілесних хробаків*, які не пов'язані з жодними файлами.

Віруси (а також хробаки і "троянські коні") із свого боку протидіють антивірусним засобам різними, часто досить вибагливими способами.

Головним засобом проти пошуку сигнатур став так званий поліморфізм – модифікація коду вірусу від одного екземпляру до іншого. Для реалізації поліморфізму, як правило, здійснюється зашифровування коду з використанням різних ключів, а першим компонентом вірусу, який отримує керування, є розшифрувальник.

Деякі віруси досить ефективно приховують себе від програм, які контролюють розмір файлів (наприклад, на системний запит видають невірну інформацію про довжину файла, дату його модифікації, тощо). Подібні технології отримали назву ***"стелс"*** (англ. – *stealth*).

Досить неприємною для антивірусних засобів є тенденція розсилати код вірусу упакованим в архів (антивірусні засоби для виявлення сигнатури повинні вміти розпаковувати всі необхідні формати архівів). Ще більшим утрудненням стало пакування вірусів у архіви, що захищені паролем (пароль надсилається окремо, наприклад, вірус – у приєднаному до електронного листа файлі, а пароль – в самому листі).

Також віруси можуть включати в себе механізми захисту від дослідження, протидії запуску в режимі налагодження, а також "логічні бомби", які спрацьовують при спробі видалення компонентів вірусу.

ТЕМА 5. ОСНОВНІ ПОНЯТТЯ ПРО КОМПЛЕКСНУ СИСТЕМУ ЗАХИСТУ ІНФОРМАЦІЇ (КСЗІ)

5.1. Базові визначення та основні поняття про комплексну систему захисту інформації (КСЗІ)

В НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» (підрозділ 4.1 - Терміни і визначення) надано наступне визначення комплексної системи захисту інформації. ***Комплексна система захисту інформації (КСЗІ)*** - сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС.

5.1.1. Вимоги до складу, технічні та організаційні передумови створення КСЗІ

Склад КСЗІ визначено у відносно новому документі НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі». Згідно з цім документом, до складу КСЗІ мають входити ***заходи та засоби, які реалізують способи, методи, механізми захисту інформації*** від:

- ***витоку технічними каналами***, до яких відносяться канали побічних електромагнітних випромінювань і наведень, акустоелектричні та інші канали;
- ***несанкціонованих дій та несанкціонованого доступу (НСД) 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;
- ***спеціального впливу на інформацію***, який може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту.

Для кожної конкретної ІТС склад, структура та вимоги до КСЗІ визначаються ***властивостями оброблюваної інформації, класом автоматизованої системи та умовами експлуатації ІТС***.

Створення комплексів технічного захисту інформації від витоку ***технічними каналами*** здійснюється, якщо в ІТС обробляється інформація, що становить ***державну таємницю***, або коли необхідність цього визначено власником інформації.

У випадках, визначених законодавством, роботи з проектування, розроблення, виготовлення, випробування, експлуатації ІТС мають виконуватись у комплексі із заходами, щодо забезпечення ***режиму секретності, протидії технічним розвідкам (ПДТР), а також з організаційними заходами щодо охорони інформації з обмеженим доступом, яка не є державною таємницею.***

Інженерно – технічну основу будь якої КСЗІ складає ***комплекс засобів захисту від несанкціонованого доступу (КЗЗ)***. Створення КЗЗ здійснюється в усіх ІТС, де обробляється інформація, що є власністю держави, належить до державної чи іншої таємниці або до окремих видів інформації, необхідність захисту якої визначено законодавством, а також в ІТС, де така необхідність визначена власником інформації.

Рішення щодо необхідності вжиття заходів захисту від ***спеціальних впливів на інформацію*** приймається власником інформації в кожному випадку окремо.

Роботи зі створення КСЗІ виконуються ***організацією-власником*** (розпорядником) ІТС ***з дотриманням вимог нормативно-правових актів щодо провадження господарської діяльності у сфері захисту інформації.***

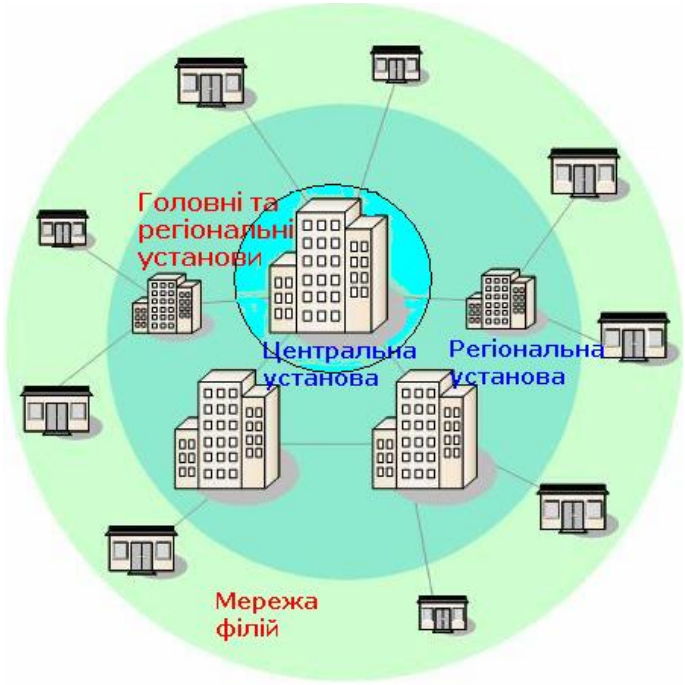
У залежності від складу КСЗІ може виявитись, що для її створення необхідно виконувати декілька різних видів робіт, які ***підлягають ліцензуванню*** в межах господарської діяльності з технічного захисту інформації. У цьому випадку розробник КСЗІ повинен мати право на провадження ***хоча б одного з таких видів робіт***. ***Для виконання робіт, на провадження яких розробник***

КСЗІ не має ліцензії, залучаються співвиконавці, які відповідні ліцензії мають.

Для організації робіт зі створення КСЗІ в ІТС створюється ***служба захисту інформації (СЗІ)***, порядок створення, завдання, функції, структура та повноваження якої визначено в НД 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі». СЗІ створюється після прийняття рішення про необхідність створення КСЗІ. Як виняток СЗІ може створюватися на більш пізніх етапах робіт, але не пізніше етапу підготовки КСЗІ до введення в дію.

5.1.2. Характеристика інформаційної системи, як об'єкту захисту КСЗІ

Сучасні інформаційні системи різного призначення, розміру, форми власності можуть мати спільні риси і, навидь, схожу структуру. Наведемо приклад організації (компанії) з позиції обробки інформації (наприклад, страхової компанії, виробничого об'єднання, органа державної влади, тощо) (рис). Інформація такої організації обробляється з використанням інформаційно-комунікаційної системи, приклад структурної схеми якої наведемо на наступному рисунки.



Центральна установа забезпечує накопичення та аналітичну обробку інформації, централізовану підтримку служб, а також реалізацію стратегій масштабу організації

Регіональні установа

Рис. Приклад організації (компанії) з позиції обробки інформації

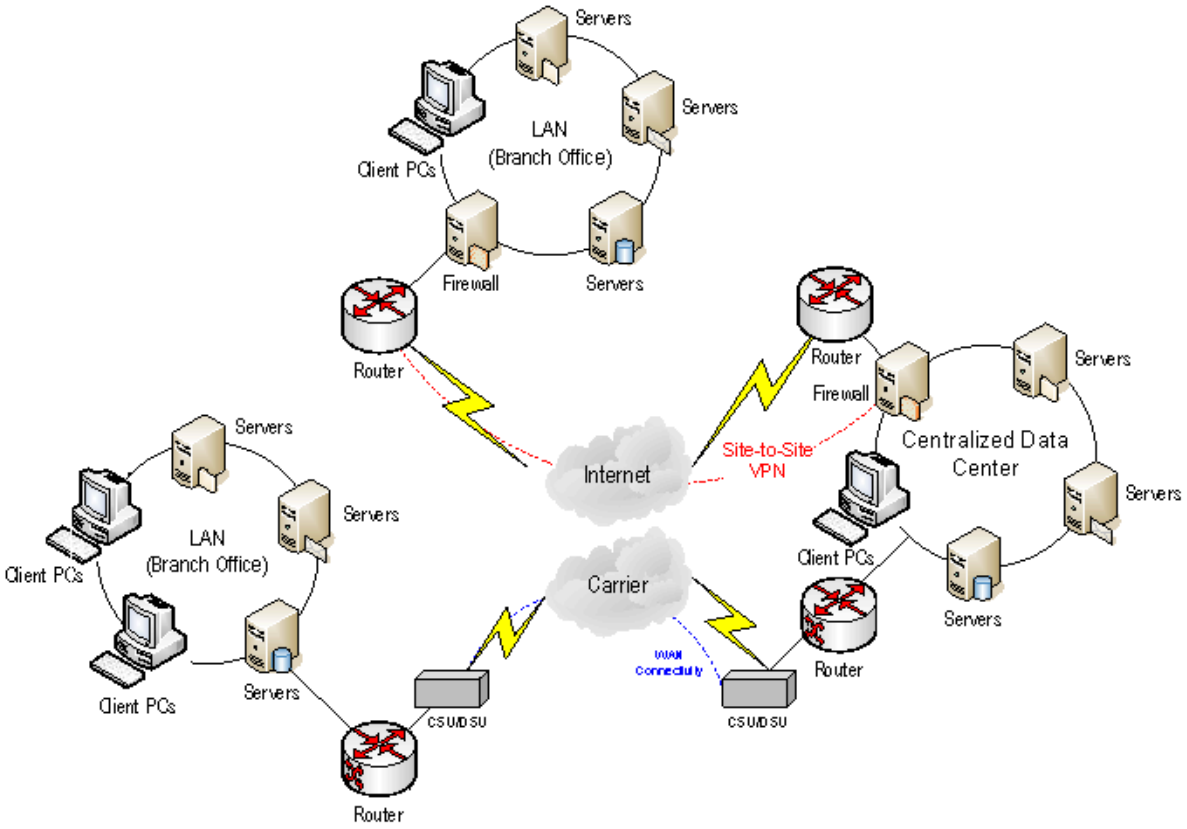


Рис. Структурна схема ІКС

При детальному порівнянні різних систем можна виділити спільні риси. В будь-якій ІКС можна виділити типові рівні, на яких вирішуються задачі, спільні для всіх систем. Як правило, виділяють 4 рівня (рис. 2.1).

Рис. Типові рівні ІКС

Розглянемо типові рівні ІКС знизу вверх:

- ***Рівень мережі*** – відповідає за взаємодію вузлів ІКС. Елементами ІКС, що відносяться до цього рівня, є модулі, які реалізують стеки протоколів мережевої взаємодії, наприклад, TCP/IP. Також на цьому рівні функціонує специфічна апаратура – мережеве обладнання.

- ***Рівень операційних систем*** (ОС) – відповідає за обслуговування програмного забезпечення, яке реалізує більш високі рівні, і його взаємодію з обладнанням. В якості типових елементів цього рівня можна назвати такі поширені ОС, як Microsoft Windows, Sun Solaris, Linux.
- ***Рівень систем керування базами даних*** (СКБД) – відповідає за зберігання та обробку даних. В якості типових елементів цього рівня можна назвати СКБД Oracle і MS SQL Server. Іноді СКБД є центральним елементом ІС (наприклад, облік товарів на складі), а іноді СКБД функціонує прозоро для користувачів і виконує допоміжні функції, зокрема для зберігання технологічної інформації самої ІС. Так, наприклад, система підтримки конфіденційного документообігу OPTiMA WorkFlow базується на СКБД MS SQL Server.
- ***Рівень прикладного ПЗ*** (застосувань) - найвищий рівень. Розрізняють прикладний компонент і компонент подання (рос. – *представления*), які є складовими прикладного рівня. Прикладний компонент забезпечує виконання специфічних функцій ІС. Компонент подання відповідає за взаємодію з користувачем і подання даних у необхідній формі. На рівні прикладного ПЗ функціонують, наприклад, офісні застосування, такі як популярні Microsoft Office, Star Office або Open Office, бухгалтерські програми, спеціально розроблені для кожної окремої ІС програмні засоби, що реалізують специфічні для неї функції, і будь-які інші прикладні програми.

Кожному рівню ІКС притомні типові вразливості.

5.1.3. Типові вразливості ІКС на різних рівнях

Несанкціонований доступ на рівні мережі. Рівень мережі – потенційно може надати доступ користувачеві, який не лише не має повноважень у системі, але й знаходиться поза її межами. На цьому рівні можлива атака на дані, які передаються у мережі, а також вплив через мережеві засоби на вузли системи – сервери і робочі станції, внаслідок чого можуть бути створені передумови для

доступу на більш високих рівнях, наприклад, створений обліковий запис користувача-порушника з правами адміністратора.

Несанкціонований доступ на рівні ОС. Порушник може спробувати здійснити доступ на рівні ОС. Зокрема, такий доступ може полягати у несанкціонованому копіюванні файлів бази даних засобами файлової системи сервера.

Несанкціонований доступ на рівні СКБД. Інший шлях – доступ на рівні СКБД. Такий доступ порушник здійснює в обхід прикладного ПЗ безпосередньо до бази даних. Для цього він може згенерувати специфічний SQL-запит або скористатись засобами самої СКБД для перегляду таблиць даних.

Вразливості на рівні прикладного ПЗ. Порушник може спробувати здійснити доступ до захищених даних на рівні прикладного ПЗ. Наприклад, для цього він може спробувати підібрати пароль іншого користувача, якому доступ до цієї інформації дозволений. Або отримати доступ з правами адміністратора і змінити права доступу до захищених об’єктів чи свої повноваження. Нарешті, він може спробувати знайти вразливість у прикладному ПЗ або використати відому вразливість. Як правило, для цього він має створити якийсь специфічний запит, не передбачений розробниками ПЗ (у найпростішому випадку включити у текстовий рядок спеціальні керуючі символи, або ввести числові значення, що виходить за межі дозволеного діапазону), у відповідь на який система може надати порушнику несанкціонований доступ.

5.2. Порядок створення, введення в дію, атестації та супроводження КСЗІ

Порядок створення КСЗІ визначено у трьох анонсованих вище документах: «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі НД ТЗІ 3.7-001-99», НД 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі», НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі».

В останньому нормативному документі (НД ТЗІ 3.7-003-05) надано детальний опис етапів процесу побудови КСЗІ кий наочно демонструє як склад так порядок дій розробників по створенню КСЗІ. Розрізняють шість етапів побудови КСЗІ:

1. Формування вимог до КСЗІ;
2. Розробка політики безпеки;
3. Розробка технічного завдання на створення КСЗІ;
4. Розробка проекту КСЗІ;
5. Введення КСЗІ в дію;
6. Супроводження КСЗІ.

Етапи та їх склад наведено на наступному рисунку.

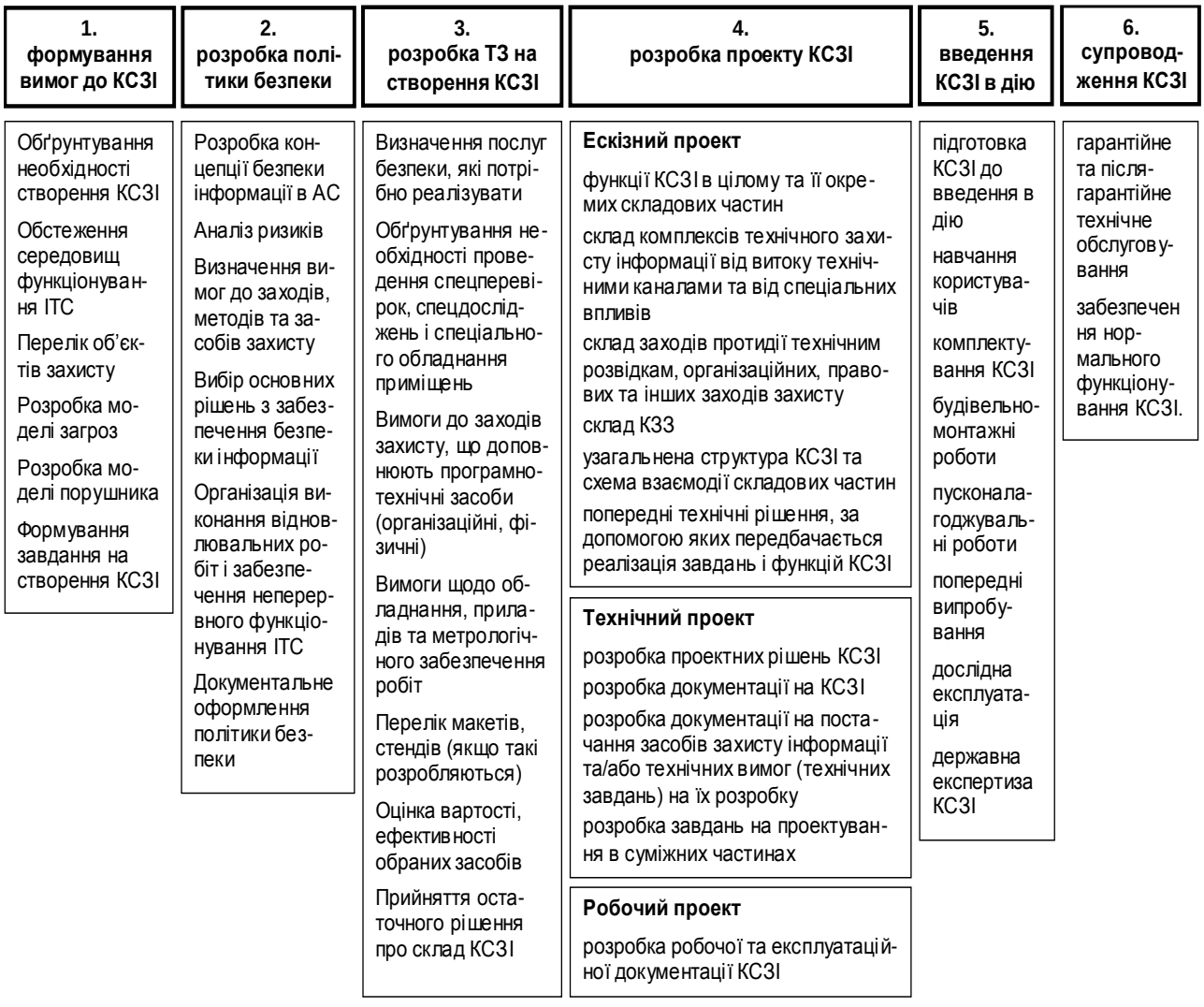


Рис. Основні етапи та зміст робіт по побудові КСЗІ

1. На першому етапі формування вимог до КСЗІ виконуються наступні завдання:

1.1. Обґрунтування необхідності створення КСЗІ. При цьому обов'язково аналізуються нормативно-правові акти, на підставі яких може встановлюватися обмеження доступу до певних видів інформації, або, навпаки, заборона такого обмеження;

1.2. Обстеження середовищ функціонування ІТС. Обстеженню підлягають: обчислювальна система; фізичне середовище; середовище користувачів; інформація, що обробляється, та технологія її обробки.

Процес обстеження призваний виявити у середовищах ті їхні складові та їхні поєднання, які прямо чи непрямо впливають на безпеку інформації. На основі цих даних затверджується перелік об'єктів захисту, потенційних загроз інформації, а також ***розробляється модель загроз та модель порушника***;

В НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» (підрозділ 4.3 Створення і експлуатація захищених систем) надано наступне визначення модель загроз та модель порушника. ***Модель загроз*** (model of threats) - абстрактний формалізований або неформалізований опис методів і засобів здійснення загроз. ***Модель порушника*** (user violator model) - абстрактний формалізований або неформалізований опис порушника.

1.3. Формування завдання на створення КСЗІ. При цьому:

- Мають бути визначені: завдання захисту інформації в інформаційній системі; мета створення КСЗІ; рішення задач захисту відповідно до ДСТУ 3396.1; напрями забезпечення захисту;
- Здійснюється ***аналіз ризиків*** – вивчаються можливі загрози, ймовірність їхнього здійснення та величина фінансових втрат в разі їх потенційної реалізації;
- Визначається перелік умов, обмежень, в узгодженні з якими має створюватись КСЗІ.

В НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» (підрозділ 4.3 Створення і експлуатація захищених систем) надано наступне визначення ***аналізу ризиків*** та пов'язаних з ним термінів ризику, керування ризиком та залишкового ризику. ***Ризик*** (risk) - функція ймовірності реалізації певної загрози, виду і величини завданих збитків. ***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. ***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. ***Залишковий ризик*** (residual risk) - ризик, що залишається після впровадження заходів забезпечення безпеки.

2. На другому етапі створення КСЗІ розробляється політика безпеки інформації в ІКС. В НД ТЗІ 1.1-003-99 (підрозділ 4.1 - Терміни і визначення) надано наступне визначення політики безпеки інформації - ***Політика безпеки інформації*** (information security policy) - сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок обробки інформації.

Методологія розроблення політики безпеки включає в себе наступні роботи:

- розробка концепції безпеки інформації в ІТС;
- аналіз ризиків;
- визначення вимог до заходів, методів та засобів захисту;
- вибір основних рішень з забезпечення безпеки інформації;
- організація виконання відновлювальних робіт і забезпечення неперервного функціонування ІТС;
- документальне оформлення політики безпеки.

Детальні рекомендації з розробки політики безпеки наведені в **НД ТЗІ 1.4-001-2000** «Типове положення про службу захисту інформації в автоматизованій системі».

3. На третьому етапі створення КСЗІ розробляється технічне завдання на створення КСЗІ.

Технічне завдання (ТЗ) на створення КСЗІ – організаційно-технічний документ, що має виняткове значення у процедурі розробки і впровадження КСЗІ. Порядок розробки ТЗ на створення КСЗІ, його зміст, порядок погодження та затвердження регламентуються **НД ТЗІ 3.7-001-99.** ТЗ на створення КСЗІ погоджується ДССЗЗІ України

4. На четвертому етапі створення КСЗІ здійснюється розробка проекту КСЗІ.

Проект розробляється на підставі ТЗ і має відповідати вимогам цього ТЗ. Виділяють наступні стадії проекту: ***ескізний; технічний; робочий***.

На етапі ***ескізного проектування*** КСЗІ визначаються: функції КСЗІ в цілому та її окремих складових частин; склад комплексів технічного захисту інформації від витоку технічними каналами та від спеціальних впливів; склад заходів протидії технічним розвідкам, організаційних, правових та інших заходів захисту; склад КЗЗ; узагальнена структура КСЗІ та схема взаємодії складових частин; попередні технічні рішення, за допомогою яких передбачається реалізація завдань і функцій КСЗІ.

На етапі ***технічний проектування*** КСЗІ виконується: розробка проектних рішень КСЗІ; розробка документації на КСЗІ; розробка документації на постачання засобів захисту інформації та/або технічних вимог (технічних завдань) на їх розробку; розробка завдань на проектування в суміжних частинах.

На етапі ***робочого проектування*** КСЗІ виконується розробка робочої та експлуатаційної документації КСЗІ.

Стадія ескізного проекту може бути вилучена, а технічний та робочий етапи проекту можуть бути поєднані у єдиний етап техноробочого проекту.

5. На п'ятому етапі створення КСЗІ здійснюється введення КСЗІ в дію.

При цьому мають виконуватися таки роботи:

5.1. Підготовка наступних організаційних заходів захисту інформації: навчання користувачів; забезпечення готовності функціонування організаційно-

адміністративних заходів: перепускних режимів, порядку доступу до інформаційної системи та ін.; розробка документів, які регламентують діяльність по забезпеченню захисту інформації в інформаційній системі.

5.2. Комплектація КСЗІ;

5.3. Будівельно-монтажні роботи (якщо такі передбачені);

5.4. Інсталяція та налагодження комплексу засобів захисту;

5.5. Перевірка працездатності укомплектованої системи;

5.6. Попередні випробування КСЗІ;

5.6. Попередні випробування КСЗІ; При цьому: попередні випробування здійснюються за програмою та методиками випробувань, які має підготувати розробник КСЗІ; програми та методики випробувань узгоджуються замовником; головує випробуваннями спеціально створена комісія, голова якої є представником замовника; результати попередніх випробувань заносяться до протоколу, у якому надається висновок щодо готовності КСЗІ до дослідної експлуатації; Акт про прийняття КСЗІ до дослідної експлуатації оформлюється після усунення виявлених недоліків.

5.7. Дослідна експлуатація КСЗІ. Дослідна експлуатація дає змогу користувачам та СЗІ набути навичок роботи по використанню засобів КСЗІ. При наявності недоліків чи зауважень з боку замовника – розробник під час дослідної експлуатації усуває їх, здійснює конфігурування, налагодження, та коригує за необхідності робочу та експлуатаційну документацію. За результатами дослідної експлуатації робиться висновок щодо можливості (неможливості) представлення КСЗІ на державну експертизу.

5.8. Державна експертиза КСЗІ. В ході державної експертизи визначається відповідність КСЗІ технічному завданню, вимогам нормативних документів із захисту інформації, та визначається можливість введення КСЗІ в складі ІТС в експлуатацію. Державна експертиза КСЗІ в ІТС проводиться згідно з Положенням про державну експертизу в сфері технічного захисту інформації.

У роботах з державної експертизи КСЗІ беруть участь: ДССЗЗІ України; замовник; організатор експертизи; розробник. Визначено наступну послідовність робіт з експертизи КСЗІ:

- Передача замовником необхідних документів на КСЗІ організатору експертизи;
- Розробка програми та методик випробувань;
- Узгодження програми випробувань замовником;
- Узгодження програми та методик випробувань ДССЗЗІ України;
- Проведення випробувань;
- Оформлення результатів випробувань, передача в ДССЗЗІ проекту експертного висновку;
- Розгляд на експертній раді ДССЗЗІ результатів експертизи та проекту експертного висновку;
- Видача замовнику ***Атестата відповідності КСЗІ***;
- Передача ІТС у промислову експлуатацію.

6. На шостому етапі здійснюється супроводження КСЗІ. *Еman супроводження КСЗІ передбачає:*

- Гарантійне та післягарантійне технічне обслуговування;
- Забезпечення нормального функціонування КСЗІ.

Супроводження КСЗІ здійснює ***Служба захисту інформації (СЗІ).*** Зазвичай така служба формується із числа штатних співробітників організації-замовника, для інформаційних потреб якої будується система захисту. СЗІ рекомендується створювати на першому етапі створення КСЗІ, але не пізніше, ніж на початку етапу введення КСЗІ в дію. Порядок створення, завдання, функції, структура та повноваження СЗІ визначені в **НД ТЗІ 1.4-001-2000.**