УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ

Модуль 1. Теорія управління інформаційною безпекою

Лекція 1. Основні поняття інформаційної безпеки. Стандарти управління інформаційною безпекою

1. Поняття ІБ та кібербезпеки.
2. Поняття кіберінцидента/кібератаки.
3. Управління та політики кібербезпеки.
4. Нормативно-правова база України у сфері управління кібербезпекою.
5. Міжнародна стандартизація.

Поняття ІБ та кібербезпеки

Інформаційна безпека – стан (рівень) захищеності інформаційних ресурсів – інформаційних об'єктів та інформаційних систем – від негативних дій, які можуть завдати збитку самій інформації і засобам її передачі та обробки, а отже негативно відбитися на власниках інформаційних ресурсів, державі, суспільстві і інших учасниках процесів інформаційного обміну.

Інформаційна безпека – стан захищеності інформаційного середовища суспільства, що забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави.


Ціль забезпечення ІБ досягнута, якщо:
Інформація доступна тоді, коли це потрібно, а інформаційні системи стійкі до атак, можуть уникати їх або швидко відновлюватись
Інформація доступна тільки тим, хто має відповідні права
Інформація коректна, повна і захищена від неавторизованих змін
Обмін інформацією з партнерами та іншими організаціями надійно захищений

Основні складові ІБ та загрози

Складові інформаційної безпеки

Конфіденційність	Стан інформації, при якому доступ до неї здійснюють тільки суб’єкти, що мають на це право.
Цілісність	Стан інформації, при якому відстутні будь-які її зміни або зміни здійснюються тільки умисно суб’єктами, що мають на це право.
Доступність	Стан інформації, при якому суб’єкти, що мають право доступу, можуть безперешкодно його реалізувати.

Головні **загрози**, які можуть спричинити порушення цих категорій, а також негативно вплинути на компоненти ІС, призвівши навіть до їх втрати, знищення чи збою функціонування, такі: розголошення інформації, її витік або несанкціонований доступ до такої інформації

Розголошення	Витік	Несанкціонований доступ
• Навмисні або випадкові дії співробітників, що рпизвели до ознайомлення з конфіденційною інформацією осіб, які не мають до неї доступу • Реалізується через передачу, надання та пересилання повідомлень каналами їх поширення	• Безконтрольне виведення конфіденційної інформації за межі організації або кола осіб, яким її було довірено • Реалізується через візуально-оптичні, акустичні, електромагнітні, матеріальні та інші канали	• Протиправне ознайомлення з конфіденційною інформацією кола осіб за межами організації або осіб, які не мають до неї доступу. Порушення цілісності і доступності інформації • Реалізується способами співробітництва, підслуховування, спостерігання, викрадення, копіювання...

Під час побудови системи захисту інформаційних активів підприємства важливим є визначення та систематизація загроз, що діють на них. **Створення ефективної системи захисту інформації** на підприємстві є важливий та трудомісткий процес, що складається з наступних **етапів**:

– визначення меж огляду;
– ідентифікація активів та установлення залежності між ними;
– оцінювання активів та установлення залежності між ними;
– оцінювання загроз;
– оцінювання вразливостей;
– ідентифікація наявних і (або) запланованих засобів захисту;
– оцінювання ризиків;
– вибір засобів захисту.

Виявлення загроз – це дії з визначення конкретних загроз та їхніх джерел, які завдають той або інший вид збитку. До таких дій можна віднести виявлення фактів розкрадання або шахрайства, а також фактів розголошення конфіденційної інформації або випадків несанкціонованого доступу до джерел комерційних секретів.

Припинення або **локалізація загроз** – це дії, спрямовані на усунення діючої загрози і конкретних злочинних вчинків. Ліквідація наслідків має на меті відновлення стану, що передував настанню загрози.

Конкретне підприємство буде мати і специфічні загрози, характерні для його середовища і характеру діяльності.

Після визначення меж огляду, інвентаризації та проведення оцінки активів важливим є визначення загроз, які можуть діяти на інформаційну систему підприємства. Потенційно можливий несприятливий вплив, що приводить до зниження цінності ресурсів підприємства, називається **загрозою**.

У випадку реалізації загрози цінність інформаційного ресурсу підприємства може знизитись внаслідок порушення цілісності, конфіденційності та доступності інформації. Всі загрози повинні бути *визначені*, а ймовірність їх прояву *оцінена*.

Оцінку вартості повинні проводити *власники інформаційних активів*. Але в більшості випадків вони не здатні визначити перелік усіх загроз, які можуть впливати на їхні ресурси. Тому перелік загроз інформаційним активам в організації, потрібно скласти із залученням *спеціалістів у сфері інформаційної безпеки*, а також керівників та їх власників. У зв'язку з постійною модифікацією та удосконаленням загроз такий перелік потрібно періодично переглядати та вносити до нього зміни.

Загрози
(за природою походження)

Об'єктивні

(виникають незалежно від прямої діяльності людини і пов'язані з різними стихійними природними явищами)

Суб'єктивні

(виникнення залежить від діяльності людини)

Навмисні

(пов'язані з діями людини, спрямованими на отримання певної вигоди)

Випадкові

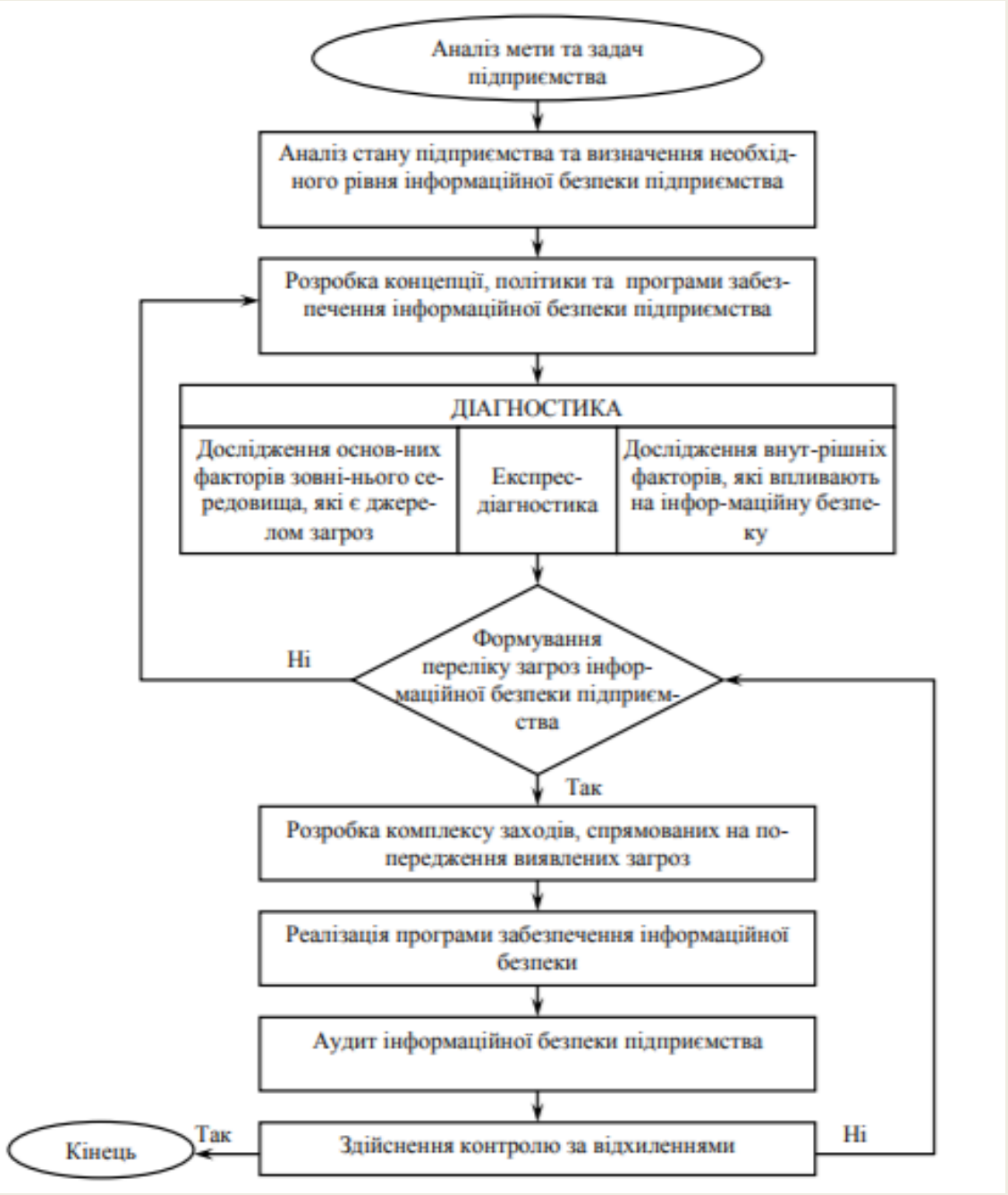
(пов'язані з помилками людини, її недбалістю, проектно-технологічними недоліками в програмному та апаратн. забезпеченні тощо)

Таблиця 1.1. Перелік можливих загроз

№ пп	Загроза	Суб'єктивна		Об'єктивна
		навмисна	випадкова	
1	2	3	4	5
1	Землетрус			+
2	Повінь	+	+	+
3	Буревій			+
4	Блискавка			+
5	Промисловий вплив	+		+
6	Бомбова атака	+		+
7	Використання зброї	+		+
8	Вогонь	+		+
9	Навмисне пошкодження	+		
10	Несправність електроживлення		+	
11	Несправність водопостачання		+	
12	Несправність кондиціювання повітря	+	+	
13	Відмова апаратури		+	
14	Нестабільність живлення		+	+
15	Екстремальні значення температури і вологості	+	+	+
16	Пил			+
17	Електромагнітне випромінювання	+	+	+
18	Електростатичний заряд			+
19	Злодійство	+		
20	Неуповноважене використання носіїв даних	+		
21	Погіршення носіїв даних			+
22	Помилка оперативного персоналу	+	+	
23	Помилка обслуговуючого персоналу	+	+	
24	Програмний збій	+	+	
25	Використання програмного забезпечення неуповноваженими користувачами	+	+	
26	Використання програмного забезпечення не уповноваженим способом	+	+	
27	Невідповідність ідентифікатора користувача	+		
28	Незаконне використання програмного забезпечення	+	+	
29	Зловмисна програмна закладка	+	+	
30	Незаконний імпорт або експорт програмного забезпечення	+		
31	Помилка оператора	+	+	
32	Помилка супроводу	+	+	
33	Доступ до мережі не уповноваженими користувачами	+		
34	Використання мережних засобів не уповноваженим способом	+		
35	Технічна несправність мережних компонентів		+	
36	Помилка під час пересилання інформації		+	
37	Пошкодження ліній зв'язку	+	+	
38	Перевантаження трафіка	+	+	
39	Підслуховування	+		
40	Просочування даних під час зв'язку	+		
41	Неуповноважений аналіз потоків інформації	+		
42	Неправильна маршрутизація повідомлень		+	
43	Зміна маршруту повідомлень	+		
44	Збій послуг зв'язку	+	+	
45	Недоліки, які допускає персонал в роботі		+	
46	Помилки користувача	+	+	
47	Неправильне застосування ресурсів	+	+	

Після визначення складових інформаційної безпеки, а також визначення джерел загроз інформаційної безпеки та методів і засобів захисту конфіденційної інформації на підприємстві слід розробити *алгоритм створення системи забезпечення інформаційної безпеки підприємства*, який може бути показаний наступною послідовністю дій.

Запропонований алгоритм не прив'язаний до конкретних завдань та проблем, що стоять перед підприємством, тому він має універсальний характер і може використовуватися на усіх підприємствах галузі зв'язку.



Алгоритм створення системи забезпечення ІБ підприємства

1. Аналізується мета та задачі підприємства.
2. Аналізується стан підприємства та визначається необхідний рівень інформаційної безпеки підприємства. На основі цієї інформації оцінюються критерії інформаційної безпеки, їхні відхилення від порогових значень, аналізуються причини виникнення відхилень.
3. Розробляється концепція, політика та програми забезпечення інформаційної безпеки підприємства.
4. Проводиться діагностика підприємства. Аналізуються основні фактори зовнішнього середовища, які є джерелом загроз, та внутрішні фактори, які впливають на інформаційну безпеку.
5. Формулюється перелік загроз інформаційної безпеки підприємства. Якщо цей перелік сформульований, то переходимо до розробки комплексу заходів, спрямованих на попередження виявлених загроз. Якщо цей перелік важко сформулювати, повертаємось до аналіз стану підприємства та визначення необхідного рівня інформаційної безпеки підприємства.
6. Розробляється комплекс заходів, спрямованих на попередження виявлених загроз або зниження витрат у випадку їхньої реалізації, у тому числі й заходів щодо локалізації загроз та ліквідації їхніх наслідків.
7. Реалізується програма забезпечення інформаційної безпеки.
8. Проводиться аудит інформаційної безпеки підприємства.
9. Здійснюється контроль по відхиленнях після проведення аудиту.

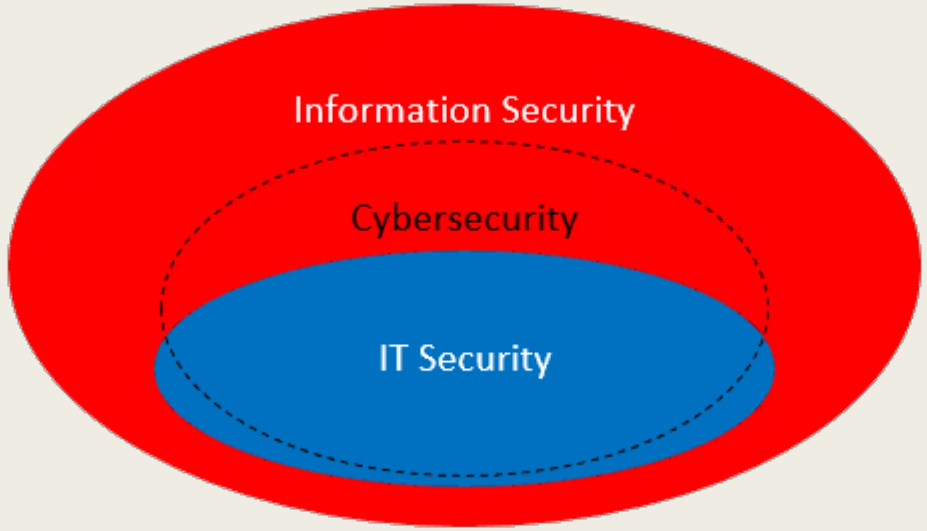
Безпека ІТ (комп’ютерна безпека, цифрова безпека, ІТ-безпека) – це захист від хакерів, вірусів, спаму, фішингу та безлічі інших загроз, що виникають, головним чином, з Інтернету. Цей захист найчастіше реалізується зниженням тих чи інших організаційних або технічних вразливостей безпеки.

Безпека ІТ – це забезпечення цілісності, доступності, конфіденційності та інших вимог безпеки, що пред’являються до обчислювальної та комунікаційної техніки та інформації, яку вона зберігає, обробляє та передає.

Кібербезпека – стан захищеності кіберпростору держави в цілому або окремих обєктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і/або національним інтересам

Кібербезпека включає в себе захист інформації, але не обмежується цим. Це захист від вірусів, хакерських атак, підробки даних, які можуть не тільки видалити/вкрасти, але і вплинути на роботу і продуктивність співробітників.

Ближче всього до поняття «кібербезпеки» знаходиться поняття системи управління інформаційною безпекою, тобто це набір процесів та засобів управління безпекою організації.



Взаємозв’язок понять «ІБ» та «кібербезпека»

Кіберпростір — це середовище існування, що виникло в результаті взаємодії людей, програмного забезпечення і послуг в інтернеті за допомогою технологічних пристроїв і мереж, під'єднаних до них, якого не існує в будь-якій фізичній формі.

Дійові особи кіберпростору та їх вплив на інформаційну і кібербезпеку	Легальні користувачі (негативно не впливають)
	Хакери, що не мають власних намірів(впливають негативно лише для власного самозадоволення та самовираження)
	Хакери, що мають корисливі цілі (впливають негативно, керуючись намірами щодо помсти або заради корисливих інтересів)
	Мережні комбатанти (впливають опосередковано, маючи на меті досягнення власних цілей)
	Кіберзлочинці (впливають негативно, намагаючись досягти суто злочинних цілей)
	Кібертерористи (впливають негативно, намагаючись досягти суто терористичних цілей)
	Підрозділи державних та недержавних структур, що здійснюють інформаційні операції (впливають, намагаючись досягти суто воєнно-політичних цілей)
	Кібервійська (впливають комплексно)

Поняття кіберінцидента/кібератаки

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

Хакерська атака (кібератака) – спроба реалізації загрози. Тобто, це дії кібер-зловмисників (хакерів) або шкідливих програм, які спрямовані на захоплення інформаційних даних віддаленого комп'ютера, отримання повного контролю над ресурсами комп'ютера або на виведення системи з ладу.

Під **атакою** (англ. attack, англ. intrusion) **на інформаційну систему** розуміють дії (процеси) або послідовність зв'язаних між собою дій порушника, які приводять до реалізації загроз інформаційним ресурсам шляхом використання уразливостей цієї інформаційної системи.

Стратегія по захисту підприємства від кіберінцидентів

Типи атак на інформаційні системи:

Віддалене проникнення (remote penetration)	Локальне проникнення (local penetration)	Атака на відмову в обслуговуванні(DoS, DDoS)
Мережні сканери (network scanners)	Сканери уразливостей (vulnerability scanners)	Зламувачі паролів (password crackers)
Аналізатори протоколів (sniffers)	Спам e-mail (Mailbombing)	Перехоплення каналу зв’язку (Man-in-the-Middle)

Управління ІБ. Система управління інформаційною безпекою

Управління інформаційною безпекою (Information Security Management, ISM) – процес, який забезпечує конфіденційність, цілісність і доступність активів, інформації, даних та послуг організації.

Основна мета ISM – забезпечення ефективного управління інформаційною безпекою всіх послуг і діяльностей. ІБ призначена для захисту від порушення конфіденційності, доступності і цілісності інформації, інформаційних систем і комунікацій.

Управління інформаційною безпекою є невід'ємним елементом управління підприємством і дозволяє колективно використовувати конфіденційну інформацію, забезпечуючи при цьому її захист, а також захист обчислювальних ресурсів.

Управління інформаційною безпекою – це циклічний процес, що включає:	Усвідомлення ступеня необхідності захисту інформації
	Збір та аналіз даних про стан інформаційної безпеки в організації
	Оцінку інформаційних ризиків
	Планування заходів з обробки ризиків
	Реалізацію і впровадження відповідних механізмів контролю
	Розподіл ролей і відповідальностей
	Навчання та мотивацію персоналу
	Оперативну роботу по здійсненню захисних заходів
	Моніторинг функціонування механізмів контролю
	Оцінку їх ефективності та відповідні коригуючі дії

Для забезпечення необхідного рівня ІБ на підприємстві створюється комплексна **система управління інформаційною безпекою (СУІБ).** Кінцевою метою створення такої системи є попередження або мінімізація збитків, умисно нанесених зловмисниками або ненавмисно – працівниками підприємства шляхом небажаної взаємодії на інформацію, її носії і процеси обробки.

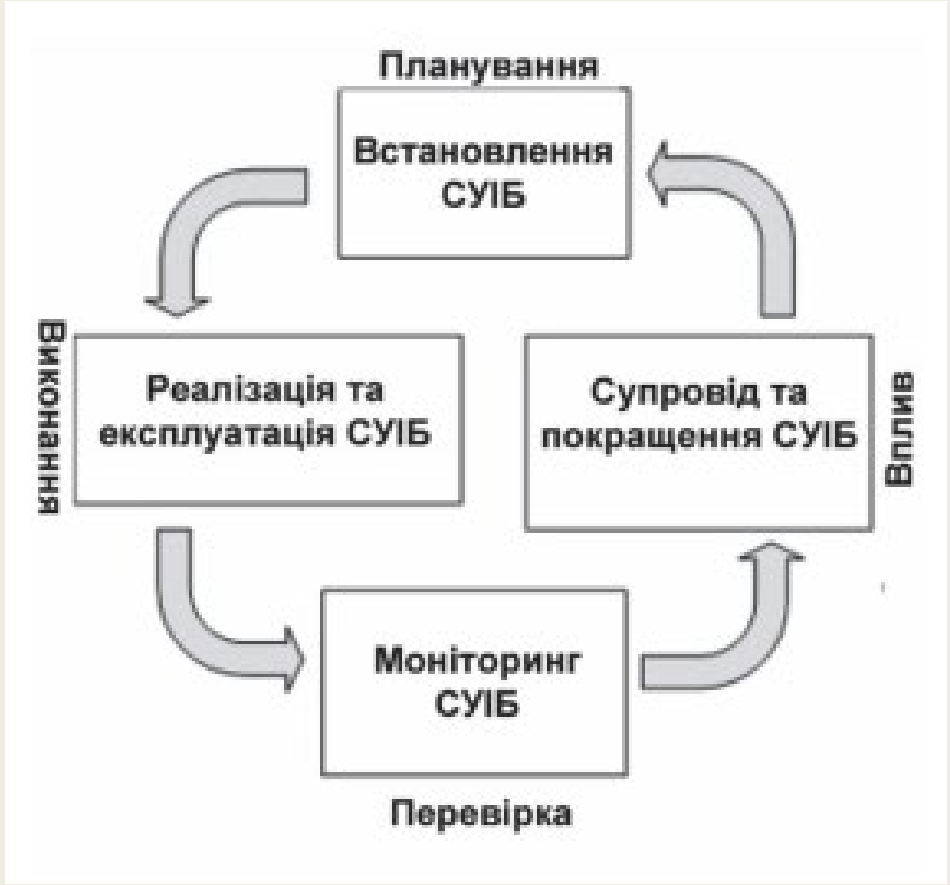
Згідно з ISO 27001, **система управління інформаційною безпекою** — це «та частина загальної системи управління організації, заснованої на оцінці бізнес ризиків, яка створює, реалізує, експлуатує, здійснює моніторинг, перегляд, супровід і вдосконалення інформаційної безпеки».

Система управління містить структуру організації, політики, планування, посадові обов'язки, практики, процедури, процеси і ресурси. Створення та експлуатація СУІБ вимагає застосування такого ж підходу, як і будь-яка інша система управління.

Використовувана в ISO 27001 для опису СУІБ процесна модель передбачає безперервний цикл заходів PDCA (Plan-Do-Check-Act): планування, виконання, перевірка, вплив (управління, коригування), відомий як цикл Шухарта-Демінга.

Опис циклу PDCA для впровадження СУІБ

PDCA	Опис
Планування	Розроблення політики безпеки, визначення мети, процесів та процедур, пов'язаних з управлінням ризиками та підвищенням інформаційної безпеки для досягнення результатів відповідно до загальної політики та цілей організації
Виконання	Впровадження та використання політики безпеки, елементів керування, процесів та процедур, механізмів контролю
Перевірка	Оцінювання та вимірювання ефективності роботи відповідно до політики безпеки, цілей та практичного досвіду, а також підготовка звіту про результати для керівництва з метою подальшого аналізу й аудиту
Вплив (управління, коригування)	Застосування коригувальних та профілактичних заходів з метою досягнення постійного вдосконалення СУІБ на основі результатів аналізу; перегляд політики безпеки; підвищення поінформованості персоналу



Модель PDCA для впровадження СУІБ

Управління

Управління IT-безпекою

- визначає, хто уповноважений ухвалювати рішення щодо кіберризиків в організації;
- визначає відповідальність і забезпечує нагляд, щоб гарантувати, що будь-які ризики належним чином знижуються, а стратегії безпеки узгоджуються з бізнес-цілями організації та відповідають правилам.

Управління інформаційною безпекою

- визначає та реалізує засоби контролю, які організація повинна мати для зменшення ризиків.

Управління даними

- визначає, хто уповноважений приймати рішення щодо даних в організації.

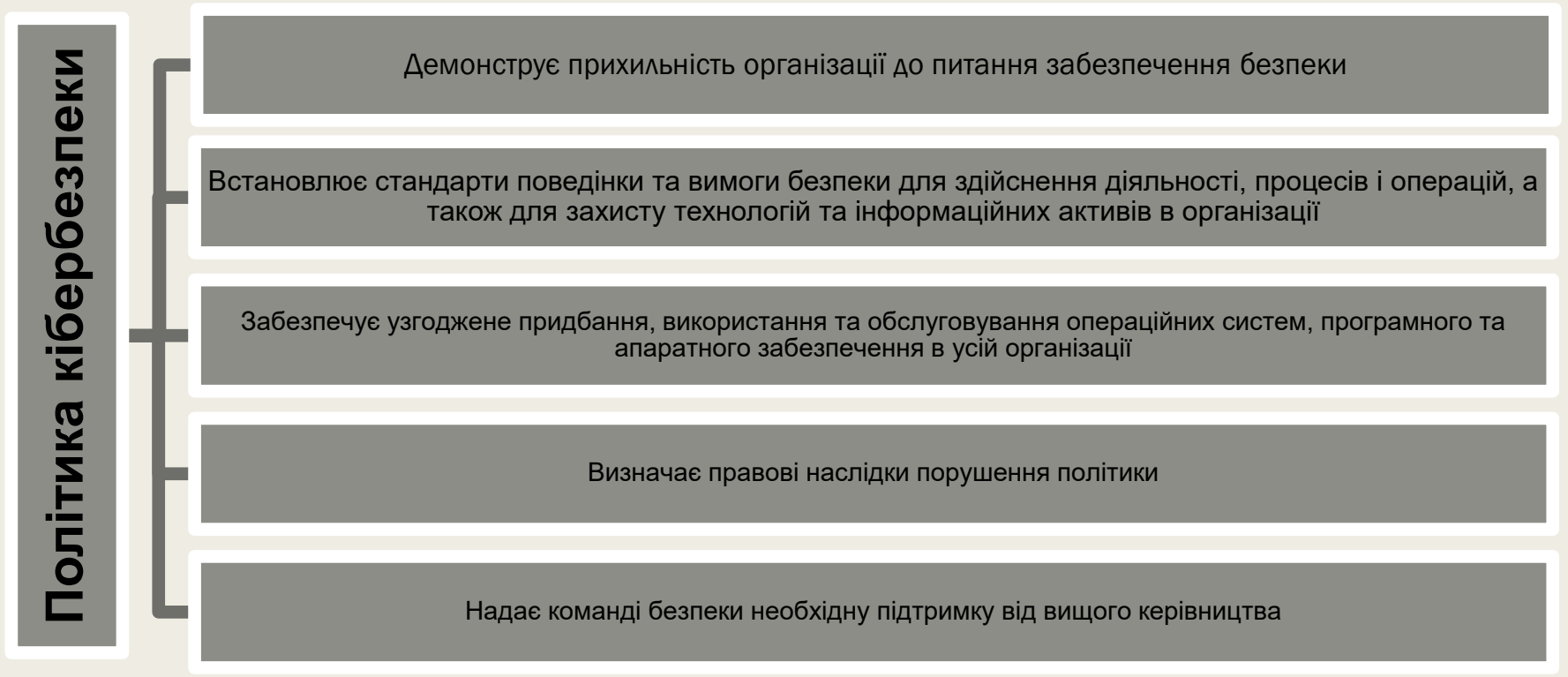
Управління даними

У ефективних програмах управління даними визначено кілька ключових ролей:

Власник даних	Особа, яка забезпечує дотримання політик та процедур, класифікує інформаційні активи та визначає критерії доступу до інформаційних активів.
Контролер даних	Особа, яка визначає цілі та спосіб обробки персональних даних.
Обробник даних	Особа або організація, яка обробляє персональні дані від імені контролера даних.
Зберігач даних	Особа, яка контролює класифікацію та безпеку даних, відповідно до встановлених власником даних правил. Іншими словами, зберігач даних відповідає за технічний контроль даних.
Адміністратор даних	Особа, яка гарантує, що дані підтримують бізнес-потреби організації та відповідають нормативним вимогам.
Фахівець з питань захисту даних	Особа, яка наглядає за стратегією захисту даних в організації.

Політики кібербезпеки

Політика кібербезпеки — це високорівневий документ, в якому викладено бачення кібербезпеки в організації, включаючи цілі, потреби, зміст та відповідальність.



Типи політик кібербезпеки

До найпоширеніших політик кібербезпеки належать:

- **Основна політика кібербезпеки**
  - Політика, викладена у концепції кібербезпеки організації, яка служить стратегічним планом впровадження засобів контролю кібербезпеки.

- **Системна політика**
  - Цей тип політики розроблений для конкретних пристроїв або комп'ютерних систем і має на меті стандартизувати затверджені додатки, програмне забезпечення, конфігурації операційної системи, апаратне забезпечення, а також посилити контрзаходи в організації.

- **Цільова політика**
  - Цей тип політики розробляється для певних експлуатаційних проблем, обставин або умов, які можуть вимагати більш детальних вимог і вказівок.

Організація повинна встановити чіткі та детальні політики безпеки, що доведені до відома **усіх** співробітників.

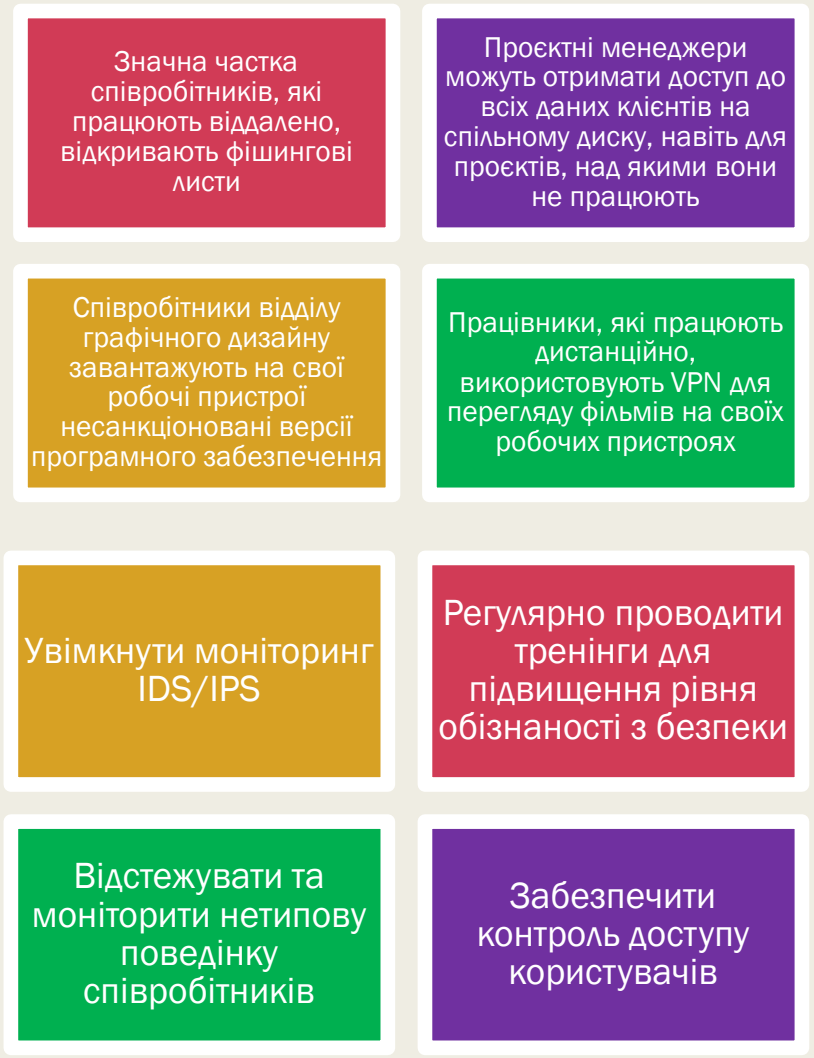
Типи політик кібербезпеки

Політика ідентифікації та аутентифікації	Визначає того, кому може бути надано доступ до мережних ресурсів, а також вказує на існуючі процедури перевірки, які цьому сприяють.
Політики використання паролів	Визначає мінімальні вимоги до пароля.
Політика прийнятного використання	Висвітлює сукупність правил, які визначають доступ до мережних ресурсів та їх використання.
Політика віддаленого доступу	Вказує, як віддалено підключитися до внутрішньої мережі організації, та пояснює, яка інформація доступна віддалено.
Політика обслуговування мережі	Описує процедури оновлення обраних організацією операційних систем та програм кінцевих користувачів.
Політики обробки інциденту	Надає рекомендації щодо того, як повідомляти та реагувати на інциденти, пов’язані з безпекою в організації.
Політика даних	Встановлює вимірювані правила обробки даних в організації, наприклад, вказує, де зберігати дані, як дані класифікувати, а також, як дані обробляти та як дані видаляти.
Політика повноважень	Забезпечує дотримання правил створення облікових записів.
Організаційна політика	Надає рекомендації щодо того, як потрібно виконувати роботу в організації.

Принципи управління людськими ресурсами

Загрози		Контроль безпеки	
Значна частка співробітників, які працюють віддалено, відкривають фішингові листи	Проєктні менеджери можуть отримати доступ до всіх даних клієнтів на спільному диску, навіть для проєктів, над якими вони не працюють	Увімкнути моніторинг IDS/IPS	Регулярно проводити тренінги для підвищення рівня обізнаності з безпеки
Співробітники відділу графічного дизайну завантажують на свої робочі пристрої несанкціоновані версії програмного забезпечення	Працівники, які працюють дистанційно, використовують VPN для перегляду фільмів на своїх робочих пристроях	Відстежувати та моніторити нетипову поведінку співробітників	Забезпечити контроль доступу користувачів

Принципи управління людськими ресурсами



Додаткові заходи, які організації можуть запровадити для управління загрозами користувачам, включають:

•Узгодження заходів для забезпечення безпеки із цілями службової атестації.
•Увімкнення фільтрації контенту, щоб дозволити чи заборонити використовувати певні домени відповідно до застосованої політики використання.
•Вимкнення внутрішніх CD-приводів та USB-портів.
•Увімкнення автоматичного сканування для пошуку загроз на підключених дискових носіях, у файлах і у вкладеннях електронної пошти.
•Надання дозволу на запис і видалення даних тільки їх власнику.

Етика фахівця з кібербезпеки

Фахівець з кібербезпеки повинен розуміти як закон, так і інтереси організації, щоб мати можливість ухвалювати правильні рішення

Етику можна розглядати з різних поглядів:

Утилітарна етика	Вона базується на принципі, що наслідок дії є найважливішим фактором, щоб визначити моральність чи аморальність вчинку. Наприклад, етичним вибором є дія, яка максимізує найбільше благо для найбільшої кількості людей.
Правовий підхід	Правовий підхід керується принципом, який стверджує, що особа має право зробити власний вибір, який не може бути порушений рішенням іншої особи. Це рішення має поважати та враховувати основні права людини. До таких основних прав належать право на правду, право на конфіденційність, право на безпеку і справедливе застосування суспільством законів до всіх членів суспільства.
Підхід загального блага	Підхід загального блага пропонує вважати етичними дії, які приносять користь усій громаді. Це провокує людей визнавати та дотримуватися спільних з іншими членами громади цінностей та цілей.

Десять заповідей комп'ютерної етики

Дослідження кіберетики

Завантажувати захищені авторським правом музичні файли для прослуховування на роботі

Заходити у сторонній додаток, використовуючи дані колеги, коли адміністратор не доступний

Завантаження плану проекту колеги після виявлення помилки

Отримувати доступ до файлів клієнта, щоб побачити, як колега займається своєю справою

Посилатися на джерело в дописі у блозі

Скаржитися на роботу колеги в приватній чат-групі

Розміщення повідомлення на внутрішньому форумі, щоб подякувати колезі за допомогу

Дослідження кіберетики

Завантаження захищених авторським правом музичних файлів для прослуховування на роботі

Заходити у сторонній додаток, використовуючи дані колеги, коли адміністратор не доступний

Оновлення плану проекту колеги після виявлення помилки

Отримувати доступ до файлів клієнта, щоб побачити, як колега займається своєю справою

Посилатися на джерело в дописі у блозі

Скаржитися на роботу колеги в приватній чат-групі

Розміщення повідомлення на внутрішньому форумі, щоб подякувати колезі за допомогу

Кіберзлочинність

Кіберзлочини поділяються на три категорії:

1. **Злочини проти комп’ютерів –** це злочини, в яких об’єктом злочинної діяльності є комп’ютери. Наприклад, атака зловмисного програмного забезпечення, злом або атака відмови в обслуговуванні.

2. **Злочини, пов'язані із використанням комп'ютерів,** мають місце тоді, коли комп’ютер використовується для вчинення злочину, наприклад, крадіжки або шахрайства.

3. **Випадкові комп'ютерні злочини** мають місце тоді, коли комп’ютер надає випадкову інформацію щодо фактичного злочину. Наприклад, комп’ютер використовується для зберігання незаконно завантажених відео, а не як інструмент для вчинення злочину.

Кіберзлочинність зростає набагато швидше, ніж здатність правової системи створювати закони та нормативні акти, які це забороняють.

Закони про кібербезпеку

Статутне право	Конгрес США створив федеральні адміністративні установи і нормативну базу, яка передбачає як цивільні, так і кримінальні покарання за недотримання правил. Кримінальні закони забезпечують дотримання загальноприйнятого морального кодексу, підкріпленого повноваженнями уряду. Наприклад, Закон про комп'ютерне шахрайство та зловживання (Computer Fraud and Abuse Act) – це закон, який забороняє доступ до комп'ютера без дозволу або із завищеними правами доступу. Порушення цих правил може призвести до штрафу або позбавлення волі.
Адміністративне право	Як правова база, що регулює діяльність адміністративних органів влади, адміністративне право гарантує, що державні органи влади діють відповідно до закону. Наприклад, Федеральна комісія з комунікацій (Federal Communications Commission – FCC) і Федеральна торгова комісія (Federal Trade Commission – FTC) займаються такими проблемами, як крадіжка інтелектуальної власності та шахрайство.
Загальне право	Справи загального права проходять через судову систему, створюючи прецеденти та конституційні основи для законотворчості.

Національне законодавство

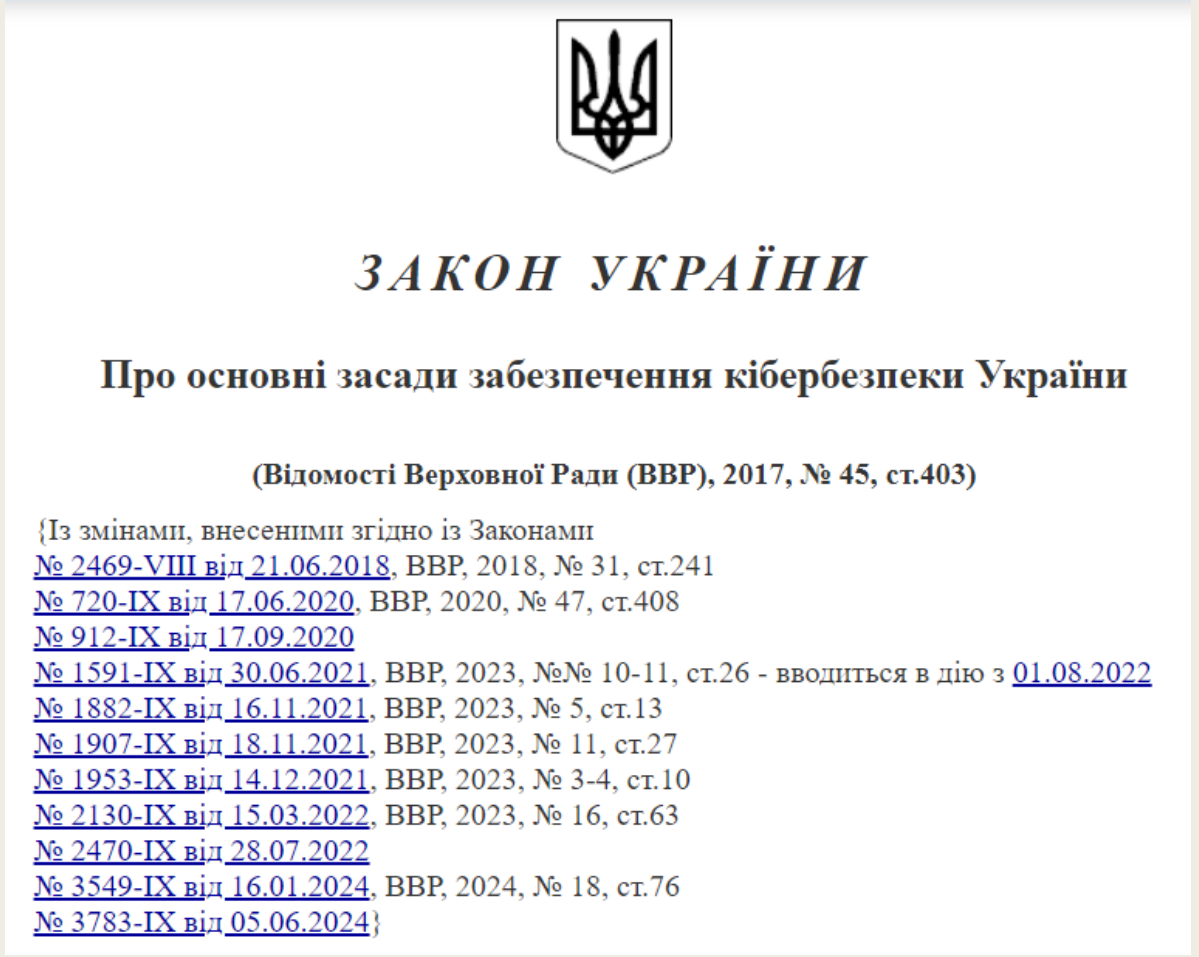
КОНСТИТУЦІЯ УКРАЇНИ

Стаття 17. Захист суверенітету і територіальної цілісності України, забезпечення її економічної та ***інформаційної безпеки*** є найважливішими функціями держави, справою всього Українського народу.

Нормативно-правова база України у сфері управління кібербезпекою

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

https://zakon.rada.gov.ua/laws/show/2163-19?find=1&text=%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA#Text



ЗАКОН УКРАЇНИ

Про основні засади забезпечення кібербезпеки України

(Відомості Верховної Ради (ВВР), 2017, № 45, ст.403)

{Із змінами, внесеними згідно із Законами
№ 2469-VIII від 21.06.2018, ВВР, 2018, № 31, ст.241
№ 720-IX від 17.06.2020, ВВР, 2020, № 47, ст.408
№ 912-IX від 17.09.2020
№ 1591-IX від 30.06.2021, ВВР, 2023, №№ 10-11, ст.26 - вводиться в дію з 01.08.2022
№ 1882-IX від 16.11.2021, ВВР, 2023, № 5, ст.13
№ 1907-IX від 18.11.2021, ВВР, 2023, № 11, ст.27
№ 1953-IX від 14.12.2021, ВВР, 2023, № 3-4, ст.10
№ 2130-IX від 15.03.2022, ВВР, 2023, № 16, ст.63
№ 2470-IX від 28.07.2022
№ 3549-IX від 16.01.2024, ВВР, 2024, № 18, ст.76
№ 3783-IX від 05.06.2024}

Закон України "Про основні засади забезпечення кібербезпеки України"

- **Стаття 3.** Правові основи забезпечення кібербезпеки України
- 1. Правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, цей та інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України.

Стаття 9.

CERT-UA - Урядова команда реагування на комп'ютерні надзвичайні події України, яка функціонує в рамках Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України

Завдання CERT-UA:

- накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів;
- надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об'єктів;
- організація та проведення практичних семінарів з питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту;
- підготовка та розміщення на своєму офіційному веб-сайті рекомендацій щодо протидії сучасним видам кібератак та кіберзагроз;
- взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки;
- взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамках участі у Форумі команд реагування на інциденти безпеки FIRST із сплатою щорічних членських внесків;
- взаємодія з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору;
- опрацювання отриманої від громадян інформації про кіберінциденти щодо об'єктів кіберзахисту;
- сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам.

Нормативно-правова база України у сфері кібербезпеки

Стратегія Кібербезпеки України - визначає пріоритети, цілі та завдання забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

https://zakon.rada.gov.ua/laws/show/447/2021#n12

Стратегія Кібербезпеки України

Основні цілі

- Дієва кібероборона
- Ефективна протидія розвідувально-підривній діяльності у кіберпросторі та кібертероризму
- Ефективна протидія кіберзлочинності
- Розвиток асиметричних інструментів стримування
- Національна кіберготовність та надійний кіберзахист
- Професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки
- Безпечні цифрові послуги
- Зміцнення системи координації
- Формування нової моделі відносин у сфері кібербезпеки
- Прагматичне міжнародне співробітництво

Міжнародна стандартизація

Конвенція про кіберзлочинність (Будапештська угода) - перша міжнародна угода, яка стосується Інтернет- та цифрових злочинів.

Конвенцією наголошуються спільні дії на національному та міждержавному рівнях з припинення несанкціонованого втручання в роботу комп'ютерних систем, незаконного перехоплення даних і втручання в комп'ютерні системи. Відповідно цьому всі кіберзлочини Конвенція ділить на чотири види:

- злом комп'ютерних систем;
- шахрайство;
- заборонений контент;
- порушення авторських прав.

Конвенція
про кіберзлочинність

Статус Конвенції див. (994_789)

{ Додатковий протокол від 28.01.2003
до Конвенції див. (994_687)}

(Конвенцію ратифіковано із застереженнями і заявами Законом
N 2824-IV (2824-15) від 07.09.2005, ВВР, 2006, N 5-6, ст.71)

Дата підписання: 23.11.2001

Дата ратифікації: 07.09.2005

Дата набрання чинності: 01.07.2006

Станом на квітень 2023 року ***68 держав*** ратифікували конвенцію.

ISO/IEC 27000

- ISO/IEC 27000 — це серія стандартів або найкращих практик інформаційної безпеки, які допомагають організаціям покращити свою інформаційну безпеку.
- Опубліковані Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (ICO), стандарти ISO 27000 встановлюють вимоги до комплексної системи управління безпекою інформації (ISMS).
- ISMS складається з адміністративних, технічних та операційних засобів контролю інформаційної безпеки в організації.
- Стандарт ISO 27000 представлений дванадцятьма незалежними доменами.
- Ці дванадцять доменів забезпечують основу для розробки стандартів безпеки та ефективних практик управління безпекою в організаціях, а також допомагають полегшити спілкування між організаціями.

ISO/IEC 27000

Оцінка ризиків	Перший крок у процесі управління ризиками, який передбачає кількісне та якісне вимірювання ризику конкретної ситуації чи загрози.
Політика безпеки	У цьому документі розглядаються обмеження та дії співробітників в організації, а також часто вказується, як і хто може отримати доступ до даних.
Організація інформаційної безпеки	Це модель управління інформаційною безпекою, що впроваджена організацією.
Управління ресурсами	Це схема проведення інвентаризації та класифікації інформаційних активів в організації.
Безпека людських ресурсів	Стосується процедур безпеки, що пов'язані із прийняттям, переміщення всередині організації та звільненням працівників.
Фізична безпека та безпека середовища	Стосується фізичного захисту об’єктів та інформації в організації.
Комунікаційний та операційний менеджмент	Стосується управління технічними засобами контролю безпеки систем і мереж організації.

ISO/IEC 27000

Придбання, розробка та обслуговування інформаційних систем	Стосується безпеки як невід'ємної частини інформаційних систем організації.
Контроль доступу	Описує, як організація обмежує права доступу до мереж, систем, функцій програм і даних, щоб запобігти несанкціонованому доступу користувачів.
Керування подіями інформаційної безпеки	Описує організаційний підхід до прогнозування та реагування на порушення інформаційної безпеки.
Керування безперервністю бізнесу	Описує здатність організації захищати, підтримувати та відновлювати критичну для бізнесу діяльність після збою в роботі інформаційних систем.
Відповідність	Описує процес забезпечення відповідності політикам, стандартам і нормам інформаційної безпеки.

- Структура цієї моделі кібербезпеки ISO відрізняється від моделі взаємозв'язку відкритих систем (OSI) тим, що це однорангова модель, яка використовує домени, а не шари для опису категорій безпеки.
- Кожен домен має прямий зв'язок з іншими доменами.
- Ці дванадцять доменів складаються з **цілей контролю** (ISO 27001) і **засобів контролю** (ISO 27002).

Цілі та засоби контролю

Цілі контролю

Визначають високорівневі вимоги для впровадження комплексної системи управління ІБ в організації і, зазвичай, надають контрольний список, який використовується під час аудиту ISMS.

Проходження цього аудиту свідчить про те, що організація відповідає стандарту ISO 27001 і запевняє партнерів у безпечності даних та операцій організації.


CERTSYSTEMS

СЕРТИФІКАТ

системи менеджменту якості

"СПЛАЙН СІСТЕМЗ"

ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ

Україна, 37600, Полтавська обл., місто Миргород, вулиця Гоголя, будинок 178

Код ЄДРПОУ 42436210

Орган сертифікації DP CERTSYSTEMS підтверджує, що система менеджменту якості вищезазначеної організації перевірена і відповідає вимогам міжнародного стандарту

ISO 9001:2015 «Системи менеджменту якості. Вимоги»

ДСТУ ISO 9001:2015 (ISO 9001:2015, IDT) «Системи управління якістю. Вимоги»
ДСТУ EN ISO 9001:2018 (EN ISO 9001:2015, IDT; ISO 9001:2015, IDT) «Системи управління якістю. Вимоги»

Сфера сертифікації:

- 25.11 Виробництво будівельних металевих конструкцій і частин конструкцій;
- 25.50 Кування, пресування, штампування, профілювання; порошкова металургія;
- 25.62 Механічне оброблення металевих виробів;
- 25.99 Виробництво інших готових металевих виробів, н.в.і.у.;
- 71.12 Діяльність у сфері інжинірингу, геології та геодезії, надання послуг технічного консультування в цих сферах

Дата сертифікації: 29.01.2024 р.
Дійсний до: 29.01.2027 р.

Сертифікат вважається дійсним за умови щорічного підтвердження:
2025 р. - до 29.01.2025 р.
2026 р. - до 29.01.2026 р.

Дійсність сертифіката перевіряють використовуючи QR код або на сайті euro-cert.net

Директор органу сертифікації С. Петрова

ECS Зареєстрований у Реєстрі Системи Сертифікації EUROCERT SYSTEM сертифікат № ECS.UA.02.4156 від 29.01.2024р.

DP CERTSYSTEMS, 07 Zelenskoho St., Apt 378, Kyiv, Ukraine, 02094. Notification Letter № ECS.UA.03.159, Date of Notification 29.04.2021 issued by EUROCERT SYSTEM: Bulgaria, Plovdiv


СЕРТИФІКАЦІЙНИЙ ЦЕНТР «СТАНДАРТ»

СЕРТИФІКАТ

відповідності системи управління інформаційною безпекою

Цим сертифікатом посвідчується,
що система управління інформаційною безпекою стосовно:
Банківська діяльність, діяльність на фондовому ринку
(депозитарна діяльність, діяльність торговця цінними паперами).

otpbank АТ «ОТП БАНК»

вул. Жилянська, 43, м. Київ, 01033, Україна.
(відділення відповідно до Додатку).

згідно з чинними нормативними документами,
відповідає вимогам стандарту

ДСТУ ISO/IEC 27001:2015

Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT)

Перевірка відповідності сертифікованої системи управління інформаційною безпекою вимогам зазначеного стандарту здійснюється шляхом періодичних наглядових аудитів

Сертифікат виданий Органом сертифікації
ТОВ «Сертифікаційний центр «СТАНДАРТ»,
вул. Марії Капніст, 2, офіс 301, м. Київ, 03057, Україна
тел.: (044) 494-12-15

IAF

8O045
ДСТУ EN ISO/IEC 17021-1:2017

Положення щодо застосовності від "24" червня 2019 р.

Директор ТОВ «СЦ «СТАНДАРТ»

Сертифікат виданий "01" липня 2021 р.
№ 0113-ISMS21
дійсний до "30" червня 2024 р.

СТАНДАРТ /З.Д. Гуліна/

Сертифікацію за стандартом ISO 27001-2013 проводять Органи сертифікації, які акредитовані національними організаціями з акредитації. В Україні такою державною організацією є *Національне агентство з акредитації України (НААУ).*

Цілі та засоби контролю

Ціль контролю організації - забезпечення доступу до мереж за допомогою відповідних механізмів аутентифікації користувачів і обладнання.

Важливий **засіб контролю** - використання надійних паролів, що складаються щонайменше з восьми символів і комбінації великих і малих літер, цифр і символів.

Засоби контролю

Показують, як досягти цілей контролю в організації. Вони надають рекомендації щодо впровадження, підтримки та покращення управління інформаційною безпекою в організації.

Засоби контролю схожі на рекомендації. Вони **не** є обов’язковими, і часто існує кілька способів дотримання цілей контролю. Але контроль завжди має бути нейтральним і не підтримувати певний продукт чи організацію.

ISO 27000 і тріада CIA

- ISO 27000 є універсальною концепцією для організації будь-якого типу.
- Щоб ефективно використовувати концепцію у своєму середовищі та у своїй діяльності організація повинна визначити *сфери*, *цілі контролю* та *засоби контролю*.
- Для цього, більшість організацій формують заяву про застосовність (statement of applicability – SOA), яка дозволяє адаптувати доступні цілі та засоби контролю, щоб якнайкраще відповідати встановленим пріоритетам щодо **конфіденційності (confidentiality)**, **цілісності (integrity)** та **доступності (availability)**.
- Засоби контролю ISO орієнтовані на забезпечення безпеки даних у будь-якому з трьох станів: **в обробці**, **у стані спокою** (зберігання) та у **транзитному стані (передавання)**.
- Відповідальність за визначення та впровадження відповідних засобів контролю можуть нести різні групи в організації.
- Наприклад, група з безпеки мережі може відповідати за засоби контролю, які забезпечують конфіденційність, цілісність і доступність усіх даних, що передаються (дані в дорозі), група програмістів і аналітиків даних може відповідати за дані, які перебувають в обробці (в процесі), і група спеціалістів з апаратної підтримки може відповідати за зберігання даних (у стані спокою/зберігання).

Концепція професійної підготовки в галузі кібербезпеки

- *Національний інститут стандартів і технологій (NIST)* створив Національну концепцію професійної підготовки в галузі кібербезпеки для підтримки організацій, які шукають фахівців з кібербезпеки. У концепції виділено сім категорій робіт з кібербезпеки, для яких окреслено основні посадові ролі та необхідні для кожної з них навички та обов’язки:

Використання та обслуговування	Передбачає підтримку, адміністрування та технічне обслуговування, що необхідні для забезпечення ефективної та дієвої роботи і безпеки IT-систем.
Охорона та захист	Визначає, аналізує та знижує загрози для внутрішніх систем і мереж.
Розслідування	Передбачає розслідування кіберінцидентів і/або кібератак, що пов'язані з використанням IT-ресурсів.
Збір та обробка	Передбачає виконання спеціальних операцій відмови і введення в оману, а також збирання інформації про кібербезпеку.
Аналіз	Передбачає вузькоспеціалізований огляд і оцінку вхідної інформації про кібербезпеку, щоб визначити її корисність для розвідки.
Нагляд і управління	Забезпечує лідерство, управління, спрямування або розвиток та популяризацію, щоб організація могла ефективно виконувати роботу з кібербезпеки.
Забезпечення безпеки	Передбачає концептуалізацію, проєктування, придбання або створення безпечних IT-систем.

Критичний контроль безпеки CIS

- Центр Інтернет-безпеки (Center for Internet Security – CIS) розробив сукупність критичних засобів контролю безпеки, щоб допомогти організаціям з різним рівнем ресурсів і досвіду, які вони мають, покращити свій кіберзахист.
  - ***Базові засоби контролю –*** Організації з обмеженими ресурсами та наявними знаннями в галузі кібербезпеки повинні впроваджувати: інвентаризацію та контроль апаратних засобів, інвентаризацію та контроль програмних активів, неперервне управління вразливостями, контрольоване використання адміністративних привілеїв, безпечні конфігурації для апаратного та програмного забезпечення, ведення, моніторинг та аналіз журналів аудиту.
  - ***Фундаментальні засоби контролю –*** Організації, які володіють помірними ресурсами та знаннями в галузі кібербезпеки, повинні впровадити базові засоби контролю, а також: захист електронної пошти та веб-браузера, захист від шкідливих програм, обмеження та контроль мережних портів, протоколів і служб, можливості відновлення даних, безпечні конфігурації для мережних пристроїв, захист периметру, захист даних, контрольований доступ за принципом «необхідно знати», контроль бездротового доступу, моніторинг і контроль облікового запису.
  - ***Організаційні засоби контролю –*** Організації, які володіють значними ресурсами та досвідом у сфері кібербезпеки, повинні запровадити базові та фундаментальні засоби контролю, а також: програму підвищення обізнаності та навчання щодо безпеки, безпеку прикладного програмного забезпечення, реагування на інциденти та управління ними, тести на проникнення та вправи червоної команди (імітовані вправи з атаки для оцінки можливостей безпеки організації).