С. О. Лисенко
І. В. Сервецький

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ ТА ЗАХИСТ ІНФОРМАЦІЇ У СФЕРАХ СУСПІЛЬНОЇ ДІЯЛЬНОСТІ

МІЖРЕГІОНАЛЬНА
АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ

МЕТОДИЧНИЙ ПОСІБНИК
щодо забезпечення практичної роботи
слухачів курсу

“ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ ТА ЗАХИСТ ІНФОРМАЦІЇ У СФЕРАХ СУСПІЛЬНОЇ ДІЯЛЬНОСТІ”

Київ
2026

УДК 351.746:316.77-049.5](477)(076)
Л61

Автори та укладачі:
С. О. Лисенко, д-р юрид. наук, проф., директор Ін-ту безпеки, зав. кафедри інформаційної безпеки
І. В. Сервецький, д-р юрид. наук, проф., зав. кафедри національної безпеки

Схвалено Вченою радою Міжрегіональної Академії управління персоналом (протокол № 9 від 24.09.2025)

Лисенко С. О., Сервецький І. В.
Л61 Методичний посібник щодо забезпечення практичної роботи слухачів курсу “Інформаційна безпека держави та захист інформації у сферах суспільної діяльності”. Київ: Міжрегіональна Академія управління персоналом, 2026. 196 с.

ISBN 978-617-02-0437-0

Методичний посібник містить лекційний та практичний матеріали, контрольні питання для перевірки знань студентів, наявні інформаційні ресурси держави, а також список рекомендованої літератури.

Для слухачів курсу “Інформаційна безпека держави та захист інформації у сферах суспільної діяльності”, науково-педагогічних працівників, студентів, адвокатів, працівників правоохоронних органів та спеціальних служб.

УДК 351.746:316.77-049.5](477)(076)

ISBN 978-617-02-0437-0

ВСТУП

Актуальність курсу та посібника

Сучасний етап розвитку суспільства характеризується стрімкою глобалізацією інформаційних процесів та перетворенням інформації на ключовий ресурс держави, економіки та соціальної сфери. В умовах гібридної агресії проти України інформаційна безпека держави та пов'язаний з нею захист інформації набувають критичного, першочергового значення. Захист інформації у сферах суспільної діяльності є протидією деструктивним інформаційним впливам.

Якісна підготовка компетентних кадрів у цій галузі є стратегічним завданням для системи освіти та національної безпеки. Цей методичний посібник розроблено з метою забезпечення слухачів необхідним інструментарієм для формування практичних компетенцій, передбачених освітньою програмою дисципліни "Інформаційна безпека держави та захист інформації у сферах суспільної діяльності".

Мета посібника

Метою посібника є організація та методичне забезпечення ефективної практичної роботи слухачів, спрямованої на закріплення теоретичних знань, набуття вмінь аналізувати, оцінювати та мінімізувати загрози інформаційній безпеці, а також розробляти та впроваджувати комплексні системи захисту інформації на різних рівнях.

Основними завданнями посібника є:

- надання чітких інструкцій щодо виконання конкретних практичних завдань у межах кожного тематичного модуля;
- систематизація матеріалу курсу, що охоплює як загальнодержавні аспекти ІБ, так і специфіку захисту інформації у соціальній сфері;
- формування навичок роботи з нормативно-правовою базою України та міжнародними стандартами у сфері кібербезпеки та захисту даних;

- стимулювання критичного мислення та здатності самостійно приймати рішення в умовах реальних і модельованих кіберінцедентів;
- підготовка слухачів до виконання кваліфікаційних робіт і професійної участі у сферах суспільної діяльності.

Об'єкт і предмет вивчення дисципліни

Об'єктом вивчення дисципліни є сукупність процесів забезпечення стійкості інформаційного простору держави, функціонування систем захисту інформації та діяльність суб'єктів, відповідальних за інформаційну безпеку.

Предметом вивчення є методи, засоби, технології та організаційні підходи до захисту інформації, що циркулює в інформаційно-телекомунікаційних системах державних органів, установ соціальної сфери, а також механізми протидії внутрішнім та зовнішнім інформаційним загрозам.

Структура посібника

До методичного посібника входять вступ, два модулі, що охоплюють 23 практичні роботи, а також додатковий матеріал.

Модуль І "Інформаційна безпека держави" присвячений макрорівню ІБ, включаючи нормативно-правову базу, державну політику, захист критичної інфраструктури та міжнародне співробітництво.

Модуль ІІ "Захист інформації у сферах суспільної діяльності" фокусується на специфічних аспектах захисту персональних і медичних даних, медіаграмотності, протидії деструктивним впливам та кібербулінгу.

Кожна практична робота містить назву, мету, перелік необхідного обладнання/джерел та деталізовані завдання для самостійного виконання слухачами.

Посібник призначений для слухачів, студентів, аспірантів і фахівців, які прагнуть поглибити свої знання та набути практичних навичок у сфері забезпечення інформаційної безпеки України.

Перелік умовних позначень

ІБ — Інформаційна безпека.
ІТС — Інформаційно-телекомунікаційна система.
КСЗІ — Комплексна система захисту інформації.
КІІ — Критична інформаційна інфраструктура.
НП(А)О — Нормативно-правовий (акт/забезпечення/основа).
ОТЗІ — Організаційно-технічна система захисту інформації.
ПДн — Персональні дані.
РНБО — Рада національної безпеки і оборони України.
СБУ — Служба безпеки України.
ДССЗЗІ — Державна служба спеціального зв'язку та захисту інформації України.
ІПСО — Інформаційно-психологічна операція.
КНЕДП — Кваліфікований надавач електронних довірчих послуг.
РЕР — Радіоелектронна розвідка.
РЕБ — Радіоелектронна боротьба.
ДСТУ — Державний стандарт України.
ISO/IEC — Міжнародна організація зі стандартизації / Міжнародна електротехнічна комісія.
CERT-UA — Команда реагування на комп'ютерні надзвичайні події України (структурний підрозділ ДССЗЗІ).
eHealth — Електронна система охорони здоров'я.

Модуль І

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ

Тема 1. Поняття, сутність і концепція інформаційної безпеки держави

Інформація у XXI ст. стала ключовим ресурсом, від якого залежить не лише розвиток економіки, науки чи культури, а й існування держави як цілісного політичного та соціального організму. Зростання ролі інформаційних технологій і глобальних комунікацій привело до того, що безпека держави визначається не лише її військовим або економічним потенціалом, а й здатністю захистити інформаційний простір, забезпечити суверенність інформаційних ресурсів і протидіяти деструктивним інформаційним впливам.

Саме тому інформаційна безпека поряд із військовою, політичною, економічною та екологічною розглядається як одна з ключових складових національної безпеки. У сучасних умовах, коли Україна стикається з гібридною війною, масованими інформаційно-психологічними операціями та кібератаками, питання розуміння сутності інформаційної безпеки й формування ефективної системи її забезпечення набувають першочергового значення.

У науковій літературі існує кілька підходів до визначення інформаційної безпеки. У найбільш загальному вигляді її можна трактувати як **стан захищеності інформаційного простору держави, суспільства та особи від зовнішніх і внутрішніх загроз, що забезпечує збереження, цілісність, доступність та достовірність інформації**, а також безперешкодне функціонування інформаційної інфраструктури.

В українському законодавстві, зокрема у Законі України "Про національну безпеку" (2018 р.), інформаційна безпека визначається як один з основних напрямів державної політики у

сфері національної безпеки та оборони. Основними її складовими є:

- захист прав і свобод людини в інформаційній сфері;
- забезпечення розвитку інформаційного суспільства;
- захист критичної інформаційної інфраструктури;
- протидія інформаційній агресії та дезінформації.

У дисертації С. Лисенка підкреслюється, що інформаційна безпека має **подвійний характер**: з одного боку, вона є об'єктом державного управління (сфера, у якій формуються й реалізуються політики), а з іншого — результатом діяльності органів влади та суспільства, тобто досягнутим станом захищеності.

Національна безпека — це комплекс заходів, спрямованих на збереження суверенітету, територіальної цілісності, політичної стабільності та сталого розвитку країни. Інформаційна безпека у цьому контексті виступає одночасно **засобом** і **метою**:

- як засіб — вона гарантує стабільність у політичному, економічному та військовому житті;
- як мета — передбачає створення умов для розвитку інформаційного суспільства, інноваційної економіки, цифрової держави.

Інформаційна безпека тісно пов'язана з іншими складовими національної безпеки:

- з військовою безпекою — через використання інформаційних технологій у бойових діях, кібероперація, розвідці;
- з економічною безпекою — оскільки цифрові фінансові системи є об'єктом атак;
- з політичною безпекою — адже маніпуляції інформацією можуть впливати на легітимність влади й демократичні процеси;
- із соціальною безпекою — через інформаційний вплив на суспільну свідомість і рівень довіри між громадянами.

Таким чином, інформаційна безпека не є ізольованим явищем, а виступає **інтегруючим елементом системи національ-**

ної безпеки, що визначає ефективність функціонування інших її компонентів.

Класична міжнародна модель (CIA triad) визначає три основні складові інформаційної безпеки:

1. **Конфіденційність (Confidentiality)** — забезпечення доступу до інформації лише уповноважених осіб:
   - приклад: захист державних таємниць, персональних даних, військових розробок;
   - інструменти: криптографія, системи контролю доступу, розмежування прав користувачів.
2. **Цілісність (Integrity)** — збереження незмінності та достовірності інформації, недопущення її несанкціонованої модифікації:
   - приклад: захист електронних реєстрів від фальсифікацій;
   - інструменти: контроль цілісності даних, цифрові підписи, блокчейн-технології.
3. **Доступність (Availability)** — гарантування доступу до інформації та інформаційних ресурсів у потрібний час:
   - приклад: безперебійна робота державних електронних сервісів;
   - інструменти: резервування, відновлення після збоїв, кіберзахист від DDoS-атак.

У сучасному розумінні до цих базових складових додають ще дві:

1. **Автентичність (Authenticity)** — підтвердження достовірності джерела інформації.
2. **Незаперечність (Non-repudiation)** — гарантія, що відправник не зможе заперечити факт передачі інформації.

Інформаційна безпека держави повинна розглядатися з позицій **системного підходу**, де всі елементи взаємопов'язані й взаємозалежні.

Основні компоненти системи:

- правова база — закони, нормативно-правові акти, стандарти;

- органи державного управління — РНБО, СБУ, ДССЗЗІ, Міністерство оборони, Національний центр кібербезпеки тощо;
- технологічна інфраструктура — телекомунікаційні мережі, центри обробки даних, державні реєстри, інформаційні системи критичної інфраструктури;
- суб'єкти інформаційного простору — ЗМІ, соціальні мережі, громадянське суспільство, приватні компанії, міжнародні партнери;
- ресурсне забезпечення — кадрове, фінансове, науково-технічне, організаційне.

Системний підхід дає змогу розглядати інформаційну безпеку як **динамічний процес**, що включає моніторинг, прогнозування, попередження, реагування та відновлення після загроз.

Сучасний етап розвитку України характеризується низкою особливостей, які безпосередньо впливають на стан інформаційної безпеки:

Глобалізація:

- транснаціональний характер інформаційних потоків;
- залежність від іноземних IT-платформ (Google, Meta, Microsoft);
- необхідність гармонізації національного законодавства з міжнародними нормами.

Інформаційні технології:

- швидкий розвиток штучного інтелекту, квантових обчислень, 5G-мереж;
- зростання кількості кіберзлочинів, хактивізму, кібершпигунства;
- поява нових викликів: deepfake-технології, інформаційні маніпуляції.

Загрози війни та гібридні виклики:

- використання інформаційного простору як арени війни;
- масові кібератаки на державні установи (наприклад, атака на урядові сайти України у січні 2022 р.);

- інформаційно-психологічний вплив на суспільну свідомість через дезінформацію та пропаганду;
- потреба у створенні системи стійкості держави до інформаційних загроз.

Інформаційна безпека держави — це багатовимірне явище, що охоплює правові, технологічні, політичні та соціальні аспекти. Вона визначає здатність держави захищати свої інтереси в інформаційному просторі та забезпечувати розвиток демократичного суспільства.

Основними складовими інформаційної безпеки виступають конфіденційність, цілісність і доступність інформації, які повинні гарантуватися через системний підхід до управління цією сферою.

У сучасних умовах глобалізації, цифровізації та гібридної війни питання інформаційної безпеки виходять на рівень **стратегічних пріоритетів державної політики України**. Саме від ефективності системи стратегічного управління у цій сфері залежить не лише стабільність, а й майбутнє держави.

Контрольні питання

1. У чому полягає сутність інформаційної безпеки держави?
2. Які ключові елементи становлять концепцію інформаційної безпеки?
3. Чим відрізняється інформаційна безпека від інформаційної політики?
4. Які основні загрози впливають на національну інформаційну безпеку?
5. Які інтереси держави захищає система інформаційної безпеки?
6. Які міжнародні підходи до визначення поняття інформаційної безпеки?

Практичне питання

Мета

Закріпити базові уявлення про зміст інформаційної безпеки та концептуальні підходи до її розуміння.

Практичні завдання

1. Порівняльний аналіз: порівняти 3 різні наукові підходи до визначення поняття “інформаційна безпека”.
2. Кейс-аналіз: проаналізувати конкретну ситуацію (наприклад, витік персональних даних державного органу) та визначити, які елементи інформаційної безпеки були порушені.
3. Створити концептуальну схему “Система інформаційної безпеки держави: структурні елементи”.

Питання для обговорення

Чи може інформаційна безпека існувати без інформаційної політики?

Тема 2. Стратегічне управління: теоретико-методологічні засади

У сучасному світі держави функціонують у надзвичайно складному і динамічному середовищі, яке формується під впливом глобалізаційних процесів, геополітичних змін, технологічних інновацій та зростання ролі інформаційних ресурсів. У таких умовах традиційні методи державного управління вже не гарантують належного рівня безпеки і розвитку. Це зумовлює потребу у переході від тактичного чи адміністративного управління до **стратегічного управління** — управління, орієнтованого на довгострокові цілі, випереджальне реагування на виклики та комплексну інтеграцію різних сфер суспільного життя.

Особливої ваги стратегічне управління набуває у сфері інформаційної безпеки. В умовах гібридної війни, масштабних інформаційно-психологічних операцій та зростання кіберзагроз лише стратегічний підхід дає змогу сформувати цілісну політику захисту національного інформаційного простору.

Стратегічне управління — це діяльність органів державної влади, спрямована на визначення довгострокових пріоритетів,

формування стратегічних цілей і завдань, а також розроблення та реалізацію комплексних програм, спрямованих на досягнення сталого розвитку і зміцнення національної безпеки.

У науковій літературі стратегічне управління визначається як **процес прогнозування, планування, реалізації та коригування стратегій**, що забезпечує адаптивність держави до змін середовища.

Ключові ознаки стратегічного управління:

- довгостроковий горизонт планування — 10–20 років і більше;
- орієнтація на результат — досягнення стратегічних цілей, а не лише поточних завдань;
- гнучкість і адаптивність — здатність змінювати стратегії залежно від нових викликів;
- комплексність — охоплення політичної, економічної, соціальної, інформаційної, екологічної сфер;
- інноваційність — використання нових методів аналізу, прогнозування, інформаційних технологій.

Таким чином, стратегічне управління виступає не лише технологією управління, а й **методологією державної політики**, що визначає напрями розвитку країни.

Формування ефективної стратегії потребує використання сучасних методологій прогнозування та планування. Серед найбільш поширених підходів виокремлюють:

Форсайт (Foresight)

Форсайт — це метод системного прогнозування майбутнього, що ґрунтується на експертних оцінках, моделюванні сценаріїв і колективному обговоренні можливих варіантів розвитку. Цей метод:

- використовується для визначення технологічних трендів (наприклад, розвиток штучного інтелекту, квантових технологій);
- дає змогу формувати довгострокові пріоритети державної політики;

- в Україні застосовується у формуванні цифрових стратегій та дорожніх карт інтеграції до ЄС і НАТО.

Сценарне планування

Цей метод передбачає розроблення кількох можливих сценаріїв розвитку подій — від оптимістичного до кризового. Для сфери інформаційної безпеки це означає:

- сценарії кібератак на критичну інфраструктуру;
- сценарії масових кампаній дезінформації;
- сценарії геополітичних загострень, які впливають на інформаційний простір.

Сценарне планування дає змогу підготувати систему управління до **найгірших можливих варіантів** і забезпечити стійкість держави.

SWOT-аналіз

Метод оцінки сильних (Strengths) і слабких (Weaknesses) сторін, а також можливостей (Opportunities) і загроз (Threats).

У сфері інформаційної безпеки SWOT-аналіз допомагає виявити:

- сильні сторони — наявність фахівців, міжнародна підтримка;
- слабкі сторони — залежність від іноземних ІТ-платформ, недосконалість законодавства;
- можливості — інноваційні технології, цифрова інтеграція з ЄС;
- загрози — кібертероризм, інформаційна агресія.

Ризик-менеджмент

Система ідентифікації, аналізу, оцінювання та управління ризиками. Для державного управління інформаційною безпекою це означає створення **карти ризиків** та визначення **пріоритетних заходів** їх нейтралізації.

Стратегічне управління здійснюється на кількох рівнях, які взаємодіють між собою:

Державний рівень:

- визначення національних стратегічних інтересів;
- формування доктрин, стратегій, концепцій (наприклад, Стратегія національної безпеки, Кіберстратегія України);
- координація діяльності всіх органів влади;
- міжнародна співпраця у сфері безпеки.

Регіональний рівень:

- адаптація національних стратегій до умов конкретного регіону;
- захист регіональної інформаційної інфраструктури;
- моніторинг локальних загроз (наприклад, кібератак на органи місцевого самоврядування).

Організаційний рівень:

- забезпечення інформаційної безпеки підприємств, установ, ЗМІ;
- впровадження стандартів управління безпекою (ISO/IEC 27001, NIST);
- створення систем внутрішнього моніторингу та реагування на інциденти.

Важливо, щоб між усіма рівнями існувала **координація і вертикаль відповідальності**. Недостатність комунікації між державним, регіональним і організаційним рівнями може призвести до **фрагментарності управління** та зниження ефективності всієї системи.

Сьогодні інформаційна безпека розглядається не лише як сфера оборони, а й як **ключовий чинник розвитку держави**. Її інтеграція у стратегії розвитку означає:

У політичній сфері:

- формування єдиної інформаційної політики;
- протидія пропаганді, дезінформації та маніпуляціям;
- зміцнення інформаційного суверенітету.

В економічній сфері:

- захист фінансових і банківських систем від кібератак;
- розвиток цифрової економіки;
- інвестиції у кібербезпекові стартапи та інновації.

У соціальній сфері:

- підвищення рівня медіаграмотності населення;
- формування культури кібергігієни;
- підтримка свободи слова при одночасному захисті від маніпуляцій.

У військовій сфері:

- розвиток кіберсил оборони;
- створення системи кіберрозвідки;
- інтеграція інформаційних операцій у військові доктрини.

У міжнародній сфері:

- співпраця з НАТО, ЄС та іншими організаціями;
- участь у міжнародних ініціативах кібербезпеки;
- гармонізація законодавства з міжнародними стандартами.

Таким чином, інформаційна безпека є **транверсальною складовою** усіх стратегій розвитку держави, без якої неможливе забезпечення її стійкості та конкурентоспроможності.

Стратегічне управління є фундаментом сучасної державної політики. Воно дає змогу забезпечити довгостроковий розвиток країни, адаптуватися до глобальних викликів і формувати стійку систему інформаційної безпеки.

Методологічні підходи — форсайт, сценарне планування, SWOT-аналіз і ризик-менеджмент створюють наукове підґрунтя для прогнозування майбутніх загроз та вироблення адекватних стратегій.

Рівні управління — державний, регіональний, організаційний утворюють єдину систему, в якій інформаційна безпека інтегрується в усі сфери розвитку держави: політичну, економічну, соціальну, військову та міжнародну.

У результаті стратегічне управління стає **необхідною умовою збереження національного суверенітету та ефективної протидії сучасним інформаційним викликам**.

Контрольні питання

1. Що таке стратегічне управління у сфері інформаційної безпеки?
2. Які етапи включає стратегічне управління?
3. Які методи використовуються для стратегічного аналізу загроз?
4. У чому полягає різниця між стратегією і політикою безпеки?
5. Які чинники впливають на вибір стратегічних пріоритетів держави?
6. Які моделі стратегічного управління поширені у світовій практиці?

Практичне питання

Мета

Опрацювати інструменти стратегічного аналізу у сфері інформаційної безпеки.

Практичні завдання

1. SWOT-аналіз інформаційної безпеки України.
2. Створити дерево цілей державної стратегії інформаційної безпеки.
3. Розробити пропозиції до стратегічного плану (3 стратегічні й 3 оперативні цілі).

Питання для обговорення

Чому стратегічне управління в інформаційній сфері має бути адаптивним?

Тема 3. Внутрішні та зовнішні чинники формування загроз інформаційній безпеці

Інформаційна безпека сучасної держави формується у складному й багатовимірному середовищі, де взаємодіють як

внутрішні, так і зовнішні чинники. Їх поєднання створює широкий спектр загроз, що впливають на стабільність політичної системи, розвиток економіки, рівень соціальної згуртованості, а також здатність держави протидіяти зовнішнім викликам.

У дисертаційних дослідженнях стратегічного управління інформаційною безпекою наголошується, що для ефективного реагування на сучасні виклики держава має системно аналізувати природу цих чинників, розуміти їх динаміку та взаємозалежність. Лише тоді можна вибудувати адекватні механізми захисту національного інформаційного простору.

Глобальні політичні трансформації безпосередньо впливають на стан інформаційної безпеки кожної країни. Для України це питання має особливе значення з огляду на:

Зростання конкуренції між світовими центрами сили:

- США, ЄС, Китай, росія змагаються за контроль над глобальними інформаційними потоками, технологіями й цифровими ринками;
- призводить до використання інформаційної зброї як одного з головних інструментів геополітичного протистояння.

Гібридна війна росії проти України:

- інформаційна агресія супроводжує військові дії, формуючи ворожі наративи;
- масовані кібератаки на державні органи, критичну інфраструктуру, фінансову систему;
- кампанії дезінформації на міжнародному рівні для дискредитації України.

Міжнародні інформаційно-психологічні операції:

- поширення фейкових новин, пропагандистських матеріалів у глобальних медіа та соціальних мережах;
- спроби впливу на вибори й політичні процеси у демократичних країнах (наприклад, у США, Франції, Німеччині).

Інтеграційні процеси:

- вступ України до ЄС і співпраця з НАТО вимагають гармонізації національного законодавства з міжнародними стандартами;

- водночас посилюється залежність від міжнародних інформаційних систем і платформ, що створює нові ризики.

Таким чином, міжнародна обстановка виступає як **двосторонній чинник**, з одного боку, надає Україні доступ до ресурсів та міжнародної підтримки, а з іншого — робить її об'єктом інформаційних атак у глобальній конкуренції.

Внутрішні процеси також значною мірою визначають уразливість держави до інформаційних загроз. До них належать:

Політичні чинники:

- нестабільність політичної системи може стати підґрунтям для маніпуляцій у ЗМІ, поширення дезінформації, використання інформаційних ресурсів у міжпартійній боротьбі;
- недовіра громадян до влади посилює ефективність інформаційних атак ззовні;
- корупція та кланово-олігархічні інтереси використовують медіа як інструмент політичного впливу, що підриває незалежність інформаційного простору.

Соціально-економічні чинники:

- економічна криза сприяє зростанню соціальної напруги, яку легко експлуатувати інформаційними маніпуляціями;
- міграційні процеси (зовнішня трудова міграція, внутрішнє переміщення населення внаслідок війни) формують нові виклики для інформаційної політики;
- нерівний доступ до інформаційних ресурсів у сільській місцевості та малих громадах може призводити до інформаційної ізоляції та посилення вразливості.

Культурно-освітні чинники:

- низький рівень медіаграмотності частини населення підвищує ефективність ворожих дезінформаційних кампаній;
- мовна та культурна різноманітність може використовуватися зовнішніми гравцями для поширення наративів, спрямованих на розкол суспільства.

Таким чином, внутрішні соціально-політичні й економічні умови створюють середовище, у якому інформаційні загрози можуть або послаблюватися, або навпаки — посилюватися.

Технологічні зміни водночас відкривають нові можливості для розвитку держави та породжують ризики для інформаційної безпеки.

Розвиток інтернету та соціальних мереж:

- створюють умови для швидкого поширення інформації, а також для масових дезінформаційних кампаній;
- формують "інформаційні бульбашки", що посилюють поляризацію суспільства.

Інтернет речей (IoT):

- розширює можливості управління інфраструктурою, транспортом, медициною;
- водночас створює нові вразливості, адже злом IoT-пристроїв може паралізувати цілі системи.

Штучний інтелект і Big Data:

- застосовуються для прогнозування загроз, управління ризиками, виявлення фейкових новин;
- водночас використовуються для створення deepfake-контенту, автоматизації кібератак.

Рівень цифровізації суспільства:

- цифровізація державних послуг ("Дія", електронні реєстри, онлайн-освіта) підвищує ефективність управління;
- робить державу більш залежною від безперервної роботи цифрової інфраструктури.

Кіберзлочинність:

- розвиток технологій спричинив появу організованих кіберугруповань;
- Україна є однією з головних цілей для випробування нових форм кібератак.

Отже, технологічний прогрес має амбівалентний характер: він стає як ресурсом для розвитку, так і джерелом нових загроз.

Інформаційно-комунікаційна інфраструктура (ІКІ) є "каркасом" функціонування сучасної держави, а її стійкість визначає рівень інформаційної безпеки.

Складові ІКІ:

- телекомунікаційні мережі (інтернет, мобільний зв'язок, супутникові системи);
- державні електронні реєстри й бази даних;
- центри обробки даних;
- платформи електронного врядування та надання послуг;
- медійні системи та канали масової комунікації.

Загрози для ІКІ:

- кібератаки на критичну інфраструктуру;
- диверсії у сфері енергетики та транспорту, що призводять до паралічу комунікацій;
- залежність від імпортного обладнання й програмного забезпечення;
- недостатнє резервування та дублювання каналів зв'язку.

Роль держави у захисті ІКІ:

- створення національних центрів кіберзахисту та моніторингу;
- прийняття нормативно-правових актів, що визначають порядок захисту критичної інфраструктури;
- розвиток державно-приватного партнерства для забезпечення безпеки у телекомунікаційній сфері;
- інтеграція української ІКІ в європейські та світові системи колективної кібербезпеки.

Формування загроз для розвитку інформаційної безпеки України створюють такі чинники:

- зовнішні чинники — геополітичні зміни, гібридні війни, міжнародні інформаційні кампанії;
- внутрішні чинники — політична нестабільність, економічні труднощі, низький рівень медіаграмотності;
- технологічний розвиток — цифровізація та інновації, що поряд із перевагами несуть нові ризики;

- інформаційно-комунікаційна інфраструктура — фундамент сучасної держави, вразливість якої прямо впливає на рівень національної безпеки.

Для формування ефективної системи стратегічного управління необхідно враховувати взаємодію цих чинників, проводити постійний моніторинг і прогнозування, інтегрувати національні заходи із міжнародними ініціативами та створювати стійку систему реагування на загрози.

Контрольні питання

1. Які внутрішні чинники найбільше впливають на стан інформаційної безпеки?
2. Які зовнішні чинники формують інформаційні загрози?
3. Як глобалізація впливає на інформаційну безпеку держави?
4. Роль політичної нестабільності як внутрішнього чинника загроз.
5. Як діяльність іноземних спецслужб впливає на інформаційний простір?
6. Які соціальні процеси в державі сприяють виникненню інформаційних загроз?

Практичне питання

Мета

Проаналізувати фактори, що впливають на формування загроз.

Практичні завдання

1. Класифікувати внутрішні та зовнішні загрози за заданою схемою.
2. Проаналізувати приклад зовнішнього інформаційного впливу (взяти реальний кейс, наприклад, пропагандистська кампанія рф).
3. Підготувати матрицю ризиків (ймовірність × наслідки).

Питання для обговорення

Чому внутрішні загрози часто небезпечніші за зовнішні?

Тема 4. Об'єкти, суб'єкти та джерела інформаційних загроз

Інформаційна безпека держави неможлива без чіткого усвідомлення того, **які саме об'єкти потребують захисту, хто виступає суб'єктами загроз та звідки походять основні джерела небезпек**. У наукових дослідженнях, зокрема в дисертації С. Лисенка, наголошується, що стратегічне управління у сфері інформаційної безпеки повинно починатися з ідентифікації цих елементів, оскільки лише так можна розробити адекватні моделі протидії.

Об'єкти, суб'єкти та джерела інформаційних загроз утворюють **трикутник уразливості**, який визначає загальний стан інформаційного простору. Розглянемо ці складові більш детально.

Суб'єкти загроз — це ті актори, які свідомо або несвідомо створюють небезпеку для інформаційного простору держави. Їх можна поділити на кілька основних груп:

Державні актори:

- іноземні держави, які застосовують інформаційну агресію як складову гібридної війни;
- використання спецслужб, дипломатичних каналів, офіційних медіа для поширення вигідних наративів;
- приклади: кібератаки російських спецслужб на енергосистему України (2015–2017 рр.), інформаційні кампанії щодо дискредитації України у міжнародних медіа.

Недержавні приватні актори:

- транснаціональні корпорації, які контролюють значні масиви даних (Google, Meta, Microsoft);
- їхня діяльність може як сприяти розвитку інформаційної безпеки, так і створювати ризики, пов'язані з монополізацією інформаційного простору та залежністю від іноземних технологій.

Громадські організації та неурядові структури (НУО):

- частина НУО здійснює позитивну діяльність у сфері захисту прав людини та розвитку демократії;

- псевдо-НУО, що фінансуються іноземними центрами впливу та використовуються як інструмент “м’якої сили” для поширення вигідних наративів.

Індивідуальні актори та групи:

- хакери, кіберзлочинні угруповання, хактивісти;
- мотиви: політичні, фінансові, ідеологічні;
- приклади: зломи банківських систем, атаки на державні електронні реєстри, поширення шкідливого програмного забезпечення.

Таким чином, суб’єкти загроз є багатоманітними за природою, мотивацією та ресурсами.

Об’єкти — це ті елементи, на які спрямовані деструктивні інформаційні впливи. До них належать:

Інформаційні системи та мережі:

- державні та корпоративні IT-системи;
- банківські платформи, енергетичні мережі, транспортні системи;
- через уразливість вони стають мішенню для кібератак та диверсій.

Державні інституції:

- парламент, уряд, органи виконавчої влади;
- атаки на їх репутацію та легітимність через інформаційні кампанії;
- спроби отримання доступу до секретної інформації.

Засоби масової інформації (ЗМІ):

- традиційні ЗМІ (телебачення, радіо, друковані видання) та цифрові платформи;
- використовуються для маніпуляцій, поширення дезінформації, формування громадської думки.

Суспільна свідомість:

- масова аудиторія стає головною мішенню інформаційно-психологічних операцій;
- ворожі актори прагнуть створити атмосферу недовіри, паніки чи соціального розколу.

Критична інфраструктура:

- енергетика, транспорт, фінансовий сектор, охорона здоров'я;
- кібератаки на ці об'єкти можуть паралізувати роботу держави.

Отже, захист об'єктів інформаційної безпеки має охоплювати як **технічні системи**, так і **нематеріальні цінності** — громадську думку, легітимність держави, стабільність суспільства.

Джерела загроз — це конкретні форми або канали, з яких походить небезпека. Їх можна умовно поділити на зовнішні та внутрішні.

Зовнішні джерела:

- ворожі держави, які ведуть інформаційні війни;
- міжнародні терористичні організації, які здійснюють кібератаки;
- транснаціональні корпорації, здатні маніпулювати інформаційними потоками.

Внутрішні джерела:

- політична нестабільність, корупція, тіньові групи впливу;
- недостатня кібергігієна серед населення та працівників державних структур;
- використання медіа для політичної чи фінансової вигоди.

Конкретні форми загроз

Кіберзлочинність:

- атаки з метою фінансової вигоди (крадіжка даних, вимагання);
- створення бот-мереж для дестабілізації.

Дезінформація:

- поширення фейкових новин, маніпулятивних повідомлень у соціальних мережах;
- спотворення історичних фактів для підриву національної ідентичності.

Шпигунство:

- збір розвідувальної інформації через кібератаки;

- використання “інсайдерів” у державних і приватних структурах.

Кібертероризм:

- атаки на критичну інфраструктуру для створення паніки та хаосу;
- приклад: виведення з ладу енергетичних систем у зимовий період.

Таким чином, джерела загроз можуть мати різну природу, але всі вони спрямовані на **підрив стабільності держави та зниження її суверенітету**.

Для ефективного стратегічного управління важливо розглядати зазначені категорії у взаємодії:

- суб’єкти створюють чи використовують джерела загроз;
- їх дії спрямовані проти конкретних об’єктів інформаційної безпеки;
- результатом стає послаблення держави, втрата довіри громадян, порушення функціонування інфраструктури.

Приклад: суб’єкт — іноземна держава; джерело — кампанія дезінформації у соціальних мережах; об’єкт — суспільна свідомість; наслідок — зростання соціальної напруги, зниження довіри до влади.

Аналіз об’єктів, суб’єктів та джерел інформаційних загроз дає змогу глибше зрозуміти природу сучасних викликів у сфері інформаційної безпеки:

- суб’єкти: держави, приватні компанії, NGO, хакери та інші актори, які мають ресурси для створення загроз;
- об’єкти: інформаційні системи, мережі, державні інституції, ЗМІ, суспільна свідомість, критична інфраструктура;
- джерела: зовнішні й внутрішні чинники, що виявляються у формах кіберзлочинності, дезінформації, шпигунства й кібертероризму.

Усвідомлення цієї триєдності є передумовою для розроблення дієвої стратегії управління інформаційною безпекою. Саме тому стратегічні документи України повинні системно

враховувати взаємозалежність між об'єктами, суб'єктами та джерелами загроз.

Контрольні питання

1. Які є основні об'єкти інформаційної безпеки держави?
2. Хто є суб'єктами забезпечення інформаційної безпеки?
3. Які види інформаційних загроз є найпоширенішими?
4. Які державні органи відповідають за протидію інформаційним загрозам?
5. Як класифікуються джерела інформаційних загроз?
6. Хто може виступати недержавним джерелом інформаційної загрози.

Практичне питання

Мета

Закріпити знання про учасників інформаційних відносин і джерела загроз.

Практичні завдання

1. Визначити об'єкти інформаційної безпеки для трьох різних державних секторів (військовий, інформаційний, економічний).
2. Проаналізувати діяльність одного із суб'єктів забезпечення інфобезпеки (РНБО, Держспецзв'язку, СБУ).
3. Скласти класифікацію джерел загроз на основі реальних прикладів.

Питання для обговорення

Чи можуть громадяни бути водночас об'єктами й суб'єктами інформаційних загроз?

Тема 5. Інформаційний суверенітет: зміст, значення, загрози та шляхи захисту

В умовах глобалізації та цифрової трансформації питання **інформаційного суверенітету** стає одним із ключових у забезпеченні національної безпеки. Якщо у XX ст. держави прагнули насамперед гарантувати територіальну цілісність і військову безпеку, то у XXI ст. головним простором боротьби стає **інформаційне середовище**.

Для України, яка перебуває у стані гібридної війни, забезпечення інформаційного суверенітету — це не лише стратегічний виклик, а й запорука збереження державності, довіри суспільства до влади та міжнародної легітимності.

Інформаційний суверенітет — це здатність держави самостійно формувати, контролювати та захищати свій інформаційний простір, забезпечуючи незалежність у прийнятті рішень і недопущення деструктивного зовнішнього впливу.

У дисертаційних дослідженнях підкреслюється, що інформаційний суверенітет має **подвійну природу**:

1. Він є правом держави контролювати інформаційні процеси на своїй території.
2. Він є станом фактичної незалежності від зовнішніх впливів у сфері інформаційних технологій та комунікацій.

Ключові складові інформаційного суверенітету:

- контроль над національними інформаційними ресурсами;
- можливість формувати власну інформаційну політику;
- захист інфраструктури та даних від зовнішніх загроз;
- розвиток власних технологій та кадрів у сфері ІКТ.

Інформаційний суверенітет є критично важливим для сучасних держав з кількох причин:

Політична стабільність:

- незалежність у формуванні інформаційної політики дає змогу державі протидіяти пропаганді, дезінформації та маніпуляціям з боку іноземних суб'єктів;
- інформаційний суверенітет забезпечує легітимність державних інституцій та довіру громадян.

Економічний розвиток:

- контроль над інформаційними потоками є запорукою функціонування цифрової економіки;
- власні технології знижують залежність від імпорту програмного забезпечення й апаратних рішень.

Військова безпека:

- в умовах сучасних воєн інформаційний простір використовується як арена бойових дій;
- забезпечення суверенітету у сфері зв'язку, навігації та управління військами — це питання обороноздатності.

Культурна ідентичність:

- інформаційний суверенітет дає змогу державі захищати національні цінності, мову та культуру;
- він виступає бар'єром проти асиміляції через чужі інформаційні наративи.

Таким чином, інформаційний суверенітет — це не лише технічне питання, а й **стратегічна основа існування нації**.

У сучасному світі держава стикається з численними загрозами, що підривають її інформаційну незалежність:

Технологічна залежність від іноземного програмного забезпечення та апаратури:

- використання закордонних ОС (Windows, Android, iOS), офісних програм, телекомунікаційного обладнання (Huawei, Cisco) створює ризики вбудованих уразливостей;
- відсутність власних аналогів означає стратегічну залежність від зовнішніх постачальників.

Контроль над інформаційними потоками:

- соціальні мережі (Facebook, Twitter, TikTok) та пошукові системи (Google) перебувають під юрисдикцією іноземних держав;
- алгоритми цих платформ можуть маніпулювати громадською думкою всередині країни.

Кібернетичні загрози:

- зовнішні кібератаки на державні реєстри, енергосистему, транспорт;

- використання шкідливого програмного забезпечення для шпигунства.

Дезінформація та пропаганда:

- масові кампанії дезінформації, спрямовані на підрив довіри до влади;
- використання медіа та соціальних мереж для поширення вигідних агресору наративів.

Внутрішні ризики:

- корупція у сфері телекомунікацій і державних закупівель;
- використання ЗМІ олігархічними групами для власних політичних інтересів.

Отже, загрози інформаційному суверенітету походять як ззовні, так і зсередини, роблячи державу особливо вразливою.

Для гарантування інформаційного суверенітету держава має впроваджувати **системні політики**, які охоплюють кілька ключових напрямів:

Розвиток національних технологій:

- інвестування у власне програмне забезпечення та апаратні рішення;
- стимулювання ІТ-індустрії, створення сприятливого середовища для стартапів;
- підтримка проєктів у сфері штучного інтелекту, кіберзахисту, блокчейну.

Захист інформаційної інфраструктури:

- посилення кіберзахисту державних реєстрів і критичної інфраструктури;
- розвиток системи кіберрозвідки та моніторингу загроз;
- використання державно-приватного партнерства для кібербезпеки.

Контроль над інформаційним простором:

- прийняття законів, які регулюють діяльність іноземних платформ в Україні;
- забезпечення прозорості власності ЗМІ;
- створення національних соціальних мереж і платформ електронних послуг.

Освітні та культурні програми:

- підвищення рівня медіаграмотності населення;
- розвиток національного інформаційного контенту;
- підтримка української мови та культури в інформаційному просторі.

Міжнародна співпраця:

- участь у програмах НАТО та ЄС із колективної кібербезпеки;
- співпраця з міжнародними організаціями для протидії дезінформації;
- використання дипломатичних каналів для захисту національних інтересів в інформаційній сфері.

Інформаційний суверенітет — це один із фундаментів державності у XXI ст. Він визначає здатність держави залишатися незалежною у глобальному інформаційному середовищі, протидіяти зовнішнім і внутрішнім загрозам та гарантувати безпеку для своїх громадян.

Загрози інформаційному суверенітету мають багатовимірний характер: технологічна залежність, контроль іноземних корпорацій над інформаційними потоками, кібератаки, дезінформація та внутрішні політичні ризики.

Ефективна політика захисту передбачає розвиток національних технологій, зміцнення критичної інфраструктури, регулювання діяльності іноземних платформ, підвищення медіаграмотності населення та активну міжнародну співпрацю.

Для України питання інформаційного суверенітету є не лише науковою чи адміністративною категорією, а й **екзистенційним викликом**, від якого залежить майбутнє держави, її політична незалежність, культурна ідентичність і можливість інтегруватися до світової спільноти на рівних правах.

Контрольні питання

1. У чому полягає зміст інформаційного суверенітету держави?
2. Які основні загрози інформаційному суверенітету?

3. Як глобальні технологічні корпорації можуть впливати на інформаційний суверенітет?
4. Які засоби держава використовує для захисту інформаційного суверенітету?
5. Як міжнародне право регулює питання інформаційного суверенітету?
6. Чому інформаційний суверенітет є ключовим у період війни?

Практичне питання
Мета
Визначити механізми захисту інформаційного суверенітету.

Практичні завдання
1. Порівняти підходи до захисту інформаційного суверенітету США, ЄС та України.
2. Проаналізувати загрозу — "залежність від іноземних ІТ-платформ". Як вона впливає на суверенітет?
3. Розробити пропозиції щодо підсилення інформаційного суверенітету України (мінімум 5 пунктів).

Питання для обговорення
Чи є інформаційний суверенітет тотожним цифровому суверенітету?

Тема 6. Політичні, правові та нормативно-правові основи державної політики у сфері інформаційної безпеки

Інформаційна безпека — це не лише технічна чи організаційна категорія, а й насамперед **політико-правова проблема**, що потребує комплексного врегулювання. Державна політика у цій сфері має бути побудована на системі законів, нормативно-правових актів, міжнародних угод, а також на розгалуженій

структурі органів влади, відповідальних за формування й реалізацію політики інформаційної безпеки.

У дисертаційних дослідженнях стратегічного управління інформаційною безпекою підкреслюється, що правова основа є фундаментом для всіх інших механізмів. Без законодавчої чіткості й політичної волі будь-які заходи у сфері інформаційного захисту залишаються фрагментарними й малоефективними.

Правова база інформаційної безпеки України формується на кількох рівнях:

Конституція України:

- стаття 17 визначає захист суверенітету й територіальної цілісності як головний обов'язок держави;
- стаття 34 гарантує свободу слова та доступ до інформації, але водночас передбачає можливість обмежень в інтересах національної безпеки.

Основні закони України:

- Закон "Про національну безпеку України" (2018 р.) — визначає інформаційну безпеку як один з пріоритетних напрямів державної політики;
- Закон "Про інформацію" (1992 р., зі змінами) — встановлює правові засади доступу, зберігання й поширення інформації;
- Закон "Про доступ до публічної інформації" (2011 р.) — закріплює механізми забезпечення відкритості влади;
- Закон "Про захист інформації в інформаційно-телекомунікаційних системах" (2005 р.) — регламентує порядок захисту даних в IT-середовищі;
- Закон "Про телекомунікації" (2003 р.) — визначає правові основи діяльності операторів зв'язку;
- Закон "Про основні засади забезпечення кібербезпеки України" (2017 р.) — закріплює організаційно-правові механізми кіберзахисту.

Підзаконні акти та нормативи:

- Укази Президента про введення санкцій проти ворожих інформаційних ресурсів;

- Постанови Кабінету Міністрів щодо захисту критичної інфраструктури;
- нормативні документи Державної служби спеціального зв'язку та захисту інформації (НД ТЗІ серії 2.5, 3.7).

Міжнародні угоди:

- Будапештська конвенція про кіберзлочинність (2001 р.);
- співпраця з НАТО у рамках Програми розширених можливостей та спільних навчань з кіберзахисту;
- Угода про асоціацію між Україною та ЄС (2014 р.) — гармонізація з європейським правом у сфері захисту персональних даних (GDPR);
- документи ООН та ОБСЄ щодо безпеки у сфері ІКТ.

Ефективна політика у сфері інформаційної безпеки потребує чіткої системи органів, відповідальних за її реалізацію.

Рада національної безпеки і оборони України (РНБО):

- координує та контролює діяльність у сфері національної безпеки;
- приймає ключові рішення щодо реагування на загрози інформаційному простору.

Державна служба спеціального зв'язку та захисту інформації (ДССЗЗІ):

- відповідальна за технічний захист інформації та кіберзахист;
- розробляє нормативні документи у сфері ТЗІ.

Служба безпеки України (СБУ):

- протидіє кіберзлочинності та шпигунству;
- захищає державні інформаційні ресурси.

Міністерство оборони та Генеральний штаб ЗСУ:

Відповідають за кібероборону, розвідку і протидію інформаційним атакам у військовій сфері.

Міністерство цифрової трансформації:

- реалізує політику цифровізації ("Дія");
- відповідає за розвиток електронних сервісів та їх захист.

Інші суб'єкти:

- Національний банк України — захист фінансових систем;

- оператори телекомунікацій — кіберзахист мереж;
- громадські організації та приватний сектор — учасники державно-приватного партнерства.

Сучасна держава має врегульовувати **інформаційні процеси** так, щоб одночасно забезпечувати **свободу слова і захист національних інтересів**.

Засоби масової інформації:

- Закон "Про телебачення і радіомовлення" регламентує діяльність телеканалів і радіостанцій;
- Законодавство про медіа (2022 р.) впроваджує європейські стандарти та створює єдиний регуляторний орган;
- важливим елементом є прозорість фінансування та власності ЗМІ.

Інтернет і цифрові платформи:

- законодавство щодо захисту персональних даних;
- регулювання діяльності інтернет-провайдерів та платформ (заборона доступу до ресурсів, які поширюють пропаганду чи дезінформацію);
- питання "цифрового суверенітету" — баланс між відкритим інтернетом і необхідністю блокування ворожих ресурсів.

Інформаційна діяльність громадян:

- гарантоване право на доступ до інформації;
- обмеження щодо державної таємниці та персональних даних;
- відповідальність за поширення фейків, заклики до насильства, екстремізм.

Найскладнішим викликом у формуванні правової політики є знаходження **золотої середини (балансу)** між двома протилежними **цінностями: безпекою та свободою.**

Свобода слова і доступ до інформації:

- є основою демократичного суспільства;
- дає змогу громадянам контролювати владу, брати участь у політичних процесах;

Безпека держави та суспільства:

- вимагає обмеження доступу до шкідливого контенту;
- необхідна для протидії пропаганді, тероризму, дезінформації.

У демократичних державах баланс досягається завдяки:

- прозорим законодавчим механізмам;
- незалежним судовим органам, які вирішують спірні питання;
- суспільному контролю за владою та медіа.

Для України, яка перебуває у стані гібридної війни, цей баланс є особливо складним. З одного боку, необхідно блокувати ворожі інформаційні ресурси, а з іншого — не допустити надмірного обмеження свободи слова.

Політичні, правові та нормативно-правові основи державної політики є фундаментом системи інформаційної безпеки. Вони визначають правила гри в інформаційному просторі, встановлюють баланс між демократичними правами та потребами безпеки, а також окреслюють відповідальних суб'єктів.

- **Законодавча база** України поступово гармонізується з міжнародними стандартами (ЄС, НАТО, ООН).
- **Структура управління** включає центральні органи (РНБО, СБУ, ДССЗЗІ, Мінцифри) та приватних учасників.
- **Регулювання ЗМІ та інтернету** спрямоване на захист від дезінформації, пропаганди та кіберзагроз.
- **Баланс між свободою і безпекою** залишається складним викликом, але саме він визначає демократичний характер державної інформаційної політики.

У майбутньому державна політика повинна поєднувати **посилення правового захисту** та **розвиток демократичних інститутів**, щоб гарантувати і національну безпеку, і свободу слова.

Контрольні питання

1. Які правові акти формують основу інформаційної безпеки України?

2. Які політичні чинники впливають на формування державної інформаційної політики?
3. Які міжнародні нормативні документи регулюють сферу інформаційної безпеки?
4. Яка роль Конституції України у формуванні політики інформаційної безпеки?
5. Як взаємодіють політичні інститути у забезпеченні інформаційної безпеки?
6. Які є проблеми чинної нормативно-правової бази України у цій сфері?

Практичне питання
Мета
Розібрати законодавчу базу та політичні механізми.

Практичні завдання
1. Проаналізувати Закон України "Про національну безпеку".
2. Побудувати схему нормативно-правового забезпечення інфобезпеки.
3. Виявити прогалини в чинному законодавстві (мінімум три).

Питання для обговорення
Чи потрібно приймати окремий Кодекс інформаційної безпеки?

Тема 7. Принципи державного управління інформаційною безпекою

Будь-яка сфера державної політики має спиратися на **принципи управління** — узагальнені правила та підходи, що визначають характер діяльності органів влади. У сфері інформаційної безпеки ці принципи набувають особливого значення, оскільки йдеться про захист стратегічних інтересів держави, її суверенітету, стабільності суспільства та прав громадян.

Як показують матеріали дисертації з питань стратегічного управління інформаційною безпекою, система принципів у цій сфері є багаторівневою. Вона включає як **загальні принципи державного управління**, так і **специфічні положення**, які діють в умовах війни, надзвичайного стану чи інших кризових ситуацій. Окрему групу становлять принципи **адаптивності та стійкості**, що визначають здатність держави ефективно реагувати на нові загрози.

Загальні принципи відображають основоположні норми, які застосовуються до всієї системи управління, незалежно від політичної чи безпекової ситуації.

Принцип законності:

- усі заходи держави у сфері інформаційної безпеки мають ґрунтуватися на Конституції та законах України;
- законність забезпечує легітимність дій органів влади й запобігає зловживанням;
- приклад: регулювання діяльності ЗМІ має поєднувати захист від дезінформації з гарантіями свободи слова.

Принцип ефективності:

- держава повинна раціонально використовувати ресурси для досягнення максимального рівня захисту;
- це означає розробку стратегій, які забезпечують реальні результати, а не декларативні гасла;
- приклад: створення національних центрів моніторингу кіберзагроз, які забезпечують оперативне реагування.

Принцип комплексності:

- інформаційна безпека охоплює політичні, економічні, технічні, соціальні та культурні аспекти;
- управління має бути багатовимірним, інтегрувати різні сектори держави;
- приклад: одночасна боротьба з дезінформацією, кіберзлочинністю та технологічною залежністю.

Принцип пропорційності:

- заходи із забезпечення безпеки мають бути співмірними із загрозами;

- надмірні обмеження свободи слова чи доступу до інформації можуть підривати демократичні основи держави;
- приклад: блокування інтернет-ресурсів, що поширюють пропаганду, повинно мати чітке правове обґрунтування.

Принцип відкритості та прозорості:

- державна політика у сфері інформаційної безпеки має бути зрозумілою для суспільства;
- це забезпечує довіру громадян і формує стійкість до ворожої пропаганди.

Принцип пріоритетності національних інтересів:

- будь-які міжнародні домовленості або внутрішні рішення мають узгоджуватися з національними інтересами;
- це передбачає розвиток власних технологій, захист національної культури та мови.

Військові конфлікти, гібридні війни та надзвичайні ситуації вимагають від держави застосування **специфічних принципів**, що відрізняються від звичайних демократичних умов.

Принцип пріоритету національної безпеки:

- у кризовий час свобода інформації може частково обмежуватися задля захисту життя громадян і функціонування держави;
- приклад: обмеження роботи певних телеканалів, що поширюють ворожу пропаганду під час війни.

Принцип централізації управління:

- в умовах війни управлінські рішення мають прийматися швидко й узгоджено;
- це потребує концентрації повноважень у РНБО, Генштабі, уряді.

Принцип оперативності:

- реакція на загрози має бути негайною;
- затримка навіть у кілька годин у випадку кібератаки може призвести до серйозних наслідків.

Принцип інформаційної мобілізації:

- держава повинна мобілізувати всі доступні ресурси — медіа, громадські організації, освітні установи для протидії ворожій пропаганді;

- приклад: інформаційні кампанії з роз'яснення дій влади та підтримки населення під час воєнного стану.

Принцип превентивності:

- ключовим стає не лише реагування, а й попередження загроз;
- системи раннього виявлення дезінформації, кіберзахисту, стратегічних комунікацій мають працювати на випередження.

В умовах глобальних змін інформаційного середовища держава повинна будувати політику інформаційної безпеки так, щоб вона залишалася актуальною та ефективною навіть за непередбачуваних викликів.

Принцип адаптивності:

- управлінські механізми мають змінюватися залежно від характеру загроз;
- приклад: адаптація до нових технологій (штучний інтелект, квантові обчислення, блокчейн);
- адаптивність означає здатність швидко оновлювати законодавство, стандарти та методи роботи.

Принцип стійкості:

- стійкість полягає у здатності держави витримати інформаційні атаки та швидко відновитися після них;
- це включає резервування критичних систем, дублювання інформаційних ресурсів, стратегії кібервідновлення.

Принцип багаторівневої взаємодії:

- стійкість можлива лише за умов ефективної взаємодії держави, бізнесу та громадянського суспільства;
- наприклад, державні центри кіберзахисту мають співпрацювати з приватними ІТ-компаніями.

Принцип навчання та інноваційності:

- адаптивність неможлива без постійного навчання фахівців і розвитку науки;
- Інноваційні підходи до виявлення загроз (машинне навчання для ідентифікації фейків) підвищують ефективність управління.

Приклади застосування принципів у практиці України:

- законність і пропорційність: блокування російських соціальних мереж (“ВКонтакте”, “Одноклассники”) у 2017 р. було обґрунтоване загрозами національній безпеці;
- комплексність: створення Міністерства цифрової трансформації, яке одночасно відповідає за цифровізацію й кіберзахист;
- оперативність і централізація: реагування РНБО на кібератаки в 2022 р., коли були швидко введені санкції проти ворожих ІТ-компаній;
- адаптивність і стійкість: перехід багатьох українських державних реєстрів у хмарні дата-центри ЄС під час активної фази війни.

Принципи державного управління інформаційною безпекою формують **методологічну основу** для політики України в умовах сучасних викликів:

- загальні принципи (законність, ефективність, комплексність, пропорційність, відкритість) визначають стабільність і демократичний характер управління;
- специфічні принципи (централізація, оперативність, превентивність, мобілізація) дають змогу ефективно діяти в умовах війни та надзвичайного стану;
- принципи адаптивності та стійкості забезпечують здатність держави зберігати керованість і захищеність у непередбачуваних умовах.

Система цих принципів дає змогу Україні будувати ефективне стратегічне управління інформаційною безпекою, що є ключовим фактором виживання та розвитку у XXI ст.

Контрольні питання

1. Які принципи лежать в основі державного управління інформаційною безпекою?
2. Що означає принцип пріоритетності національних інтересів?

3. У чому полягає принцип комплексності управління безпекою?
4. Як реалізується принцип відповідальності суб'єктів?
5. Що означає принцип збалансованості державного втручання?
6. Як забезпечується принцип законності в управлінні інформаційною безпекою?

Практичне питання
Мета
Опанувати базові принципи державного управління.
Практичні завдання
1. Створити перелік принципів управління з їх прикладним застосуванням.
2. Проаналізувати порушення принципів у конкретному кейсі (наприклад, неефективне реагування державного органу).
3. Запропонувати систему контролю дотримання принципів.

Питання для обговорення
Які принципи найважче реалізувати в умовах війни?

Тема 8. Стратегічне планування інформаційної безпеки в умовах миру, надзвичайного стану та війни

Стратегічне планування є ключовим елементом державного управління у сфері інформаційної безпеки. Воно забезпечує **системність дій**, орієнтацію на довгострокові цілі та підготовку до можливих кризових і воєнних сценаріїв. У сучасному світі, де інформаційні технології стали як рушієм розвитку, так й інструментом війни, планування інформаційної безпеки є не лише управлінським завданням, а й **екзистенційною потребою для держави**.

Матеріали дисертаційних досліджень з проблем стратегічного управління інформаційною безпекою наголошують: від якості планування залежить не лише стійкість інформаційної інфраструктури, а й здатність держави вистояти у глобальній конкуренції, протистояти гібридним загрозам і забезпечити демократичний розвиток.

Сценарії стратегічного планування: мир, криза, війна. У сфері інформаційної безпеки надзвичайно важливо враховувати різні сценарії розвитку подій. Кожен з них вимагає специфічних підходів до планування.

Сценарій миру:

- головний акцент робиться на розвиток інформаційного суспільства;
- пріоритет — створення інноваційної цифрової економіки, підтримка наукових досліджень, розвиток національних IT-компаній;
- у сфері безпеки — формування превентивних механізмів, розвиток культури кібергігієни, підвищення медіаграмотності населення;
- важливим завданням є гармонізація національної політики з міжнародними стандартами (NATO, EU, ISO, NIST).

Сценарій кризи чи надзвичайного стану:

- причини: масштабні кібератаки, техногенні катастрофи, внутрішні заворушення, економічні шоки;
- пріоритети:
  - захист критичної інформаційної інфраструктури;
  - забезпечення безперебійної роботи державних реєстрів і систем управління;
  - контроль за поширенням панічної чи деструктивної інформації;
  - мобілізація державних і приватних ресурсів для ліквідації наслідків кризи.

Сценарій війни:

- інформаційний простір стає полем бою;
- пріоритети:

– стратегічні комунікації, контрпропаганда, інформаційна мобілізація населення;
– кібероборона, захист військових і урядових систем управління;
– перенесення інформаційних ресурсів у безпечні середовища (резервні дата-центри, хмарні технології);
– міжнародна співпраця для колективної безпеки.

Таким чином, стратегічне планування має бути гнучким і багатосценарним, передбачаючи як розвиток у мирний час, так і дії у кризових та воєнних умовах.

Стратегічні цілі, цільові показники та KPI. Планування інформаційної безпеки повинно спиратися на чіткі цілі та індикатори ефективності.

Стратегічні цілі:

- забезпечення стійкості інформаційної інфраструктури;
- захист суверенітету інформаційного простору;
- протидія дезінформації та інформаційним операціям;
- розвиток національних технологій у сфері ІКТ;
- інтеграція в європейську та світову систему кібербезпеки.

Цільові показники:

- рівень захищеності державних інформаційних ресурсів (у відсотках);
- кількість кіберінцидентів, яким вдалося запобігти;
- частка національного софту в державному секторі;
- кількість навчальних програм і підготовлених кадрів у сфері ІБ;
- рівень довіри громадян до державних інформаційних ресурсів.

KPI (ключові показники ефективності):

- середній час реагування на кіберінциденти;
- кількість проведених навчань і тренувань з кіберзахисту;
- обсяг інвестицій у розвиток національних технологій;
- відсоток гармонізованих з міжнародними стандартами нормативних документів.

Таким чином, стратегічне планування має бути вимірюваним: не декларації, а конкретні показники дають змогу оцінити прогрес.

Без ресурсного забезпечення жодна стратегія не може бути реалізована. **Планування у сфері інформаційної безпеки** має враховувати:

1. **Фінансові ресурси:**
   - державний бюджет (статті на кіберзахист, розвиток цифрових сервісів);
   - міжнародна допомога (гранти ЄС, НАТО, Світового банку);
   - державно-приватне партнерство.
2. **Кадрові ресурси:**
   - підготовка фахівців з кібербезпеки у вишах;
   - створення центрів підвищення кваліфікації;
   - стимулювання молодих спеціалістів залишатися в Україні.
3. **Технологічні ресурси:**
   - розвиток національних дата-центрів і хмарних сервісів;
   - створення власного програмного забезпечення;
   - впровадження сучасних систем моніторингу й кіберзахисту.
4. **Організаційні ресурси:**
   - координація діяльності органів влади (РНБО, СБУ, ДССЗЗІ, Мінцифри);
   - взаємодія держави з приватним сектором;
   - створення кризових штабів для реагування на інциденти.

Ефективність стратегічного планування залежить від того, наскільки **раціонально розподілені ресурси** між різними напрямами.

Для розуміння практичного виміру стратегічного планування важливо розглянути **приклади** українського та міжнародного досвіду.

Український досвід:

- Стратегія національної безпеки України (2020 р.) — визначає інформаційну безпеку як пріоритетну складову;
- Кіберстратегія України (2021 р.) — спрямована на розвиток національної системи кібербезпеки, захист критичної інфраструктури;
- Доктрина інформаційної безпеки України (2017 р.) — закріпила засади протидії дезінформації та інформаційній агресії;
- Закон "Про основні засади забезпечення кібербезпеки України" (2017 р.) — визначив організаційно-правову структуру кіберзахисту.

Міжнародний досвід:

- Стратегія кібербезпеки ЄС (2020 р.) — акцент на колективній безпеці, розвиток цифрового суверенітету Європи;
- Доктрина НАТО з кібероборони — визначає кіберпростір як окремий домен воєнних дій;
- Національна стратегія кібербезпеки США (2023 р.) — підкреслює партнерство держави та приватного сектору, пріоритет захисту критичної інфраструктури;
- Tallinn Manual (2017 р.) — міжнародний науковий документ, що регламентує застосування міжнародного права у кіберконфліктах.

Порівняння показує, що Україна рухається у напрямі гармонізації з міжнародними практиками, однак потребує більшої ресурсної бази та глибшої інтеграції з колективними механізмами безпеки.

Стратегічне планування інформаційної безпеки є комплексним процесом, який враховує **різні сценарії розвитку подій** — від мирного часу до війни:

- у мирний час акцент робиться на розвитку цифрової економіки й гармонізації з міжнародними стандартами;
- у кризових ситуаціях — на мобілізації ресурсів та забезпеченні безперебійної роботи державних систем;

- у воєнних умовах — на інформаційній мобілізації, кібероборoні та міжнародній кооперації.

Ефективність планування визначається чіткими **стратегічними цілями**, **показниками та KPI**, а також реалістичним плануванням ресурсів.

Українські та міжнародні стратегії демонструють, що успішне забезпечення інформаційної безпеки можливе лише за умови **поєднання внутрішніх реформ, ресурсної мобілізації та міжнародної співпраці**.

Отже, стратегічне планування у сфері інформаційної безпеки є не тільки управлінським інструментом, а й **ключовим чинником виживання та розвитку держави у XXI ст**.

Контрольні питання

1. Чим відрізняється планування в умовах війни від планування у мирний час?
2. Які інструменти використовуються під час стратегічного планування у кризових умовах?
3. Які органи координують планування у період надзвичайного стану?
4. Як змінюються пріоритети під час військової агресії?
5. Які міжнародні стандарти враховують під час планування?
6. Як оцінюється ефективність стратегічних планів інформаційної безпеки?

Практичне питання

Мета

Вивчити механізми стратегічного планування з урахуванням режимів держави.

Практичні завдання

1. Порівняльний аналіз стратегічних планів у різних режимах (мир – НС – війна).
2. Створити сценарний прогнозу загроз в умовах війни.

3. Скласти план реагування державного органу у разі кібератаки.

Питання для обговорення

Чи повинні плани мирного часу бути максимально наближеними до воєнних?

Тема 9. Механізми реагування на інформаційні загрози та кризові ситуації

Інформаційні загрози стали одним із головних викликів для сучасних держав. Вони виникають у вигляді **кібератак, кампаній дезінформації, інформаційно-психологічних операцій**, а також як наслідок кризових ситуацій — військових конфліктів, терористичних актів чи техногенних катастроф.

Для України, яка вже понад десятиліття перебуває під постійним інформаційним та кібертиском з боку рф, питання ефективних механізмів реагування є не лише теоретичним, а й практичним завданням національної безпеки.

У цій лекції ми розглянемо ключові елементи системи реагування: моніторинг і розвідку, механізми раннього попередження, оперативні заходи, координацію між органами, протидію дезінформації та інформаційним операціям, а також правові інструменти відповідальності та санкцій.

Моніторинг інформаційного простору:

- систематичне відстеження традиційних і цифрових ЗМІ, соціальних мереж, блогосфери;
- використання інструментів Big Data та штучного інтелекту для виявлення “аномальних” інформаційних кампаній;
- участь державних і недержавних структур у спільному моніторингу (наприклад, ініціативи StopFake).

Розвідка в інформаційній сфері:

- кіберрозвідка (збір інформації про потенційні загрози в мережі);

- використання відкритих джерел (OSINT) для аналізу інформаційних потоків;
- співпраця з міжнародними партнерами (NATO StratCom, Європейський центр передового досвіду з протидії гібридним загрозам).

Раннє попередження:

- створення системи індикаторів, які дають змогу завчасно виявляти кампанії дезінформації або підготовку кібератак;
- приклад: відстеження бот-мереж, які активізуються перед виборами;
- інтеграція систем раннього попередження у структуру РНБО та ДССЗЗІ.

Таким чином, моніторинг і розвідка формують **базовий рівень превентивної безпеки**, без якого неможлива ефективна реакція.

Система реагування: оперативні заходи та координація між органами.

Оперативні заходи:

- технічна протидія: блокування атакованих IP-адрес, відключення заражених сегментів мережі, ізоляція вірусів;
- інформаційна протидія: офіційні роз'яснення, спростування фейкових новин, публічні заяви державних органів;
- кризові комунікації: швидке інформування населення для запобігання паніці.

Координація між органами влади:

- РНБО: ухвалення стратегічних рішень у кризових ситуаціях;
- СБУ: протидія шпигунству, кіберзлочинності, терористичним загрозам;
- ДССЗЗІ: технічний захист інформаційних систем;
- Мінцифра: розвиток цифрових сервісів і кіберзахист державних реєстрів;
- Національний банк України: безпека фінансових систем.

В умовах кризи потрібна **централізація управління** та єдина вертикаль прийняття рішень.

Міжнародна координація:

- співпраця з НАТО (кіберцентри у Таллінні, Ризі);
- обмін інформацією в рамках ЄС та ООН;
- використання механізмів міжнародних санкцій проти агресорів.

Інформаційні операції та протидія дезінформації

Ворожі інформаційні операції:

- формування хибних наративів (наприклад, про "нелегітимність" української державності);
- використання deepfake-відео для дискредитації керівництва держави;
- маніпуляції фактами з історії, політики та соціальної сфери.

Механізми протидії дезінформації:

- фактчекінг: незалежні організації, що перевіряють достовірність інформації;
- офіційні комунікації: публікація швидких спростувань у державних каналах;
- освітні програми: медіаграмотність населення, навчання критичному мисленню;
- алгоритмічні рішення: співпраця з платформами (Facebook, Google, Twitter) для маркування фейкових новин.

Контрнаративи:

- держава має не лише спростовувати, а й створювати власні інформаційні наративи;
- приклад: кампанії з підкреслення ролі України як демократичної держави у європейському просторі.

Кримінальна та адміністративна відповідальність:

- відповідальність за поширення державної таємниці, кіберзлочини, шпигунство;
- адміністративні санкції за поширення фейків, що дестабілізують суспільство.

Санкційна політика:

- блокування доступу до іноземних ресурсів, що поширюють пропаганду;
- персональні санкції проти осіб та організацій, причетних до інформаційної агресії;
- обмеження на діяльність іноземних корпорацій, що сприяють поширенню ворожого контенту.

Міжнародно-правові механізми:

- використання Будапештської конвенції проти кіберзлочинності;
- застосування норм міжнародного гуманітарного права (Tallinn Manual) до інформаційних війн;
- залучення міжнародних судів для притягнення до відповідальності держав-агресорів.

Приклади з практики України:

- 2017 р. — NotPetya: масштабна кібератака на державні установи та бізнес. Реакція включала ізоляцію мереж, міжнародну співпрацю з Microsoft та НАТО;
- 2022 р. — масові атаки перед повномасштабним вторгненням: блокування урядових сайтів, масова дезінформація про "капітулювання" влади. Реакція — централізовані повідомлення від уряду та президента, перенесення реєстрів у хмарні дата-центри за кордон;
- 2023–2024 рр. — кампанії дезінформації у соцмережах: робота бот-мереж, поширення фейків про економічний стан України. Відповідь — блокування акаунтів, активність фактчекінгових організацій.

Механізми реагування на інформаційні загрози та кризові ситуації формують **операційний рівень державної політики у сфері інформаційної безпеки**:

- моніторинг, розвідка та раннє попередження дають змогу своєчасно ідентифікувати загрози;
- протидія дезінформації та інформаційним операціям передбачає не лише спростування, а й створення власних позитивних наративів;

- система реагування забезпечує технічну, організаційну та комунікаційну протидію загрозам;
- юридична відповідальність і санкції гарантують невідворотність покарання для порушників і зміцнюють правову основу безпеки.

Для України важливо розвивати комплексну модель реагування, інтегровану у міжнародну систему колективної безпеки, щоб ефективно протистояти як внутрішнім, так і зовнішнім інформаційним викликам.

Контрольні питання

1. Що таке механізм реагування в інформаційній сфері?
2. Які інституції відповідають за оперативне реагування?
3. Які інструменти використовують для нейтралізації інформаційних атак?
4. У чому полягає роль моніторингових центрів?
5. Як здійснюється оцінювання наслідків інформаційної кризи?
6. Які етапи включає система кризового реагування?

Практичне питання

Мета

Опанувати інструменти кризового реагування.

Практичні завдання

1. Розробити алгоритм реагування на фейкову інформаційну кампанію.
2. Проаналізувати модель реагування НАТО/ЄС на інформаційні кризи.
3. Створити систему індикаторів інформаційної кризи.

Питання для обговорення

Наскільки важливим є фактор часу в інформаційному реагуванні?

Тема 10. Інформаційна війна, дезінформація, психологічні операції як інструменти загроз

Інформаційне середовище стало ключовим полем боротьби у XXI ст. Якщо в минулому держави змагалися переважно у військовій, економічній чи дипломатичній сферах, то сьогодні дедалі частіше вирішальною стає здатність контролювати інформаційні потоки, впливати на свідомість населення й формувати вигідні наративи.

У дисертаційних дослідженнях із питань стратегічного управління інформаційною безпекою зазначається, що **інформаційна війна** — це не лише допоміжний інструмент традиційних воєн, а й самостійна форма конфлікту, здатна підривати держави без застосування зброї. Її складовими є **дезінформація та психологічні операції**, що здійснюють цілеспрямований вплив на суспільство, військових і політичні еліти.

Інформаційна війна — це сукупність заходів, спрямованих на досягнення політичних, військових або економічних цілей шляхом впливу на інформаційні системи, комунікаційні канали, суспільну свідомість та управлінські рішення противника.

Основні характеристики інформаційної війни:

- ведеться постійно як у мирний час, так і під час збройних конфліктів;
- поєднує кібероперації, інформаційно-психологічні впливи, пропаганду й маніпуляції;
- націлена не лише на військових, а й на цивільне населення;
- використовує сучасні технології: інтернет, соціальні мережі, штучний інтелект, Big Data.

Україна є прикладом держави, проти якої системно ведеться інформаційна війна. Починаючи з 2014 р., росія здійснює масштабні інформаційні операції: дискредитація уряду, створення панічних настроїв, поширення фейків про ЗСУ, використання тролів та ботів у соцмережах.

Види психологічних операцій. Психологічні операції (ПсО) є складовою інформаційних воєн, які впливають на психіку та поведінку цільових аудиторій.

За об'єктом впливу:

- проти військових — поширення деморалізуючої інформації, фейків про втрати, недовіру до командування;
- проти цивільного населення — створення паніки, розколу, зневіри у власній державі;
- проти міжнародної спільноти — формування образу України як "нестабільної держави", щоб знизити підтримку з боку партнерів.

За методами впливу:

- пропаганда — систематичне поширення ідеологічних меседжів;
- маніпуляція фактами — використання правдивої інформації у спотвореному контексті;
- фейки та дезінформація — вигадані новини, що видаються за реальні;
- чутки — навмисно поширювані неперевірені повідомлення;
- залякування — перебільшення небезпеки, створення відчуття безвиході.

За рівнем організації:

- тактичні ПсО — спрямовані на короткостроковий результат (наприклад, вплив на рішення військових підрозділів);
- стратегічні ПсО — мають на меті довготривалі зміни у свідомості населення (наприклад, формування образу "братніх народів" для виправдання агресії).

Таким чином, психологічні операції — це багатогранний інструмент, що працює одночасно у різних площинах: від фронту до світової інформаційної арени.

Дезінформація — це ключовий елемент інформаційної війни. Її створення і поширення відбувається за чіткою технологією.

Механізм вироблення дезінформації:

- створення фейкових новинних ресурсів;

- використання “псевдоекспертів” та підконтрольних журналістів;
- генерація фото- та відеофейків (deepfake-технології).

Поширення дезінформації:

- масове використання бот-мереж і тролів у соцмережах;
- запуск “вірусного контенту”, який активно поширюється самими користувачами;
- використання мікротаргетингу — персоналізованих повідомлень для різних груп населення.

Закріплення дезінформації:

- повторення одного й того ж меседжу у різних каналах (телебачення, інтернет, радіо, чутки);
- підкріплення фейків “напівправдою” — включення у вигаданий сюжет реальних фактів для правдоподібності;
- використання “експертних думок” для легітимації неправдивої інформації.

Приклад: кампанії дезінформації про “нелегітимність української влади”, які поширюються як у внутрішньому інформаційному просторі, так і через міжнародні медіа.

Контрзаходи. Ефективна протидія інформаційній війні, дезінформації та психологічним операціям вимагає комплексного підходу, де поєднуються **освітні, державні та міжнародні заходи**.

Критичне мислення:

- формування навичок аналізу інформації серед громадян;
- пошук першоджерел, перевірка фактів, аналіз контексту;
- приклад: навчальні курси з медіаграмотності для школярів та студентів.

Медіаграмотність:

- освітні програми, спрямовані на розуміння механізмів роботи ЗМІ;
- вміння відрізняти новини від коментарів чи маніпуляцій;

- використання платформ фактчекінгу (StopFake, VoxCheck).

Державні механізми:

- створення центрів стратегічних комунікацій;
- блокування ресурсів, що поширюють ворожу пропаганду;
- регулювання діяльності соціальних мереж, вимога прозорості алгоритмів;
- санкційна політика проти осіб та компаній, які займаються інформаційною агресією.

Міжнародна співпраця:

- участь у програмах НАТО та ЄС щодо протидії гібридним загрозам;
- обмін досвідом та інформацією з партнерами;
- використання міжнародного права для притягнення агресорів до відповідальності.

Український досвід:

- 2014–2022 рр.: масові кампанії російської дезінформації, спрямовані на делегітимізацію української влади та ЗСУ;
- 2022 р.: під час повномасштабного вторгнення поширювалися фейки про "капітулювання" та "втечу керівництва". Реакція — оперативні звернення Президента та уряду, які зруйнували дезінформаційні меседжі;
- освітні ініціативи: введення у школах курсу з медіаграмотності, розвиток громадських організацій фактчекінгу;
- міжнародна підтримка: співпраця з ЄС у сфері протидії дезінформації, участь у стратегічних комунікаційних ініціативах НАТО.

Інформаційна війна є комплексним викликом, що поєднує кібероперації, дезінформацію та психологічні операції. Її головна мета — послабити державу зсередини, підірвати довіру до влади, деморалізувати населення та створити вигідні умови для агресора.

- **Поняття інформаційної війни** відображає нову реальність міжнародних відносин, де зброєю стає інформація.

- **Психологічні операції** — це системний інструмент впливу на свідомість і поведінку людей.
- **Дезінформація** виробляється за чіткою технологією: створення, поширення, закріплення.
- **Контрзаходи** мають бути багаторівневими: розвиток критичного мислення та медіаграмотності, державні та міжнародні політики, санкційний тиск.

Для України протидія інформаційній війні є питанням **національного виживання**, а не лише інформаційної політики. Саме тому стратегічне управління у цій сфері повинно поєднувати освітні реформи, розвиток технологій, зміцнення інституцій та активну міжнародну співпрацю.

Контрольні питання

1. Які ознаки інформаційної війни?
2. У чому полягає сутність дезінформації?
3. Які цілі переслідують психологічні операції?
4. Як класифікуються методи інформаційної війни?
5. Які механізми протидії дезінформації?
6. Як інформаційна війна впливає на демократичні інститути?

Практичне питання

Мета

Сформувати розуміння методів і засобів інформаційної війни.

Практичні завдання

1. Аналіз інформаційної операції рф (обрати відомий приклад, наприклад, МН-17, “біолабораторії”, “зовнішнє управління”).
2. Визначити інструменти дезінформації у медіатексті (приклад дається викладачем).
3. Скласти план протидії психологічній операції.

Питання для обговорення

Чим дезінформація відрізняється від пропаганди?

Тема 11. Цифровізація, ІКТ-інфраструктура та її роль

Цифровізація стала однією з найпотужніших тенденцій розвитку людства у XXI ст. Вона охоплює всі сфери — економіку, політику, соціальні відносини, культуру, безпеку. Інформаційно-комунікаційні технології (ІКТ) є основою цього процесу: вони забезпечують збирання, обробку, передавання й зберігання інформації, створюють нові можливості для розвитку та водночас породжують нові ризики.

У дисертаційних дослідженнях стратегічного управління інформаційною безпекою держави підкреслюється, що роль ІКТ-інфраструктури є подвійною: з одного боку, вона є **рушієм інновацій**, а з іншого — **вразливим елементом**, який може стати мішенню для інформаційних атак. Тому розуміння структури сучасних технологій, ризиків та шляхів захисту є фундаментом національної політики інформаційної безпеки.

Сучасні ІКТ-технології

Основні напрями розвитку:

- хмарні обчислення (Cloud Computing) — забезпечують гнучкість та масштабованість ІТ-послуг;
- інтернет речей (IoT) — мережа з'єднаних між собою пристроїв, що збирають і передають дані;
- Big Data — аналіз великих масивів даних для прогнозування та прийняття рішень;
- штучний інтелект (AI) та машинне навчання — автоматизація процесів, прогнозування, обробка інформації у реальному часі;
- Blockchain — технологія децентралізованих реєстрів, яка підвищує прозорість і безпеку транзакцій;
- 5G і майбутнє 6G — нові стандарти мобільного зв'язку, що значно збільшують швидкість та обсяг передавання даних.

Роль для держави:

- розвиток електронного урядування (сервіси "Дія");

- цифровізація фінансових послуг (онлайн-банкінг, цифрові валюти);
- автоматизація систем управління (Smart City, е-здоров'я);
- модернізація оборонної сфери (цифрові системи управління військами, безпілотники).

Таким чином, ІКТ є стратегічним ресурсом, який визначає конкурентоспроможність держави.

Поняття критичної інфраструктури

Критична інформаційна інфраструктура (КІІ) — це сукупність інформаційних систем і мереж, безперебійна робота яких є життєво необхідною для функціонування держави та суспільства.

Основні елементи КІІ:

- енергетика (системи управління електромережами, АЕС, газопроводи);
- транспорт (авіаційні системи, залізниця, морські перевезення);
- фінансовий сектор (банківські системи, платіжні сервіси);
- урядові реєстри та системи управління;
- системи охорони здоров'я (електронні медичні бази, телемедицина);
- військові системи управління та зв'язку.

Вразливості КІІ:

- використання застарілого обладнання;
- залежність від імпортних технологій;
- недостатній рівень кіберзахисту;
- складність координації між різними секторами.

Атаки на КІІ можуть паралізувати державу: прикладом є кібератаки на українську енергосистему у 2015–2016 рр.

Ризики, пов'язані з IoT, хмарними сервісами, Big Data та AI

Інтернет речей (IoT):

- переваги: автоматизація виробництва, розумні будинки, транспорт, медицина;

- ризики: уразливість “розумних” пристроїв, можливість віддаленого зламу, збір персональних даних;
- приклад: використання заражених IoT-пристроїв у бот-мережах (DDoS-атаки).

Хмарні сервіси:

- переваги: економія ресурсів, гнучкість, доступність;
- ризики: витік даних, контроль над інформацією з боку іноземних провайдерів, складність контролю;
- приклад: атаки на хмарні сервіси Microsoft, які вплинули на діяльність десятків країн.

Big Data:

- переваги: прогнозування епідемій, економічний аналіз, політичне планування;
- ризики: маніпуляція суспільною думкою (скандал Cambridge Analytica), втрата конфіденційності.

Штучний інтелект (AI):

- переваги: автоматизація процесів, підвищення точності рішень, використання у сфері оборони;
- ризики: створення deepfake-контенту, автономні кібер-атаки, етичні проблеми контролю;
- приклад: використання AI для автоматичного поширення дезінформації.

Кібергігієна населення:

- використання складних паролів і багатофакторної автентифікації;
- оновлення програмного забезпечення;
- обережність у соцмережах та під час отримання електронних листів;
- навчальні кампанії для школярів, студентів, держслужбовців.

Кібергігієна організацій:

- проведення регулярних аудитів безпеки;
- використання антивірусних і мережевих фільтрів;
- сегментація корпоративних мереж;
- проведення тренінгів для персоналу.

Захист державних мереж:

- централізоване управління інцидентами (CERT-UA);
- використання криптографічних засобів захисту інформації;
- розробка національних стандартів кіберзахисту;
- співпраця з міжнародними партнерами для обміну інформацією про загрози.

Інноваційні підходи:

- використання штучного інтелекту для виявлення аномалій у мережах;
- перехід на квантові технології захисту у довгостроковій перспективі.

Приклади з міжнародного та українського досвіду:

- Україна: перенесення державних реєстрів у хмарні датацентри ЄС у 2022 р., що забезпечило їх безперервну роботу під час війни;
- ЄС: впровадження стандартів NIS2 для захисту критичної інфраструктури;
- США: розвиток Національного агентства з кібербезпеки та використання концепції Zero Trust;
- Естонія: створення "кібер-уряду" з максимальною цифровізацією, який пережив масштабну атаку у 2007 р. та став прикладом для інших.

Цифровізація та розвиток ІКТ-інфраструктури створюють **безпрецедентні можливості для розвитку держави й суспільства**, але водночас породжують **нові вразливості**:

- сучасні технології (IoT, AI, Big Data, Cloud) радикально змінюють функціонування держави та бізнесу;
- критична інформаційна інфраструктура потребує особливого захисту, оскільки атаки на неї можуть паралізувати країну;
- ризики, пов'язані з цифровими технологіями, охоплюють витік даних, маніпуляцію свідомістю, дезінформацію, кіберзлочинність;
- основою безпеки є кібергігієна населення та організацій, а також розвиток державної системи кіберзахисту.

Україна, як і інші держави, повинна будувати політику інформаційної безпеки з урахуванням глобальних тенденцій цифровізації, але водночас забезпечувати **технологічний суверенітет та інтеграцію у міжнародні стандарти**.

Контрольні питання

1. Яку роль відіграє цифровізація у державному управлінні?
2. Що таке ІКТ-інфраструктура та які її складові?
3. Які ризики виникають під час цифрової трансформації?
4. Як цифровізація впливає на інформаційну безпеку?
5. Які міжнародні моделі розвитку ІКТ-інфраструктури є найбільш ефективними?
6. Чому захист критичної цифрової інфраструктури є пріоритетним?

Практичне питання

Мета

Оцінити вплив цифрової інфраструктури на державне управління.

Практичні завдання

1. Оцінити критичні елементи ІКТ-інфраструктури України.
2. Проаналізувати ризики цифровізації (мінімум 5).
3. Запропонувати заходи щодо захисту критичної ІКТ-інфраструктури.

Питання для обговорення

Чи може цифровізація створювати більше загроз, ніж можливостей?

Тема 12. Кібербезпека як складова інформаційної безпеки: виклики та міжнародний досвід

У сучасному світі інформаційна безпека неможлива без потужної **системи кіберзахисту**. Якщо інформаційна безпека охоплює широку сферу — від політики, економіки, культури до правових механізмів, то **кібербезпека** є її техніко-технологічним ядром. Вона забезпечує захист інформаційних систем, мереж, даних і технологій від несанкціонованого доступу, пошкодження чи знищення.

Матеріали дисертаційних досліджень наголошують: кібербезпека сьогодні є не просто частиною інформаційної політики, а її критичною основою, оскільки саме через кіберпростір реалізуються більшість загроз — від шпигунства до терористичних атак.

Визначення кібербезпеки та її межі

Кібербезпека — це стан захищеності кіберпростору, інформаційних систем і даних від кіберзагроз, що забезпечує їх цілісність, доступність і конфіденційність. У широкому сенсі — це здатність держави, організацій та громадян безпечно функціонувати у цифровому середовищі.

Межі кібербезпеки

Кібербезпека охоплює:

- захист критичної інформаційної інфраструктури;
- безпеку державних і корпоративних інформаційних систем;
- кіберзахист військової сфери;
- захист персональних даних і цифрової ідентичності громадян;
- попередження та протидію кіберзлочинності.

Таким чином, кібербезпека є невід'ємною складовою національної безпеки, а не лише технічною функцією.

Міжнародні стандарти у сфері кібербезпеки

ISO/IEC:

- ISO/IEC 27001 — міжнародний стандарт систем управління інформаційною безпекою (ISMS);
- ISO/IEC 27002 — кодекс практик для контролю інформаційної безпеки;
- ISO/IEC 27032 — стандарт, присвячений кібербезпеці, визначає взаємодію держави, бізнесу та громадян.

NIST (Національний інститут стандартів і технологій, США):

- NIST Cybersecurity Framework (CSF) — базова структура управління кіберризиками, яка містить п'ять функцій: Identify, Protect, Detect, Respond, Recover;
- NIST SP 800 Series — серія публікацій, що регламентують різні аспекти кіберзахисту (криптографія, управління ідентичністю, оцінка ризиків).

Європейські підходи:

- Директива NIS (2016) та NIS2 (2022) — правові механізми ЄС для захисту критичної інфраструктури та гармонізації політик кібербезпеки;
- GDPR (2018) — регламент ЄС про захист персональних даних, який тісно пов'язаний із кіберзахистом.

Інші стандарти та практики:

- CIS Controls (Center for Internet Security) — набір практичних рекомендацій для організацій;
- COBIT 2019 — стандарт управління IT-процесами, що включає аспекти кіберзахисту.

Використання цих стандартів підвищує стійкість інформаційних систем і дає змогу інтегруватися у світовий безпековий простір.

Міжнародне співробітництво у сфері кібербезпеки

Регіональні формати:

- Європейський Союз: Європейське агентство з кібербезпеки (ENISA), програма "Цифрова Європа";

- НАТО: Центр передового досвіду з кібероборони в Таллінні, стратегія колективної кібероборони.

Глобальні ініціативи:

- Будапештська конвенція про кіберзлочинність (2001 р.) — головний міжнародний договір у сфері протидії кіберзлочинам;
- ООН: робочі групи з питань розвитку правил поведінки держав у кіберпросторі;
- G7 і G20: узгодження політик кіберзахисту, координація санкцій проти кіберагресорів.

Двосторонні та багатосторонні угоди України:

- співпраця з НАТО у межах трастових фондів;
- участь у європейських програмах кіберзахисту;
- партнерство з США, Канадою, Великою Британією для обміну інформацією про кіберінциденти.

Міжнародна співпраця є життєво важливою, оскільки кібератаки не мають кордонів, і лише колективна безпека може забезпечити належний рівень захисту.

Міжнародні кіберінциденти та їх аналіз

Атака на Естонію (2007 р.):

- масштабна DDoS-атака на державні органи, банки, ЗМІ;
- результат — тимчасовий параліч державних систем;
- наслідок — створення у Таллінні Центру кібероборони НАТО.

Вірус Stuxnet (2010 р.):

- ціль — іранська ядерна програма;
- вірус уразив системи управління промисловими об'єктами (SCADA);
- демонстрація нової ери кібервійни — використання шкідливого ПЗ як "цифрової зброї".

Атака NotPetya (2017 р.):

- удар по Україні: урядові системи, банки, транспорт, енергетика;

- поширення у світовому масштабі, збитки оцінюються у мільярди доларів;
- визнана однією з наймасштабніших кібератак в історії.

SolarWinds (2020 р.):

- злам американської компанії SolarWinds, через який постраждали урядові установи США та міжнародні корпорації;
- атака на ланцюги постачання, що підкреслює уразливість глобалізованої цифрової економіки.

Український досвід (2022–2023 рр.):

- масові атаки перед і під час повномасштабного вторгнення росії;
- кібератаки на державні реєстри, енергетику, телекомунікації;
- рішення: перенесення частини систем у хмарні датацентри ЄС, створення міжнародних альянсів кіберзахисту.

Кібербезпека є **ключовою складовою інформаційної безпеки**, без якої неможливе нормальне функціонування держави та суспільства:

- вона визначає стійкість критичної інфраструктури, захист державних і приватних систем, безпеку громадян;
- міжнародні стандарти (ISO/IEC, NIST, NIS2, GDPR) створюють базу для ефективного управління ризиками;
- міжнародне співробітництво забезпечує колективний захист і спільну відповідь на атаки;
- реальні кейси (Естонія, Stuxnet, NotPetya, SolarWinds, атаки на Україну) показують, що кіберзагрози є глобальними та потребують системної протидії.

Для України кібербезпека є не лише сферою технічної політики, а й питанням **виживання та суверенітету**. Її розвиток повинен ґрунтуватися на поєднанні національних зусиль і міжнародної кооперації, інтеграції у світову систему кіберзахисту та постійному оновленні стратегій відповідно до нових викликів.

Контрольні питання

1. Які основні виклики постають перед кібербезпекою держави?
2. Які види кібератак є найпоширенішими?
3. Які міжнародні організації формують політику у сфері кібербезпеки?
4. Як міжнародний досвід можна адаптувати в Україні?
5. Які принципи кіберзахисту є ключовими?
6. Які механізми співпраці держави з приватним сектором у кібербезпеці?

Практичне питання

Мета

Вивчити основні кіберзагрози й практики реагування.

Практичні завдання

1. Класифікація кібератак за реальними прикладами (DDoS, фішинг, шифрування).
2. Аналіз кіберінциденту (наприклад, атака NotPetya).
3. Розробити модель кіберзахисту для державної установи.

Питання для обговорення

Чи можлива повна кібербезпека?

Тема 13. Система стратегічного управління інформаційною безпекою: моделі, інструменти, оцінка ефективності

У сучасному глобалізованому світі питання інформаційної безпеки є одним із центральних викликів для держави. Гібридні загрози, кібератаки, інформаційні війни та масштабні кампанії дезінформації вимагають від урядів системного підходу до стратегічного управління.

Матеріали дисертаційних досліджень з цієї проблематики наголошують: стратегічне управління інформаційною безпекою має поєднувати **моделі організації, інструменти політики та менеджменту**, а також **механізми оцінювання ефективності**, які дають змогу коригувати стратегії відповідно до нових умов.

Моделі управління інформаційною безпекою

Єдина національна система:

- передбачає централізоване управління з боку держави;
- головний координаційний центр: РНБО, органи спеціального зв'язку, спецслужби;
- переваги: узгодженість дій, швидкість реагування, чітка вертикаль відповідальності;
- недоліки: ризик бюрократизації, обмежена гнучкість.

Децентралізовані моделі:

- більше повноважень делегується регіональним органам влади, приватному сектору та громадянському суспільству;
- переваги: адаптивність, залучення різних ресурсів і досвіду;
- недоліки: складність координації, ризик дублювання функцій.

Моделі змішаного типу:

- поєднують централізовану координацію з автономією окремих секторів (фінансовий, енергетичний, телекомунікаційний);
- діють у ЄС та США, де єдині стратегії поєднуються з гнучкістю у приватному секторі.

Український досвід:

- Україна застосовує модель централізованого управління з елементами державно-приватного партнерства;
- РНБО виконує роль стратегічного координатора, а Мінцифра, ДССЗЗІ та СБУ — операційних суб'єктів;
- водночас залучаються приватні компанії та міжнародні партнери.

Інструменти стратегічного управління

Рамкові політики:

- доктрина інформаційної безпеки, Стратегія кібербезпеки, Національна стратегія безпеки;
- визначають базові цілі та пріоритети держави.

Міжнародні стандарти:

- ISO/IEC 27001, 27032 — управління інформаційною безпекою і кіберзахистом;
- NIST Cybersecurity Framework — інструмент управління ризиками;
- NIS2 — директива ЄС для захисту критичної інфраструктури.

Аудити та перевірки:

- регулярні аудити державних і корпоративних інформаційних систем;
- виявлення уразливостей, оцінка готовності до інцидентів.

Форсайт і сценарне планування:

- використання прогнозів розвитку технологій та загроз;
- формування сценаріїв реагування (мир, криза, війна);
- приклад: передбачення ризиків від AI чи квантових обчислень.

Ризик-менеджмент:

- ідентифікація, оцінка та мінімізація ризиків;
- використання методик OCTAVE, FAIR, ISO 31000;
- пріоритизація ресурсів залежно від рівня ризику.

Ключові показники ефективності (KPI):

- середній час реагування на кіберінцидент;
- кількість відвернених атак;
- рівень використання національного софту в держсекторі;
- довіра громадян до державних інформаційних ресурсів.

Моніторинги:

- постійний збір даних про загрози, вразливості та інциденти;

- використання центрів моніторингу (SOC, CERT-UA);
- автоматизовані системи виявлення аномалій.

Оцінювання ризику:

- визначення ймовірності та потенційних збитків від загроз;
- кількісні (статистичні) та якісні (експертні) методи оцінки;
- приклад: ймовірність атаки на енергосистему та можливі економічні втрати.

Бенчмаркінг:

- порівняння з кращими міжнародними практиками;
- аналіз досвіду країн ЄС, НАТО, США, Естонії.

Зворотний зв'язок та коригування стратегій. Жодна стратегія не є остаточною: вона повинна коригуватися відповідно до змін середовища.

Механізми зворотного зв'язку:

- регулярні звіти органів влади про стан інформаційної безпеки;
- опитування суспільної думки щодо довіри до ЗМІ та цифрових сервісів;
- зворотний зв'язок від приватного сектору й міжнародних партнерів.

Коригування стратегій:

- внесення змін до стратегічних документів раз на 3–5 років;
- оперативні оновлення у відповідь на нові загрози (наприклад, під час війни);
- гнучкість у плануванні ресурсів і пріоритетів.

Приклади:

- внесення змін до Доктрини інформаційної безпеки України у 2022 р. після початку повномасштабної агресії;
- модифікація стратегії кіберзахисту США після інциденту SolarWinds.

Система стратегічного управління інформаційною безпекою — це багаторівнева структура, що включає:

- моделі управління (централізовані, децентралізовані, змішані);
- інструменти (рамкові політики, стандарти, аудити, форсайт, ризик-менеджмент);
- методи оцінки (KPI, моніторинги, оцінка ризиків, бенчмаркінг);
- зворотний зв'язок і коригування, які забезпечують гнучкість і стійкість системи.

Україна, враховуючи власний досвід протидії гібридній агресії, рухається у напрямі **централізованої моделі з елементами державно-приватного партнерства**, але має поступово розвивати більш інтегровані механізми співпраці з міжнародними структурами.

Стратегічне управління інформаційною безпекою — це **динамічний процес**, що вимагає постійного оновлення. Тільки поєднання моделей, інструментів і системної оцінки ефективності може гарантувати державі стійкість у сучасному інформаційному просторі.

Контрольні питання

1. Які моделі стратегічного управління використовуються у світовій практиці?
2. Які інструменти застосовують для забезпечення інформаційної безпеки?
3. Як здійснюється оцінка ефективності заходів інформаційної безпеки?
4. Які показники використовують для вимірювання інформаційної стійкості?
5. Які проблеми існують у системі управління інформаційною безпекою в Україні?
6. Як підвищити ефективність стратегічного управління?

Практичне питання

Мета

Дослідити моделі управління й оцінювання ефективності.

Практичні завдання

1. Порівняти різні моделі управління (централізована, мережева, змішана).
2. Розробити критерії ефективності інфобезпеки для державного органу.
3. Побудувати систему індикаторів стратегічної стійкості.

Питання для обговорення

Чому оцінка ефективності часто є формальною?

Тема 14. Перспективи розвитку стратегій в Україні: виклики та можливості

Україна опинилася у ситуації, коли інформаційна безпека та стратегічне управління є не лише питанням розвитку, а й питанням **виживання держави**. Повномасштабна війна, гібридні загрози, кібератаки та інформаційні операції створили безпрецедентні виклики, що змінюють підходи до формування стратегій.

У дисертаційних дослідженнях стратегічного управління інформаційною безпекою наголошується, що ефективні стратегії майбутнього повинні бути **гнучкими, адаптивними та технологічно орієнтованими**, а також ґрунтуватися на партнерстві між державою, громадянським суспільством та міжнародною спільнотою.

Вплив війни та надзвичайного стану на стратегічні підходи

Зміна пріоритетів:

- якщо у мирний час акцент робився на розвитку цифрових сервісів та інтеграції з міжнародними стандартами, то у воєнний період пріоритетом стає **захист і стійкість систем**;
- основна увага приділяється **кібероборонi**, захисту критичної інфраструктури, інформаційній мобілізації.

Централізація управління:

- в умовах війни ухвалення рішень концентрується у вищих органах влади (РНБО, Генштаб, уряд);
- це дає змогу забезпечити швидкість реагування та координацію.

Надзвичайні заходи:

- блокування ворожих інформаційних ресурсів;
- обмеження доступу до окремих сервісів, що становлять загрозу;
- тимчасове звуження деяких свобод для захисту безпеки держави.

Формування "воєнних стратегій":

- використання стратегічних комунікацій для підтримки суспільної єдності;
- перенесення державних реєстрів у безпечні хмарні середовища за кордоном;
- масова протидія дезінформації та психологічним операціям;

Таким чином, війна радикально змінює стандартні підходи, зміщуючи акцент від розвитку до виживання і стійкості.

Технологічні тренди майбутнього. Майбутні стратегії інформаційної безпеки повинні враховувати глобальні технологічні зміни.

Штучний інтелект (AI):

- використання для автоматичного виявлення кібератак і фейкових новин;
- розвиток генеративних моделей (deepfake, чат-боти) створює як нові можливості, так і нові загрози;
- необхідність етичного й правового регулювання.

Квантові технології:

- квантові обчислення зможуть зламати традиційні криптографічні алгоритми;
- потрібно готуватися до впровадження постквантової криптографії.

Блокчейн:

- використання у сфері захисту даних, електронного урядування, виборів;
- децентралізовані реєстри можуть забезпечити більшу прозорість і захист від маніпуляцій.

Інтернет речей (IoT):

- зростання кількості "розумних" пристроїв у критичній інфраструктурі;
- ризик їх використання у кібератаках (DDoS, збір даних).

Big Data та аналітика:

- використання великих даних для прогнозування суспільних процесів і виявлення аномалій;
- ризики маніпуляцій свідомістю через таргетовану рекламу та мікротаргетинг.

Отже, технологічні тренди одночасно створюють **можливості для зміцнення безпеки** й **нові ризики**, які повинні враховувати майбутні стратегії.

Роль громадянського суспільства, ЗМІ та освіти

Громадянське суспільство:

- виконує функцію незалежного моніторингу та контролю за владою;
- бере участь у фактчекінгу, протидії дезінформації;
- партнерство з державою у сфері стратегічних комунікацій.

Засоби масової інформації:

- виконують роль "четвертої влади", формуючи порядок денний;
- у кризові часи мають бути інструментом мобілізації та консолідації суспільства;
- виклик: необхідність забезпечення редакційної незалежності та прозорості фінансування.

Освіта:

- медіаграмотність і критичне мислення — базові навички XXI ст.;

- потрібні освітні програми для школярів, студентів і держслужбовців;
- спеціалізована підготовка кадрів у сфері кібербезпеки.

Таким чином, без активної участі суспільства та якісної освіти жодна стратегія не буде життєздатною.

Формування майбутніх стратегій держави у контексті світових викликів

Глобальні виклики:

- гібридні війни: поєднання військових, інформаційних, економічних і кіберзагроз;
- глобальна конкуренція технологій: боротьба між державами за лідерство в AI і квантових обчисленнях;
- кібертероризм: використання кібератак недержавними акторами;
- залежність від транснаціональних корпорацій: контроль над інформаційними потоками великими IT-компаніями.

Принципи формування майбутніх стратегій:

- адаптивність: здатність швидко змінюватися у відповідь на нові загрози;
- міжнародна інтеграція: участь у колективних системах безпеки НАТО, ЄС, ООН;
- технологічний суверенітет: розвиток власних рішень у сфері ІКТ;
- прозорість та довіра: забезпечення відкритого діалогу з громадянами.

Український контекст:

- Україна має унікальний досвід протидії масштабній інформаційній агресії;
- цей досвід може стати основою для нових стратегій, орієнтованих на резильєнтність (стійкість) та проактивність;
- майбутні стратегії повинні інтегрувати підходи військової безпеки, інформаційного суверенітету та інноваційного розвитку.

Перспективи розвитку стратегій інформаційної безпеки в Україні визначаються комбінацією внутрішніх і зовнішніх факторів:

- війна і надзвичайний стан радикально змінюють акценти, ставлячи на перший план оборону та стійкість;
- технологічні тренди створюють нові можливості й загрози, що потребують постійного оновлення стратегій;
- громадянське суспільство, ЗМІ та освіта стають ключовими партнерами держави;
- світові виклики змушують Україну поєднувати внутрішні зусилля з міжнародною кооперацією.

Майбутнє українських стратегій інформаційної безпеки полягає у створенні **гнучкої, адаптивної та інтегрованої системи**, яка здатна протистояти загрозам, використовувати технологічні переваги та зміцнювати позиції держави у глобальному середовищі.

Контрольні питання

1. Які основні виклики стоять перед Україною у сфері інформаційної безпеки?
2. Які можливості відкриває цифровізація для посилення інформаційної безпеки?
3. Які стратегічні пріоритети мають бути враховані під час розробки нових стратегій?
4. Які міжнародні практики можуть бути адаптовані в Україні?
5. Яке значення має людський фактор у розвитку системи безпеки?
6. Які кроки потрібні для формування сучасної інформаційної доктрини?

Практичне питання

Мета

Проаналізувати можливі шляхи розвитку інформаційної політики України.

Практичні завдання

1. Скласти SWOT-аналіз майбутньої стратегії інформаційної безпеки.
2. Проаналізувати виклики, які потребують негайного реагування (мінімум 5).
3. Запропонувати концепцію нової інформаційної доктрини України.

Питання для обговорення

Які можливості відкриває інтеграція в євроатлантичний простір?

ІНФОРМАЦІЙНІ СИСТЕМИ УКРАЇНИ

I. Системи державного управління та електронного врядування

1. Єдиний державний вебпортал електронних послуг “Дія”.
   Єдина точка доступу до державних електронних сервісів.
   Компоненти: Дія.Портал, Дія.Документи, Дія.Підпис, Дія.Бізнес.
2. Національний реєстр електронних інформаційних ресурсів.
   Центральний каталог інформаційних систем держави.
3. Єдина система електронного документообігу органів влади.
   Використовується КМУ, міністерствами, ОДА.
   Містить підсистеми контролю документів, електронного підпису тощо.
4. Система “Трембіта”.
   Основна інтеграційна система для обміну даними між державними реєстрами.
   Аналог європейської X-Road.

II. Системи реєстрації населення та правового статусу громадян

5. Єдиний державний демографічний реєстр.
   Паспорт, ID-картка, закордонний паспорт, посвідки, біометрика.
6. Державний реєстр актів цивільного стану громадян (ДРАЦС).
   Народження, шлюб, смерть, зміна імені.
7. Реєстр територіальних громад.
   Місце реєстрації, формування виборчих списків.
8. Державний реєстр виборців.
   Офіційний реєстр для виборчих процесів.

III. Фінансово-економічні та податкові інформаційні системи

9. Інформаційні системи Державної податкової служби.

Електронний кабінет платника.
Реєстр ПДВ.
Системи фіскального контролю.

10. Системи Державної казначейської служби.
Єдиний казначейський рахунок.
Єдина система обробки платежів.
11. Національна система електронних платежів НБУ.
СЕП, BankID, платіжна інфраструктура.
12. Державний реєстр фінансових операцій (фінмоніторинг).
Використовується Мінфіном та Держфінмоніторингом.

IV. Реєстри власності, майна, підприємництва

13. Державний реєстр речових прав на нерухоме майно.
Нерухомість, обтяження, арешти.
14. Єдиний державний реєстр юридичних осіб, ФОП та громадських формувань (ЄДР).
Реєстрація бізнесу.
15. Державний земельний кадастр (ДЗК).
Земельні ділянки, межі, власність.
16. Електронні реєстри транспортних засобів (МВС).
Реєстрація авто, посвідчення водія.

V. Медицина та соціальна сфера

17. Електронна система охорони здоров'я України (eHealth).
Е-рецепти, декларації, медичні записи.
18 Єдина інформаційна система соціальної сфери.
Соціальні виплати, пільги, субсидії.
19. Пенсійний фонд: Реєстр застрахованих осіб.
ЄСВ, персоніфікація.

VI. Система освіти, науки та культури

20. ЄДЕБО — Єдина державна електронна база з питань освіти.
ЗНО/НМТ, диплони, реєстрація студентів.
21. Наукові реєстри та бази (НБУ, МОН).
ORCID-ідентифікація.
Реєстри наукових робіт і установ.

VII. Системи безпеки та оборонного сектору

22. Інформаційні системи сектору оборони (обмежений доступ).
    Системи управління військами.
    Розвідувальні бази.
    Оперативно-тактичні системи.
23. Системи СБУ.
    Інформаційні системи контррозвідки.
    Антитерористичні бази даних.
24. Єдиний реєстр досудових розслідувань (ЄРДР).
    Використовується всією системою кримінальної юстиції.
25. Інтегрована інформаційно-пошукова система МВС.
    Розшукові та оперативні дані.
    Бази ДНК, відбитків, кримінальних правопорушень.

VIII. Критична інфраструктура та технічні системи

26. Системи енергетичного сектору.
    Диспетчерські ІС.
    Система "Оператор ринку".
27. Системи транспорту і логістики.
    "Електронний кабінет перевізника".
    Єдина транспортна система "E-Transport".
28. Системи митниці.
    ASYCUDA.
    Реєстри митних декларацій.

IX. Спеціалізовані інформаційні системи

29. ProZorro.
    Закупівлі держави.
30. ProZorro.Продажі.
    Прозоре розпорядження державними активами.
31. Єдиний реєстр боржників.
    Наповнюється Мін'юстом.
32. Державний реєстр судових рішень.
    Публічний і спецрежим доступу.
33. Система "СОТА" (подання звітності).

СПИСОК ЛІТЕРАТУРИ

Нормативно-правові акти

1. Конституція України: Закон України від 28.06.1996 р. № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141. URL: zakon.rada.gov.ua (дата звернення: 25.11.2025 р.).
2. Про основи національної безпеки України : Закон України від 19.06.2003 р. № 964-IV. *Відомості Верховної Ради України*. 2003. № 39. Ст. 314. URL: zakon.rada.gov.ua (дата звернення: 25.11.2025 р.).
3. Про кібербезпеку : Закон України від 05.10.2017 р. № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403. URL: zakon.rada.gov.ua (дата звернення: 25.11.2025 р.).
4. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 31.05.2005 р. № 2594-IV. *Відомості Верховної Ради України*. 2005. № 26. Ст. 347. URL: zakon.rada.gov.ua (дата звернення: 25.11.2025 р.).
5. Про державну таємницю : Закон України від 21.01.1994 р. № 3855-XII. *Відомості Верховної Ради України*. 1994. № 16. Ст. 93. URL: zakon.rada.gov.ua (дата звернення: 25.11.2025 р.).
6. Про Стратегію національної безпеки України : Указ Президента України від 26.03.2021 р. № 121/2021. URL: zakon.rada.gov.ua (дата звернення: 25.11.2025 р.).
7. Про Стратегію інформаційної безпеки : Указ Президента України від 27.08.2021 р. № 447/2021. URL: zakon.rada.gov.ua (дата звернення: 25.11.2025 р.).
8. Про затвердження Порядку організації робіт із забезпечення захисту інформації в інформаційно-телекомунікаційних системах : Постанова Кабінету Міністрів України від 19.06.2013 р. № 444. URL: zakon.rada.gov.ua (дата звернення: 25.11.2025 р.).

9. Про затвердження Вимог до захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 08.05.2019 р. № 250. URL: zakon.rada.gov.ua (дата звернення: 25.11.2025 р.).

Основна та додаткова література

10. *Барабаш О. В., Розкос А. А.* Інформаційна безпека держави : навч. посіб. Київ : НАУ, 2017. 328 с.
11. *Довгань О. А.* Захист інформації в інформаційно-телекомунікаційних системах : підручник. Київ : ДУТ, 2019. 300 с.
12. *Журавель В. А., Кононенко В. С.* Міжнародна інформаційна безпека : навч. посіб. Харків : Право, 2019. 240 с.
13. Компаративний аналіз систем інформаційної безпеки держав-членів ЄС та України : монографія / за заг. ред. В. В. Остроухова. Київ : КВІЦ, 2016. 368 с.
14. *Курач С. Ю., Черняк В. О.* Інформаційна безпека України в умовах глобалізації. Київ : Центр вільної преси, 2018. 192 с.
15. *Петрик В. М., Присяжнюк М. М., Остроухов В. В.* Інформаційна безпека: концептуальні і теоретичні засади : монографія. Київ : Ін-т проблем нац. безпеки, 2017. 576 с.

Стандарти та методичні матеріали

16. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013, IDT). Київ : ДП "УкрНДНЦ", 2015. 24 с.
17. Методичні рекомендації щодо реагування на кіберінциденти / Державна служба спеціального зв'язку та захисту інформації України. URL: cert.gov.ua (дата звернення: 25.11.2025 р.).

Офіційні веб-ресурси

18. Офіційний веб-портал Верховної Ради України “Законодавство України”. URL: zakon.rada.gov.ua.
19. Веб-сайт Державної служби спеціального зв’язку та захисту інформації України (ДССЗЗІ). URL: cip.gov.ua.
20. Урядова команда реагування на комп’ютерні надзвичайні події України (CERT-UA). URL: cert.gov.ua.
21. Центр стратегічних комунікацій та інформаційної безпеки при МКІП. URL: spravdi.gov.ua.

Модуль ІІ

ЗАХИСТ ІНФОРМАЦІЇ У СФЕРАХ СУСПІЛЬНОЇ ДІЯЛЬНОСТІ

Тема 15. Поняття захисту інформації

В умовах сьогодення інформація перестала бути допоміжним ресурсом виробництва, а перетворилась у визначальну складову будь-якого бізнесу. Оскільки роль інформації як виробничого ресурсу постійно зростає, не можна залишати сферу інформаційного забезпечення управління без достатньої уваги. Отже, вирішення завдання ефективного інформаційного забезпечення неможливе без захисту інформації.

Деякі науковці під захистом інформації розуміють систему безпеки загалом, або лише захист інформації. Також варто зазначити, що багато авторів ототожнюють поняття — "захист інформації", "комп'ютерна безпека" або "безпека автоматизованих систем". Захист інформації є складовою інформаційної безпеки. На жаль, на більшості підприємств на сьогодні підрозділ інформаційної безпеки відірваний від реалій бізнесу та прив'язаний суто до інформаційних технологій.

Захист інформації — сукупність методів і засобів, що забезпечують її цілісність, конфіденційність і доступність за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації.

Термін вживається в Україні для опису комплексу заходів із забезпечення інформаційної безпеки.

Захист інформації ведеться для підтримки таких **властивостей інформації**, як:

- **цілісність** — неможливість модифікації інформації неавторизованим користувачем;
- **конфіденційність** — інформація не може бути отримана неавторизованим користувачем;

- **доступність** — полягає у тому, що авторизований користувач може використовувати інформацію відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (прийнятного) інтервалу часу.

Загрози інформації

Відповідно до властивостей інформації, виділяють такі загрози її безпеці:

- загрози цілісності:
  - знищення;
  - модифікація;
- загрози доступності:
  - блокування;
  - знищення;
- загрози конфіденційності:
  - несанкціонований доступ (НСД);
  - витік;
  - розголошення.

Аспекти захисту інформації

До аспектів захисту інформації відносять:

- конфіденційність — захист від несанкціонованого ознайомлення з інформацією;
- цілісність — захист інформації від несанкціонованої модифікації;
- доступність — захист (забезпечення) доступу до інформації, а також можливості її використання. Доступність забезпечується як підтриманням систем у робочому стані, так і завдяки способам, які дають змогу швидко відновити втрачену чи пошкоджену інформацію.

Види захисту інформації

Кожен вид захисту інформації забезпечує окремі аспекти інформаційної безпеки:

- технічний — забезпечує обмеження доступу до носія повідомлення апаратно-технічними засобами (антивіруси, фаєрволи, маршрутизатори, токіни, смарткарти тощо):
  - попередження витоку по технічним каналам;
  - запобігання блокуванню;
- інженерний — запобігає руйнуванню носія внаслідок навмисних дій або природного впливу інженерно-технічними засобами (сюди відносять обмежувальні конструкції, охоронно-пожежна сигналізація);
- криптографічний — попереджує доступ за допомогою математичних перетворень повідомлення (ІП):
  - попередження несанкціонованої модифікації;
  - попередження НС розголошення;
- організаційний — попередження доступу на об'єкт інформаційної діяльності сторонніх осіб за допомогою організаційних заходів (правила розмежування доступу).

Структура інформаційного забезпечення має складатись з економічної розвідки, інформаційної безпеки та аналітично-консультативного забезпечення.

Система інформаційної безпеки включає:

- перевірку достовірності інформації;
- визначення важливості та рівня секретності інформації;
- надання допуску та доступу до інформації;
- захист інформації, комерційної таємниці.

Враховуючи наведене, бачимо, що **схема реалізації захисту інформації** основана на таких складових: технічної, організаційної, дозвільної, попереджувальної, правової.

Оскільки у будь-якій системі всі елементи та підсистема є взаємопов'язаними, більшість завдань захисту інформації виконується разом із основними та допоміжними підсистемами системи економічної безпеки держави.

Технічна складова покликана забезпечити захист інформації та об'єктів держави, а також виявлення фактів витікання інформації та неправомірних дій персоналу та сторонніх осіб щодо даного суспільства за допомогою технічних засобів.

Організаційна складова повинна забезпечити належне поводження персоналу підприємства із секретною інформацією та іншими об'єктами захисту національного суб'єкта.

Дозвільна складова системи захисту інформації має здійснювати розподіл інформації підприємства за рівнями секретності та визначати ступінь доступу до неї. Для уникнення ефекту дезінформації та прийняття внаслідок цього хибних управлінських рішень, а також максимального зниження ймовірності витікання секретної інформації, система захисту інформації має включати попереджувальну складові.

Правова складова покликана забезпечити правовий захист інтересів держави щодо захисту інформації, а також закріплення прав громадян та користувачів щодо державної таємниці в установчих документах, договорах та інших нормативних актах.

Системи захисту інформації, що пропонуються науковцями та практиками, не відображають у повній мірі вирішення завдань та виконання функцій, які стоять перед захистом інформації в системі інформаційної безпеки, інформаційного забезпечення та економічної безпеки загалом у сучасних умовах.

Отже, **завданнями системи захисту інформації** є:

- організація особливого діловодства та контролю за секретними документами;
- виявлення, попередження та присікання каналів витікання інформації;
- створення посадових інструкцій, а також положень, пам'яток, методичних вказівок для роботи з відомостями, що становлять комерційну таємницю;
- захист інформації при використанні комп'ютерної техніки та інших технічних засобів обробки та передавання даних;
- виявлення необхідності, обґрунтування та організація встановлення необхідних технічних засобів забезпечення збереження інформації;
- захист у судових та інших державних органах інтересів підприємства щодо комерційної таємниці;

- розроблення нормативної документації щодо комерційної таємниці на підприємстві;
- навчання правилам інформаційної безпеки працівників.

Згідно із зазначеними завданнями, **система захисту інформації** має включати технічну, організаційну, попереджувальну та правову складові. Оскільки система захисту інформації становить найбільш вагому частку в інформаційній безпеці, то й більшість у системі інформаційної безпеки становлять саме складові захисту інформації.

Так, технічна, організаційна та правова складові відносяться саме до системи захисту інформації. Також до системи захисту інформації відноситься попереджувальна складова в частині передбачення, виявлення та перекриття каналів витікання інформації.

Активний розвиток комп'ютерних та інформаційних технологій позитивно позначається абсолютно на всіх сферах економіки держави. Для кожної нової компанії саме інформація вважається необхідним ресурсом, у результаті зберігання, грамотного розпорядження якою вдається розвивати власний бізнес, зменшуючи всілякі ризики. Тому для більшості організацій та держави загалом популярною залишається проблема забезпечення інформаційної безпеки і захисту інформації.

Інформаційна безпека (ІБ) є комплексом певних заходів технічного, організаційного плану. Ці заходи стосуються заощадження, захисту інформаційних даних, а також різного устаткування, що буде потрібне для обробки інформації, запису, зберігання, передачі.

Під таким комплексом прийнято розглядати інноваційні технології, способи і встановлені стандарти, що відповідають за успішне управління інформацією, тим самим забезпечуючи її надійний захист від сторонніх осіб.

Інформаційна безпека та захист інформації дають змогу зберегти всю необхідну структуру різних компаній, підприємств від негативного впливу ззовні.

Такі дії можуть бути абсолютно різними:

- випадковими;
- навмисними.

Водночас вони мають зовнішній чи внутрішній характер. Результати можуть бути найрізноманітнішими: починаючи з втрати важливих даних, несанкціонованої зміни і закінчуючи використанням інформації третіми особами в особистих цілях.

Тому захист інформації є обов'язковою умовою під час забезпечення життєдіяльності будь-якого суспільства, що може гарантувати безперервну роботу його організації та підприємств.

Контрольні питання

1. Що розуміють під поняттям "захист інформації"?
2. Які основні цілі забезпечення захисту інформації?
3. Чим відрізняється захист інформації від забезпечення інформаційної безпеки?
4. Які види інформації підлягають обов'язковому захисту в державі?
5. Які основні принципи формування системи захисту інформації?
6. Які нормативно-правові акти регулюють захист інформації в Україні?

Практичне питання

Мета

Сформувати розуміння сутності, завдань і компонентів захисту інформації.

Практичні завдання

1. Скласти схему "Система захисту інформації: структури та функції" (не менше 7 елементів).
2. Проаналізувати реальний кейс (наприклад, витік даних у держоргані): визначити, які заходи із захисту інформації були порушені.

3. Порівняти два підходи — “захист інформації” та “інформаційна безпека”. Визначити відмінності й точки перетину.
4. Розробити перелік (не менше 5) видів інформації, які підлягають обов’язковому захисту відповідно до законодавства.

Питання для обговорення

Чому повний захист інформації неможливий, і як це впливає на управлінські рішення?

Тема 16. Вимоги до захисту інформації в інформаційних системах

Досягнутий у даний час баланс у системі правових норм, які регулюють інформаційні відносини, у тому числі у сфері інформаційної безпеки та захисту інформації, не є абсолютним. Правові засоби завжди обмежені рівнем суспільного розвитку. Цілі, які визначаються законодавцем, є ідеальними, але за суттю не завжди узгоджуються з рівнем розвитку впровадження та використання інформаційних технологій. Це призводить до невідповідності у відносинах поставлених цілей та вибраних для їх досягнення засобів. Активізація процесу законотворчості з регулювання правовідносин в інформаційній сфері значно ускладнена відсутністю стрункої системи регламентації правових відносин і розвитком цього сегмента законодавства.

Специфіку нормативно-правового регулювання відносин у сфері забезпечення інформаційної безпеки визначають дві обставини.

Перша обставина — це невизначеність кордонів і змісту державних, суспільних та приватних інтересів в інформаційній сфері, що пояснюється широтою та багатоаспектністю останньої.

Друга обставина пов’язана з об’єктивно зумовленою різницею динаміки правотворчого процесу та темпів технічного й технологічного розвитку у сфері інформаційної взаємодії.

Така відмінність визначає існування непереборної неадекватності правового регулювання характеру суспільних зв'язків щодо засобів і способів отримання, накопичення, обробки, зберігання та передачі інформації. Ефективність юридичного впливу в даному випадку може бути досягнута, якщо орієнтувати застосовувані правові регулятори не на реальні, а на прогнозовані суспільні відносини у цій галузі.

Питання захисту інформації активно впливають на забезпечення інформаційної безпеки. Захист інформації стосовно питань інформаційної безпеки має безпосереднє відношення і виступає однією з імперативних умов. Є зворотний зв'язок між ними, оскільки порушення вимог інформаційної безпеки може створити загрозу не лише порушенню конфіденційності, а й цілісності та достовірності інформації.

Інформаційна безпека передбачає захист конфіденційності та забезпечення стану захищеності конституційних права і свободи людини та громадянина. Відповідно, забезпечення інформаційної безпеки передбачає можливість доступу та використання інформації.

Великі інформаційні потоки, що розповсюджуються, у тому числі з використанням технологій великих даних, складають величезний масив, робота з яким передбачає вживання заходів для захисту інформації та забезпечення до неї доступу. Важливою складовою цих заходів є організаційно-правові, технічні, програмно-апаратні та інші заходи інформаційної безпеки.

Забезпечення захисту можна розглядати насамперед як складову стану захищеності.

Інформаційна безпека як стан захищеності передбачає низку станів, зокрема стан забезпечення та захисту права і свободи людини та громадянина. Останнє дає змогу повноцінно проводити заходи захисту інформації та забезпечувати захист прав і свобод людини та громадянина в інформаційній сфері.

Забезпечення захисту інформації постає як одна з вимог її певного законного стану. До вимог включаються вимоги щодо цілісності, достовірності, точності та повноти інформації.

Тільки за наявності сукупності цих вимог можна говорити про повноцінний захист інформації.

Відповідно до **чинних вимог** до засобів забезпечення користування офіційними сайтами органів публічної адміністрації з метою захисту інформації, розміщеної на офіційному сайті, має бути забезпечено:

- ведення електронних журналів обліку операцій, виконаних за допомогою програмного забезпечення та технологічних засобів ведення офіційного сайту, що дають змогу забезпечувати облік дій щодо розміщення, зміни та видалення інформації на офіційному сайті, фіксувати точний час, зміст змін та інформацію про уповноваженого співробітника органу виконавчої влади або оператора офіційного сайту, який здійснив зміни на офіційному сайті;
- щоденне копіювання інформації та електронних журналів обліку операцій на резервний матеріальний носій, що забезпечує можливість відновлення; захист інформації від знищення, модифікації та блокування доступу до неї, від неправомірних дій щодо інформації;
- зберігання резервних матеріальних носіїв із щоденними копіями; застосування шифрованих механізмів та сертифікатів безпеки при передачі даних, що забезпечують шифрування та захист інформації, яка передається, у тому числі персональних даних користувачів офіційних сайтів.

Цей набір заходів дає змогу забезпечити захист інформації разом із цілісністю, точністю та повнотою.

Захист інформації має важливе значення для забезпечення її конфіденційності як стану, при якому відбувається захист інформації від несанкціонованого доступу третіх осіб.

Конфіденційність сприймається як властивість інформації, що зумовлена забезпеченням інформаційної безпеки.

Правову властивість конфіденційності інформації слід визначати як стан обмеження доступу до інформації, що охороняється, у тому числі щодо її використання, розповсюджен-

ня та надання. Стан, встановлений законами, є інтегративним результатом застосування організаційно-правових заходів у межах спеціального правового режиму з метою забезпечення оборони країни та державної безпеки, інформаційної безпеки, охорони прав, свобод та законних інтересів різних суб'єктів.

Забезпечення захисту інформації доцільно розглядати як умову, що дає змогу говорити про конфіденційність інформації. Тому заходи, які вживаються задля забезпечення конфіденційності інформації, передбачають її захист.

У процесах забезпечення конфіденційності інформації обмеженого доступу має безпосередньо реалізовуватись захист інформації.

Нормативне регулювання захисту інформації у найзагальнішому сенсі включає зведення правил, які впорядковують відносини, що виникають у суспільстві щодо інформації між фізичними, юридичними особами та державою. Розвиток науково-технічного прогресу та експансія цифрової економіки зумовили необхідність внесення суттєвих поправок до правового регулювання, яке не встигає адекватно реагувати на зміни, що стрімко відбуваються у соціумі.

Численні автори розглядають вимогу щодо забезпечення захисту інформації як складову поряд з конфіденційністю при забезпеченні інформаційної безпеки стосовно певного виду інформації обмеженого доступу. Щодо професійної таємниці, фахівці висловлюють позицію, що суб'єкт професійної діяльності не тільки зобов'язаний забезпечувати конфіденційність відомостей, а й забезпечувати інформаційну безпеку професійної діяльності.

Надання довірителем відомостей, що становлять професійну таємницю, зумовлено наявністю довіри особистого характеру або пов'язаного з особливим професійним статусом суб'єкта професійної діяльності. Це передбачає, що обидві сторони правовідносин у сфері професійної таємниці розраховують на захист інформації, що отримується та зберігається.

У сфері комерційної таємниці, де витік інформації може призвести до значних майнових втрат, сторони, які використовують відповідну інформацію, повинні враховувати її захист. У зв'язку з цим в угодах про використання відомостей, що становлять комерційну таємницю, у договорах про передачу прав на секрети виробництва (ноу-хау) прямо передбачається вимога забезпечення захисту інформації. Власник або правовласник такої інформації повинен передавати третім особам лише необхідну інформацію, останні зобов'язані повідомляти про використання комерційно цінної інформації.

Судова практика підтверджує, що стосовно комерційної таємниці пред'являються вимоги захисту інформації, а також вимоги про належність інформації до комерційної таємниці.

З усіх видів інформації обмеженого доступу для інсайдерської інформації встановлюється вимога про заборону використання.

Інсайдерська інформація — це інформація, яка не була поширена, у тому числі відомості, що становлять комерційну, службову, банківську таємницю, іншу таємницю, що охороняється законом, поширення якої може мати істотний вплив на ціни фінансових інструментів, іноземної валюти та товарів, у тому числі відомості, що стосуються одного або кількох емітентів емісійних цінних паперів, однієї або кількох управляючих компаній інвестиційних фондів, пайових інвестиційних фондів та недержавних пенсійних фондів або одного або кількох фінансових інструментів, іноземної валюти та товарів.

Забезпечення захисту інформації прямо випливає із вимоги забезпечення конфіденційності відомостей, що належать до державної таємниці. У Законі України "Про державну таємницю" зазначено, що віднесення відомостей до державної таємниці та їх засекречення здійснюється відповідно до принципів законності, обґрунтованості та своєчасності.

Забезпечення обґрунтованості передбачає проведення експертної оцінки відомостей щодо доцільності засекречування

чи розсекречення. Доцільність віднесення засекречування недостовірної інформації навряд чи обґрунтовано.

Закон України "Про інформацію" щодо законності передбачає дотримання вимог інформаційного законодавства та реалізацію її захисту.

Вимога забезпечення захисту інформації прямо встановлена щодо кредитних історій. Зокрема, ст. 4 Закону України "Про організацію формування та обігу кредитних історій" зазначає, що принципами формування та доступу до інформації, яка складає кредитну історію, є: конфіденційність інформації та її захист.

Закон покладає на джерело формування кредитної історії обов'язок щодо повідомлення достовірної інформації та необхідності її оновлення.

Відповідно до Закону України "Про захист персональних даних" при обробці персональних даних має бути забезпечено їх захист, достатність, а за необхідності — актуальність стосовно мети обробки персональних даних.

Оператор повинен вживати необхідних заходів або забезпечувати їх прийняття щодо видалення чи уточнення неповних, або точності та актуальності інформації.

Аналіз законодавства про персональні дані свідчить, що більшість підзаконних нормативно-правових актів у цій сфері фактично дублює вимогу щодо захисту, але не розкриває заходи, направлені на захист інформації. Закон України "Про захист персональних даних" покладає на оператора персональних даних обов'язок захисту, надання точної інформації та її актуалізації, оновлення при настанні відповідних обставин і передачі відповідних даних.

Однак сьогодні кількість згод, які видає суб'єкт персональних даних, перевищує можливості людини реально відстежувати всіх операторів, кому надано такі дані. Виникає питання необхідності створення автоматизованих систем, за допомогою яких суб'єкт персональних даних міг би контролювати операторів, які обробляють його дані, та через ці системи оновлювати

свої дані. Для операторів це значно збільшить роботу з обробки даних і створить ризики витоку їх великих обсягів. У зв'язку з чим варто розглянути питання про зміну обов'язку суб'єкта захисту, оскільки даний аспект безпосередньо пов'язаний з розвитком цифрової економіки.

Питання формування єдиного інформаційного простору цифрової економіки України багато в чому дискусійне, з технологічної точки зору, має ряд теоретичних, практичних і організаційних задач національного та міжнародного рівня, що у деякій мірі враховано у Національній економічній стратегії на період до 2030 р.

Аналіз реалізації захисту інформації у відносинах, пов'язаних із забезпеченням конфіденційності стосовно інформації обмеженого доступу у контексті забезпечення інформаційної безпеки, свідчить про низку **закономірностей**:

- законодавець у цій сфері поки що не використовує активно прямі вимоги щодо забезпечення захисту інформації, частіше використовуючи вимоги щодо забезпечення точності, достатності, цілісності, незмінності інформації;
- захист інформації є однією з умов наявності конфіденційності та достатності заходів щодо її забезпечення. Вона повинна відображатися у нормативних вимогах опису заходів захисту конфіденційності стосовно всіх видів інформації обмеженого доступу;
- захист інформації повинен знайти закріплення в інституційних засадах усіх видів інформації обмеженого доступу та відображення у нормах відповідних законів, які встановлюють режими різних видів інформації, доступ до якої обмежений.

Важливо розвивати забезпечення достовірності з позиції захисту від поширення хибної інформації та іншої дезінформації як серйозної інформаційної загрози не лише на національному, а й на міжнародному рівнях. Про необхідність реалізації державної політики у сфері протидії створенню та розповсюдженню дезінформації та іншої недостовірної інформації свідчить

низка важливих документів. Поширення недостовірної інформації сприймається як загроза інформаційній безпеці.

Держави Європейського Союзу розглядають поширення дезінформації, у тому числі фейкової інформації, як правопорушення.

Серед **ключових тенденцій** у сфері правових заходів інформаційної безпеки у контексті забезпечення інформаційної безпеки фахівці виокремлюють:

- активний розвиток стратегічних документів, спеціальних нормативно-правових актів щодо захисту інформації, зокрема удосконалення Закону України "Про захист інформації в інформаційно-комунікаційних системах";
- закріплення на державному рівні системи засобів забезпечення захисту інформації, розробка планів щодо реалізації системи;
- реалізація директивних документів Європейського Союзу щодо критеріїв забезпечення захисту інформації;
- системний підхід до обмежень і заборон в інформаційному просторі, удосконалення структури органів, які здійснюють контроль і нагляд у цій сфері;
- розвиток державних програм з навчання щодо захисту інформації;
- удосконалення системи юридичної відповідальності у сфері інформаційної безпеки;
- використання технологій штучного інтелекту у протидії загрозам безпеці інформації;
- вживання комплексу спеціальних заходів щодо протидії поширенню фейкової інформації.

Аналіз стану правового регулювання захисту інформації у контексті забезпечення інформаційної безпеки дає змогу говорити, що:

- розвиток правових засобів захисту інформації в Україні відстає від технічних, організаційних, програмно-апаратних та ін.;

- відсутнє спеціальне регулювання з цього питання, не сформовано єдиний понятійний апарат, принципи правового забезпечення захисту інформації у контексті інформаційної безпеки не сформульовано на державному рівні;
- неефективно застосовується система правових заборон та обмежень в інформаційному просторі, не розвивається система мережевого державного суверенітету.

Більшість **правових засобів**, що приймаються, пов'язані з окремими інститутами:

- забезпечення захисту інформації обмеженого доступу, в тому числі державної таємниці, комерційної таємниці, персональних даних;
- інститутом критичної інфраструктури;
- протидії злочинам у сфері комп'ютерної інформації та ін.

Серед **основних завдань** адміністративно-правового регулювання щодо інформації, інформаційно-інфраструктурних відносин, об'єктом яких виступають засоби зв'язку, інформатизації, а також захист інформації та інформаційна безпека, можна виокремити контроль за інформаційними потоками, забезпечення інформаційної безпеки (в інформаційному та технічному аспектах).

У Стратегії національної безпеки України встановлено, що забезпечення інформаційної безпеки здійснюється шляхом реалізації державної політики, спрямованої на вирішення завдань щодо формування безпечного середовища обігу інформації, доведення до громадськості достовірної інформації.

Стратегія інформаційної безпеки України як документ стратегічного планування закріплює аналогічне положення. У ньому встановлюється, що реалізація національних інтересів в інформаційній сфері спрямована на формування безпечного середовища обігу інформації та стійкого до різних видів впливу інформаційної інфраструктури з метою забезпечення конституційних прав і свобод людини та громадянина, стабільного соціально-економічного розвитку країни, національної безпеки України.

У зв'язку з повномасштабним вторгненням росії в Україну від 24 лютого 2022 р. в країні запроваджений воєнний стан. Водночас російські військові здійснюють агресію проти України і у кіберпросторі. Кількість кібератак на державні інформаційні системи та об'єкти критичної інформаційної інфраструктури зросла втричі. Військові хакери рф та білорусі, діяльність яких фінансується владою, здійснюють 90 % атак.

Основна мета російських хакерів — це цивільна інфраструктура. Вони намагаються завдати якомога більше шкоди звичайним людям шляхом як ракетних та інших обстрілів, так і кібератак.

Через воєнні дії багато установ перенесли свої дані — хтось в інші, більш спокійні регіони країни, хтось — у хмару на території України, хтось — у хмару за кордон. Ми внесли відповідні зміни до законодавства, які дозволили це робити навіть державним установам.

Проте, як і раніше, всі інформаційні системи, вимоги до захисту яких закріплені в законодавстві України, мають бути захищені за чинними стандартами, зокрема КСЗІ, а в деяких випадках допустиме використання європейських стандартів ISO/IEC 27 серії. Саме системи захисту інформації є першим кордоном, що стримує ворога від знищення нашої країни у кіберпросторі.

Держспецзв'язку роз'яснює, які вимоги щодо захисту даних в інформаційних системах наразі діють в Україні, як їх будувати та як отримати підтвердження захисту у воєнний час.

Під час дії воєнного часу **вимоги щодо захисту інформації** в інформаційно-комунікаційних системах не змінюються. Вони визначені в Законі України "Про захист інформації в інформаційно-комунікаційних системах".

Відповідальність за забезпечення захисту інформації в системі лежить на власнику системи.

Ще до початку війни українські інформаційні системи зазнали потужних атак російських хакерів. Від початку повномасштабної відкритої агресії рф інтенсивність кібератак не

знижується. Російські військові хакери намагаються отримати доступ до персональних даних українців, а також завдати шкоди українським інформаційним системам. Ці атаки координуються з атаками на критичну інфраструктуру і є частиною воєнної агресії рф.

Витік персональних даних українців загрожує тим, що військові та спецслужби ворога використовують їх проти нашого населення, у тому числі на тимчасово окупованих територіях, де українці найбільш вразливі до агресії ворога. Крім того, витік чутливих даних загрожує роботі органів влади та критичної інфраструктури, якщо він буде використаний ворогом для подальших атак. Тож під час війни та протистояння російській агресії питання захисту даних в інформаційних системах постає більш гостро.

Вимоги щодо використання стандартів захисту інформації залишаються без змін. Зокрема, державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, мають оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності комплексної системи захисту інформації здійснюється за результатами державної експертизи, яка проводиться з урахуванням галузевих вимог і норм інформаційної безпеки у порядку, встановленому законодавством.

Комплекс стандартів захисту інформації (КСЗІ) як сукупність технічних та організаційних заходів захисту впроваджуються як в інформаційній системі власника у вигляді технічних (програмно-апаратних та програмних) засобів захисту та їх налаштувань, так і в установі власника у вигляді розпоряджень, планів, інструкцій, методик тощо.

Для захисту інформаційних систем, в яких не обробляється інформація з обмеженим доступом, але захист яких вимагає українське законодавство, може бути також використана альтернативна система інформаційної безпеки відповідно до європейських стандартів ISO/IEC 27 серії.

Процедура побудови КСЗІ та отримання атестата відповідності на час дії воєнного стану така сама, як і раніше.

Побудовою КСЗІ можуть займатися як спеціалізовані організації, так і самі компанії, якщо у них є відповідні фахівці. Головне, щоб побудована система відповідала усім законодавчо встановленим вимогам і змогла отримати атестат відповідності.

Вартість робіт визначається з урахуванням у тому числі вартості програмно-апаратних та програмних засобів технічного та криптографічного захисту інформації, які необхідні для забезпечення належного рівня захищеності інформаційних ресурсів.

Послугу надають кілька компаній, які конкурують між собою, тому ціну визначає ринок і складність завдання.

Атестат відповідності КСЗІ є результатом проведення державної експертизи у сфері технічного захисту інформації, яка проводиться відповідно до "Положення про державну експертизу у сфері технічного захисту інформації", яке затверджене наказом Адміністрації Держспецзв'язку від 16.05.2007 р. № 93, зареєстрованим у Міністерстві юстиції України 16.07.2007 р. № 820/14087.

Експертиза проводиться установою, яка має відповідну ліцензію, на договірних засадах, які у тому числі передбачають і терміни проведення робіт, що залежать від складності системи, досвіду експертів, якості побудови та документування КСЗІ тощо. Зазвичай середній термін проведення експертизи КСЗІ інформаційної системи становить три місяці. У разі позитивних результатів експертизи Адміністрацією Держспецзв'язку реєструється атестат відповідності КСЗІ.

Під час воєнного стану Адміністрація Держспецзв'язку продовжує реєструвати атестати відповідності у звичайному режимі.

У разі перенесення інформаційно-комунікаційних систем, які мають впроваджені КСЗІ з оціненою відповідністю, системи захисту мають бути переглянуті та модернізовані, якщо

була змінена технологія оброблення інформації в ІКС або програмно-апаратному чи програмному складі ІКС тощо.

В інших випадках атестат відповідності буде дійсним при розміщенні ІКС в інфраструктурі хмарного сервісу, механізми захисту інформації якого також пройшли відповідну оцінку.

Аналогічна ситуація як при перенесенні інфраструктури в хмару на території України.

Створення систем захисту з використанням іноземних хмарних платформ не заборонено.

Якщо компанія-ліцензіат зробить відповідний експертний аудит профілів захисту системи, яка використовує для збереження даних хмарні сервіси, розміщені за межами України, і дійде позитивних висновків, Держспецзв'язку в установленому порядку зареєструє атестат відповідності.

При побудові та оцінюванні КСЗІ враховуються сервіси хмари, які у тому числі реалізують функції захисту інформації.

Також нагадуємо, що в деяких випадках компанія може побудувати систему інформаційної безпеки відповідно до європейських стандартів ISO/IEC 27 серії з урахуванням вимог Закону України "Про захист інформації в інформаційно-комунікаційних системах".

Отже, цінність інформації щодо цифрової економіки набуває нового значення. Підходи до інформаційного менеджменту не так сприяють формуванню доданої вартості процесів захисту інформації, як створюють потенціал для отримання додаткової цінності інформації.

Реалізація захисту інформації щодо забезпечення конфіденційності здійснюється переважно з використанням законодавчих вимог забезпечення не захисту, а інших вимог, що пред'являються законодавчо. Нормативно-правове забезпечення режиму захисту інформації обмеженого доступу розвивається шляхом включення вимог щодо забезпечення достовірності, точності й інших критеріїв інформації. Захист інформації має знайти закріплення у системі інституційних принципів усіх видів інформації обмеженого доступу.

Ефективність правового регулювання захисту інформації у контексті забезпечення інформаційної безпеки виявляється у вдосконаленні законотворчої діяльності, що створює затребувані часом норми права, в яких знаходять відображення інтереси та потреби членів соціуму та присутній адміністративний ресурс силових структур держави.

Контрольні питання

1. Які основні вимоги висуваються до захисту інформації в ІС?
2. Що таке цілісність, конфіденційність і доступність інформації?
3. Які категорії інформації потребують особливих вимог до захисту?
4. Як визначають рівень захисту інформації для ІС?
5. Які технічні та організаційні засоби забезпечують відповідність вимогам?
6. Які стандарти і протоколи використовуються в інформаційних системах для забезпечення безпеки?

Практичне питання

Мета

Навчитися визначати вимоги до безпеки ІС та оцінювати їх відповідність.

Практичні завдання

1. Виділити вимоги конфіденційності, цілісності та доступності у конкретній інформаційній системі (вибрати приклад: банк, держреєстр, CRM).
2. Оцінити рівень захисту ІС за моделлю CIA — надати аргументи для кожного елемента.
3. Проаналізувати нормативні акти, що регулюють захист ІС в Україні (Закон “Про захист інформації в ІТС”, стандарти ДСТУ).
4. Створити таблицю вимог до ІС, яка обробляє інформацію з обмеженим доступом.

Питання для обговорення

Які труднощі виникають при одночасному забезпеченні конфіденційності й доступності?

Тема 17. Методи захисту інформації

Ефективне функціонування суспільства неможливе без управління ресурсами, що використовуються для досягнення мети. Згідно з поширеними нині в управлінській літературі поглядами поняття "ресурси" охоплює не лише людей, капітал, сировину, а й інформацію. Саме тому інформація, як і решта ресурсів, потребує особливого захисту.

Під **інформаційною безпекою** слід розуміти захищеність інформації і підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, що можуть призвести нанесенням шкоди власникам або користувачам інформації і підтримуючої інфраструктури. Впровадження обчислювальної техніки і різних інформаційних систем у діяльність і життя сучасних людей має безліч позитивних моментів. Але разом із користю з'явилося і безліч різних загроз.

Виділимо найпоширеніші види потенційних загроз безпеці діяльності суспільств у сфері інформаційних технологій:

- відсутність регламентованого доступу до файлів даних;
- вільне втручання в програмне забезпечення;
- відсутність протоколювання змін у програмному забезпеченні;
- відсутність регламентації користувачів інформації;
- відсутність дублювання важливих документів на документальних носіях даних;
- багаторазові удосконалення одного і того самого програмного забезпечення різними особами;
- відсутність схем інформаційного забезпечення рівнів управління;
- наявність непідзвітних посадових осіб у системі управління тощо.

Однією з найбільш нагальних проблем інформаційного суспільства є **захист інформації**, оскільки всілякі дані, що обробляються і накопичуються обчислювальною технікою, стали останнім часом визначати напрям діяльності та багато інших аспектів життя сучасного соціального організму. За допомогою незаконного володіння інформацією можна здійснювати найрізноманітніші протиправні діяння, наприклад, виробляти незаконний оборот фінансових коштів, отримувати доступ до секретної комерційної інформації та ін.

Слід зазначити, що **конфіденційна інформація** представляє величезний інтерес для конкуруючих фірм. Саме вона стає причиною посягань з боку зловмисників.

З інформаційною безпекою тісно пов'язане і таке поняття, як комерційна таємниця. **Комерційна таємниця** — інформація, яка є секретною у розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які зазвичай мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію. Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці.

Статтею 420 Цивільного кодексу України визначено, що комерційна таємниця є одним з об'єктів інтелектуальної власності. Відповідно майнові права інтелектуальної власності на комерційну таємницю належать особі, яка правомірно визнала інформацію комерційною таємницею, якщо інше не встановлено договором. Умисне розголошення комерційної або банківської таємниці без згоди її власника особою, якій ця таємниця відома у зв'язку з професійною або службовою діяльністю, якщо воно вчинене з корисливих чи інших особистих мотивів і завдало істотної шкоди суб'єкту володіння передбачає кримінальну відповідальність. Законом переслідується не лише роз-

голошення комерційної таємниці, а й приховування її (або надання недостовірної інформації) у тих випадках, коли надання такої інформації передбачено законом.

Багато проблем інформаційної безпеки пов'язані з недооцінкою важливості такої загрози, як конфіденційність інформації. У результаті для держави це може стати економічною кризою. Навіть одиничний випадок халатності суб'єктів інформаційної безпеки може принести їй багатомільйонні збитки, втрату репутації і довіри населення. Щоб цього уникнути, фахівці інформаційної безпеки використовують спеціальне обладнання, яке виробляє аналіз електромагнітних випромінювань, одержуваних під час роботи на комп'ютері. Іноді користувачі можуть спеціально провокувати внутрішній витік інформації, показуючи цим своє невдоволення життям, роботою або владою. Вони запросто можуть передати всю цінну інформацію стороннім державам, спробувати знищити її або навмисне внести у комп'ютери вірус.

Технології забезпечення інформаційної безпеки можна поділити на дві групи:

I група — захищають програмні й апаратні засоби для обробки і зберігання інформації від відмов, порушень, здатних виникнути у результаті випадкової помилки;

II група — захищають програмні й апаратні засоби обробки інформації від всіляких навмисних загроз, які заздалегідь плануються зловмисниками.

Зауважимо, що існує безліч **причин відмови техніки**, яка обробляє інформацію, що є наслідком діяльності агресорів або іншої дії.

Відзначимо найбільш поширені з них:

- старіння і знос деталей апаратного забезпечення, у результаті чого відбувається пошкодження даних;
- комп'ютерні ресурси використовуються некоректним чином;
- в структурі даних з часом накопичується велика кількість різноманітних помилок, що може призвести до їх пошкодження.

Захистити інформацію від різних дефектів апаратної частини просто: слід лише своєчасно здійснювати її діагностику і ремонт. Часто трапляється, що дані пошкоджуються через неправильне використання апаратної частини комп'ютера. Причин тому може бути досить багато, наприклад, недостатня кваліфікація фахівця.

Нерідко причиною псування інформації стає неправильно налаштоване програмне забезпечення. Найчастіше у цьому відіграє роль саме людський фактор. Так, неправильне налаштування систем обробки інформації нерідко призводить до її псування, втрату або розкрадання. Виходом із ситуації може стати робота тільки висококваліфікованого фахівця, який має великий досвід роботи у сфері інформаційних технологій.

Повноцінний захист інформації у державі повинен бути стандартизований і перебувати під повним контролем цілий рік, у реальному часі, у цілодобовому режимі. При цьому система враховує весь життєвий цикл інформації, починаючи з моменту появи і до повного її знищення або втрати значущості для суспільства.

Якісні системи інформаційної безпеки враховують всілякі об'єкти загроз, їх джерела, цілі зловмисників, способи оволодіння інформацією, а також варіанти і засоби захисту. Вони забезпечують повне збереження інформаційного середовища, підтримують функціонування робочих комплексів, вдосконалюють його в інтересах робітничого персоналу.

Для збереження і запобігання втрати даних в індустрії інформаційної безпеки розробляються системи захисту. Їх робота заснована на складних програмних комплексах з широким набором опцій, що запобігають будь-якій втраті даних.

Зазначимо, що специфікою програм є те, що для правильного їх функціонування потрібно розбірлива і налагоджена модель внутрішнього обороту даних і документів. Аналіз безпеки всіх кроків при використанні інформації ґрунтується на роботі з базами даних.

Існує **п'ять рівнів захисту інформації**:

- законодавчий;
- адміністративний;
- апаратно-програмний;
- фізичний;
- морально-етичний.

Тільки в комплексі всі ці рівні спрямовані на усунення загрози безпеки і утворюють **систему захисту інформації**.

Слід зауважити, що з метою захисту інформації кожен користувач зобов'язаний знати і здійснювати такі **заходи**:

1. Контролювати доступ як до інформації в комп'ютері, так і до прикладних програм. Необхідно мати гарантії того, що тільки авторизовані користувачі зможуть мати доступ до інформації і додатків.

2. Процедури авторизації. Адміністратору слід розробити процедури авторизації, що визначають, хто з користувачів може мати доступ до тих чи інших прикладних програм та інформації, і передбачити відповідні заходи щодо впровадження в організацію таких процедур.

3. Захист файлів. Слід розробити процедури з обмеження доступу до файлів: для вказівки типу інформації, що міститься у файлах, і необхідного рівня безпеки використовувати зовнішні та внутрішні мітки; обмежувати доступ в ті приміщення, в яких зберігаються архіви, файли і бібліотеки даних; для обмеження доступу до файлів тільки авторизованих користувачів використовувати організаційні заходи і програмно-апаратні засоби.

4. Захист цілісності інформації. Вводиму інформацію слід піддавати перевіркам на помилки, вона повинна бути авторизованою, повною і точною. Точність інформації необхідно перевіряти за допомогою процедур порівняння отриманих результатів обробки з передбачуваними.

5. Захист системних програм. При розробці програм заходи захисту повинні включати процедури щодо внесення змін до програми, її приймання і тестування до введення в експлуатацію.

6. Впровадження заходів захисту більш ефективно за рахунок залучення спеціалізованих організацій.

7. Розгляд питання про комунікації безпеки. Дані, що передаються по незахищених лініях, можуть бути перехоплені. Безсумнівно, для боротьби з тенденцією зростання злочинів в ІТ-сфері необхідна злагоджена й цілеспрямована організація процесу захисту інформаційних ресурсів. У цьому процесі повинні активно брати участь фахівці, адміністрація, співробітники і користувачі. Це визначає підвищену значимість організаційної сторони питання.

До **захисту інформації** пред'являються певні **вимоги**. Такий захист має бути:

- **безперервний**, оскільки зловмисники постійно шукають можливість для обходу систем захисту інформації;
- **плановий**. Кожна служба здійснює планування шляхом розробки детальних планів захисту інформації у сфері її компетенції і з урахуванням загальних цілей організації;
- **цілеспрямований**. Мають захищатися не всі підряд, а певні об'єкти, що відповідають конкретним цілям;
- **конкретний**. Захищаються дані, що підлягають охороні, при втраті яких може бути завдано певної шкоди організації;
- **активний**. Інформацію необхідно захищати з достатнім ступенем наполегливості;
- **надійний**. Незалежно від форми подання охоронюваних даних, мови їх вираження і виду фізичного носія, на якому вони закріплені, методи і форми захисту повинні надійно перекривати можливі шляхи неправомірного доступу до цих даних;
- **універсальний**. Незалежно від характеру, форми і виду інформації необхідно розумними і достатніми засобами перекривати будь-які види каналів витоку, де б вони не виявлялися;
- **комплексний**. Неприпустимо застосовувати лише окремі форми або технічні засоби для захисту інформації. Всі

види і форми захисту повинні застосовуватися у повному обсязі в усьому різноманітті структурних елементів.

Зазначимо, що **правовий захист інформації** як ресурс визнаний на міжнародному та державному рівнях і підтверджується міждержавними договорами, конвенціями, деклараціями, реалізується патентами, ліцензіями й авторським правом. На державному рівні правовий захист регулюється державними та відомчими актами.

У нашій країні **регуляторами є**: Конституція, закони України, цивільне, адміністративне і кримінальне право. Відомчі нормативні акти визначаються наказами, інструкціями, положеннями та інструкціями, які видаються самими відомствами, організаціями, а також підприємствами, що діють у межах певних структур.

Отже, захисту інформації від неправомірного оволодіння нею відводиться далеко не останнє місце. При цьому **цілями захисту інформації** є:

- запобігання розголошенню, витоку і несанкціонованому доступу до охоронюваних відомостей;
- запобігання протиправних дій з модифікації, знищення, перекручення, блокування і копіювання інформації;
- запобігання інших форм протизаконного втручання в інформаційні системи та інформаційні ресурси;
- забезпечення для документованої інформації правового режиму як для об'єкта власності;
- захист прав громадян, забезпечених Конституцією, на збереження особистої таємниці та конфіденційність персональних даних, які є в інформаційних системах;
- забезпечення конфіденційності документованої інформації і збереження державної таємниці відповідно до чинного законодавства;
- забезпечення прав суб'єктів у всіх інформаційних процесах, а також при розробці, виробництві та використанні інформаційних технологій, систем і засобів їх забезпечення.

Найважливішими на практиці є три аспекти інформаційної безпеки:

- цілісність — захищеність системи від несанкціонованих змін і руйнування;
- доступність — можливість швидко отримати необхідну інформаційну послугу;
- конфіденційність — захищеність від несанкціонованого прочитання.

Створюючи системи захисту інформації в державі, необхідно враховувати наступне.

По-перше, для ефективного захисту інформаційних ресурсів потрібна реалізація низки різноманітних заходів, які можна розподілити на три групи: юридичні, організаційно-економічні й технологічні.

По-друге, хоча розробкою заходів у кожній із трьох груп повинні займатися фахівці відповідних галузей знань, які застосовують свої способи і методи для досягнення заданих цілей, успіх значною мірою буде залежати від того, наскільки у межах системного підходу вдасться визначити і реалізувати взаємні зв'язки між відповідними визначеннями, принципами, способами і механізмами захисту.

Аналіз поглядів і концептуальних підходів до формування сучасних ефективних систем захисту інформації держави дав змогу сформулювати основні **функції та завдання** і намітити організаційні основи функціонування відповідних **підрозділів інформаційної безпеки**. У сучасному поданні рольових функцій служби інформаційної безпеки виділяють **чотири напрями**:

- розробка методології та методик аналізу загроз, оцінка рівня інформаційної безпеки держави і системи її забезпечення;
- організація і здійснення конкретних видів діяльності із захисту інформації;
- експлуатація технічних засобів захисту інформації;
- аудит і контроль функціонування системи інформаційної безпеки держави.

Завдання забезпечення інформаційної безпеки необхідно вирішувати системно. Це означає, що засоби захисту інформації повинні застосовуватися одночасно і під централізованим управлінням. Технології захисту даних ґрунтуються на застосуванні сучасних методів, які запобігають витоку інформації та її втраті.

Сьогодні використовується **шість основних способів захисту: перешкода, маскування, регламентація, управління, примус, спонукання**.

Усі перелічені способи націлені на побудову ефективної технології захисту інформації, при якій виключено витрати через недбалість і успішно відображено різні види загроз.

Під **перешкодою** розуміється спосіб фізичного захисту інформаційних систем, завдяки якому зловмисники не мають можливості потрапити на територію, що охороняється.

Маскування — спосіб захисту інформації, що передбачає перетворення даних у форму, непридатну для сприйняття сторонніми особами. Для розшифровки потрібне знання принципу.

Управління — спосіб захисту інформації, за яким здійснюється управління над всіма компонентами інформаційної системи.

Регламентація — найважливіший метод захисту інформаційних систем, що припускає введення особливих інструкцій, згідно з якими повинні здійснюватися всі маніпуляції з даними, що охороняються.

Примус — метод захисту інформації, тісно пов'язаний з регламентацією, що припускає введення комплексу заходів, за якими працівники змушені виконувати встановлені правила. Коли використовуються способи впливу на працівників, за якими вони виконують інструкції з етичних і особистісних міркувань, то йдеться про спонукання.

Інформаційні системи повинні використовуватися відповідно до чинного законодавства. У більшості випадків законодавство відстає від потреб практики, що створює у суспільстві певну напруженість. Для інформаційних технологій подібне

відставання законів, нормативних актів, національних і галузевих стандартів виявляється особливо болючим.

Отже, у сучасних умовах інформаційна безпека є невід'ємною складовою системи економічної безпеки господарюючого суб'єкта. Своєю чергою, надійне забезпечення інформаційної безпеки є неодмінною умовою переходу на модель стійкого розвитку не тільки окремого підприємства, а й національної економіки загалом.

Контрольні питання

1. Які існують групи методів захисту інформації?
2. У чому полягає роль криптографічних методів у захисті інформації?
3. Які організаційні методи є найефективнішими для державних установ?
4. У чому переваги та недоліки апаратних методів захисту?
5. Як працюють програмні методи забезпечення інформаційної безпеки?
6. Чим відрізняється проактивний і реактивний захист?

Практичне питання

Мета

Опанувати класифікацію та застосування методів захисту.

Практичні завдання

1. Виконати класифікацію методів захисту (організаційні, технічні, криптографічні, фізичні тощо).
2. Порівняти два методи захисту (наприклад, шифрування та автентифікацію), визначити сфери застосування.
3. Проаналізувати приклади використання криптографії у державному секторі.
4. Скласти план комбінованого захисту для невеликої установи (мінімум 6 методів).

Питання для обговорення

Чому жоден метод захисту не є самодостатнім?

Тема 18. Основні складові процесу захисту інформації

Для ефективного впровадження захисту інформації необхідно керуватися певним набором **принципів**:

Класифікація	Характеристика
Абсолютна конфіденційність	Мова йде про спеціальну організацію і подальшу підтримку постійного контролю, який дає змогу гарантувати необхідний рівень безпеки всіх даних. У результаті вдається уникнути незаконного розкрадання інформації. Особливо важливо підтримувати конфіденційність під час кожного пересилання інформації іншим особам або при збереженні даних із всіляких сторонніх джерел
Цілісність	Цілісність передбачає набір певних елементів, які впливають на послідовність отримання інформаційних даних – внутрішню і зовнішню. Якщо своєчасно подбати про цілісність інформації, можна виключити її подальше спотворення на всіх етапах роботи
Доступність	Інформаційну безпеку неможливо уявити без обов'язкової доступності. У результаті вдається організувати безперешкодний доступ до різної інформації конкретній групі осіб. Зазвичай це посадові особи, які мають певні повноваження. Такі користувачі повинні мати можливість отримувати доступ до конфіденційних даних у будь-який час дня і ночі, виконавши необхідні вимоги

Окрім того, захист інформації неможливо уявити без функції оперативного відновлення даних за наявності будь-яких збоїв. Від швидкості такого відновлення системи буде залежати робота всієї системи. Причому збої часто виникають не тільки через те, що сторонні особи спробували зламати систему, а й у результаті технічної помилки всередині цієї системи. Такі ситуації також важливо передбачити, щоб мати можливість вирішити проблему у найкоротші терміни.

Надійний **захист інформаційних даних** — це повноцінний комплекс заходів і всіляких дій різного спрямування (технічні,

правові та організаційні). Усі вони спрямовані на те, щоб запобігти можливим загрозам інформаційної безпеки і усунути їх у разі порушення правил використання інформаційних даних.

Основні **складові інформаційної безпеки** допомагають грамотно організувати роботу всієї системи з урахуванням головних особливостей, які заслуговують на першочергову увагу.

У ролі суб'єктів інформаційних відносин можуть виступати:

- власники підприємств, організацій, яким і належить ця інформація;
- користувачі, які отримали вільний доступ до інформації;
- підтримуючі інфраструктури, які мають право використовувати інформацію у різних цілях.

Однак до категорії підтримуючої інфраструктури відноситься не тільки працюючий персонал. Адже захист інформації в телекомунікаційних системах неможливий без застосування різних комп'ютерів, спеціально обладнаних приміщень, систем тощо.

Система захисту інформації — це єдина сукупність правових і морально-етичних норм, організаційних, технологічних і програмно-технічних засобів, направлених на протидію загроз інформації і системи загалом, з метою зведення до мінімуму втрат інформації.

У національних установах існує **два підходи до захисту інформації**:

- автономний — направлений на захист конкретної ділянки або частини інформаційної системи, яка зазвичай є найбільш вразливою або може бути джерелом зловживань;
- комплексний — захищає інформаційну систему загалом, всі її складові частини, приміщення, персонал тощо.

Важливим елементом попередження комп'ютерних злочинів у фінансовій діяльності стає застосування сучасних технічних засобів захисту інформації (під захистом розуміється обмеження доступу чи використання всієї або частини комп'ютерної системи).

У Положенні про технічний захист інформації в Україні зазначено: **технічний захист інформації** з обмеженим доступом в автоматизованих системах і засобах обчислювальної техніки спрямовано на запобігання порушенню цілісності інформації з обмеженим доступом та її просочення шляхом:

- несанкціонованого доступу;
- приймання й аналізу побічних електромагнітних випромінювань і наводок;
- використання закладних пристроїв;
- впровадження комп'ютерних вірусів та іншого впливу.

Технічний захист інформації з обмеженим доступом в автоматизованих системах і засобах обчислювальної техніки, призначених для формування, пересилання, приймання, перетворення, відображення та зберігання інформації, забезпечується комплексом конструкторських, організаційних, програмних і технічних заходів на всіх етапах їх створення й експлуатації.

Основними методами та засобами технічного захисту інформації з обмеженим доступом в автоматизованих системах і засобах обчислювальної техніки є:

- використання захищеного обладнання;
- регламентування роботи користувачів, технічного персоналу, програмних засобів, елементів баз даних і носіїв інформації з обмеженим доступом (розмежування доступу);
- регламентування архітектури автоматизованих систем і засобів обчислювальної техніки;
- інженерно-технічне оснащення споруд і комунікацій, призначених для експлуатації автоматизованих систем і засобів обчислювальної техніки;
- пошук, виявлення і блокування закладних пристроїв.

До основних засобів захисту інформації можна віднести такі: фізичні, апаратні, програмні, апаратно-програмні, а також криптографічні та організаційні методи.

Фізичні засоби захисту — це засоби, необхідні для зовнішнього захисту засобів обчислювальної техніки, території та

об'єктів на базі ПК, які спеціально призначені для створення фізичних перешкод на можливих шляхах проникнення і доступу потенційних порушників до компонентів інформаційних систем та інформації, що захищаються.

Найпростіший і надійний спосіб захисту інформації від загроз несанкціонованого доступу (НСД) — режим автономного використання ПК одним користувачем у спеціально виділеному приміщенні при відсутності сторонніх осіб. У цьому випадку роль замкненого контуру захисту виконує виділене приміщення, а фізичний захист — вікна, стіни, підлога, стеля, двері. Якщо стіни, стеля, підлога і двері міцні, підлога не має люків, які з'єднуються з іншими приміщеннями, вікна і двері обладнані охоронною сигналізацією, то стійкість захисту буде визначатись технічними характеристиками охоронної сигналізації при відсутності користувача у неробочий час.

У робочий час, коли ПК працює, можливий витік інформації каналами побічного електромагнітного випромінювання. Для усунення такої загрози здійснюються спеціальні дослідження щодо апаратних засобів та їх випромінювання, основним змістом яких є атестування та категорування засобів і об'єктів електронно-обчислювальної техніки (ЕОТ) з видачею відповідного дозволу на експлуатацію. Крім того, двері приміщення повинні бути обладнані механічним або електромеханічним замком.

У деяких випадках, коли відсутня охоронна сигналізація, на період тривалої відсутності користувача ПК для підвищення безпеки доцільно системний блок і машинні носії інформації зберігати у сейфі. Використання у деяких ЕОМ у системі вводу-виводу BIOS апаратного паролю, що блокує завантаження і роботу ПК, не зовсім надійно забезпечує захист від загроз НСД, оскільки при відсутності на корпусі системного блоку механічного замка та самого власника-користувача апаратна частка BIOS-носія паролю може бути замінена на іншу таку саму, оскільки вузли BIOS уніфіковані, але вже з відомим значенням паролю. Саме тому механічний замок, що блокує вмикання і завантаження ПК, найбільш ефективний захід у цьому випадку.

Спектр сучасних фізичних засобів захисту дуже широкий. До нього також належать різні засоби екранування робочих приміщень та каналів передачі даних.

Апаратні засоби захисту — це різні електронні, електронно-механічні та інші пристрої, які вмонтовуються у серійні блоки електронних систем обробки і передачі даних для внутрішнього захисту засобів обчислювальної техніки: терміналів, пристроїв введення та виведення даних, процесорів, ліній зв'язку тощо.

Основні **функції апаратних засобів захисту**:

- заборона несанкціонованого (неавторизованого) зовнішнього доступу віддаленого користувача;
- заборона несанкціонованого (неавторизованого) внутрішнього доступу до баз даних у результаті випадкових чи умисних дій персоналу;
- захист цілісності програмного забезпечення.

Ці функції реалізуються **шляхом**:

- ідентифікації суб'єктів (користувачів, обслуговуючого персоналу) і об'єктів (ресурсів) системи;
- аутентифікації суб'єкта за наданим ним ідентифікатором;
- перевірки повноважень, яка полягає у перевірці дозволу на певні види робіт;
- реєстрації (протоколювання) при звертаннях до заборонених ресурсів;
- реєстрації спроб несанкціонованого доступу.

Реалізація цих функцій здійснюється за допомогою застосування різних технічних пристроїв спеціального призначення. До них зокрема належать:

- джерела безперебійного живлення апаратури, а також: пристрої стабілізації, що оберігають від стрибкоподібних перепадів напруги і пікових навантажень у мережі електроживлення;
- пристрої екранування апаратури, ліній зв'язку та приміщень, в яких знаходиться комп'ютерна техніка;

- пристрої ідентифікації і фіксації терміналів і користувачів при спробах несанкціонованого доступу до комп'ютерної мережі;
- засоби захисту портів комп'ютерної техніки тощо.

Засоби захисту портів виконують декілька захисних функцій, а саме:

- **звірка коду.** Комп'ютер захисту порту звіряє код санкціонованих користувачів з кодом у запиті;
- **камуфляж.** Деякі засоби захисту портів камуфлюють їх існування на лінії телефонного зв'язку шляхом синтезування людського голосу, який відповідає на виклик абонента;
- **дзвінок назустріч.** У пам'яті засобу захисту портів зберігаються не тільки коди доступу, а й ідентифікаційні номери телефонів;
- **ведення автоматичного електронного журналу доступу** в комп'ютерну систему з фіксацією основних дій користувача.

Програмні засоби захисту необхідні для виконання логічних та інтелектуальних функцій захисту, які вмонтовані до складу програмного забезпечення системи.

За допомогою програмних засобів захисту реалізуються такі **задачі безпеки**:

- контроль завантаження та входу в систему за допомогою системи паролів;
- розмежування і контроль прав доступу до системних ресурсів, терміналів, зовнішніх ресурсів, постійних і тимчасових наборів даних тощо;
- захист файлів від вірусів;
- автоматичний контроль за роботою користувачів шляхом протоколювання їх дій.

Апаратно-програмні засоби захисту — це засоби, що основані на синтезі програмних та апаратних засобів. Вони широко використовуються при аутентифікації користувачів автоматизованих банківських систем. **Аутентифікація** — це

перевірка ідентифікатора користувача перед допуском його до ресурсів системи за допомогою його імені або псевдоніма, що бере участь у реєстраційній процедурі, та пароля доступу, що відомий лише користувачу. **Пароль** — це код (набір символів), що забезпечує доступ до систем, файлів, апаратних засобів тощо.

Апаратно-програмні засоби захисту використовуються також при накладанні електронно-цифрових підписів відповідальних користувачів. Найпоширенішим в автоматизованих банківських системах є використання смарт-карт, які містять паролі та ключі користувачів.

Організаційні заходи захисту засобів комп'ютерної інформації складають сукупність заходів щодо підбору, перевірки та навчання персоналу, який бере участь у всіх стадіях інформаційного процесу. Досвід зарубіжних країн свідчить про те, що найефективнішим захистом інформаційних систем є введення до штату організації посади фахівця з комп'ютерної безпеки або створення спеціальних служб як приватних, так і централізованих, виходячи з конкретної ситуації. Наявність такого відділу (служби), за оцінками зарубіжних фахівців, удвічі знижує ймовірність вчинення злочинів у сфері використання комп'ютерних технологій.

Згідно із законодавством України у державних установах та організаціях можуть створюватись підрозділи, служби, які організовують роботу, пов'язану із захистом інформації, підтримкою її рівня захисту в автоматизованих системах і несуть відповідальність за ефективність захисту інформації. Зазначимо, що ця норма за характером є не обов'язковою, а рекомендованою. З її змісту в поєднанні з іншими нормами Закону "Про захист інформації в автоматизованих системах" витікає, що захист інформації в автоматизованих системах є обов'язковою функцією, проте необов'язково під цю функцію може створюватися окрема функціональна організаційна структура. Ця функція може бути складовою іншої організаційної структури, тобто здійснюватися у поєднанні з іншими функціями.

Однак в установах створення спеціальних структур для захисту інформації є обов'язковим. У них мають бути створені спеціальні відділи комп'ютерної безпеки в межах діючих служб економічної безпеки та фізичного захисту, діяльністю яких має керувати один із спеціально призначених для цих цілей фахівець, який має у своєму розпорядженні відповідні людські, фінансові й технічні ресурси для вирішення поставлених завдань.

До функціональних обов'язків зазначених осіб (структурних підрозділів) має входити здійснення передусім таких організаційних заходів:

- забезпечення підтримки з боку керівництва конкретної організації вимог захисту засобів комп'ютерної техніки;
- розробка комплексного плану захисту інформації;
- визначення пріоритетних напрямів захисту інформації з урахуванням специфіки діяльності організації;
- складання загального кошторису витрат фінансування охоронних заходів відповідно до розробленого плану та затвердження його як додатку до плану керівництвом організації;
- визначення відповідальності співробітників організації за безпеку інформації у межах встановленої компетенції шляхом укладення відповідних договорів між співробітником та адміністрацією;
- розробка, впровадження і контроль за виконанням різного роду інструкцій, правил та наказів, які регламентують форми допуску, рівні секретності інформації, конкретних осіб, допущених до роботи з секретними (конфіденційними) даними тощо;
- розробка ефективних заходів боротьби з порушниками захисту засобів комп'ютерної техніки.

Надійним засобом підвищення ефективності заходів інформаційної безпеки є навчання та інструктаж працюючого персоналу щодо організаційно-технічних заходів захисту, які застосовуються у конкретній організації.

Крім цього, обов'язково мають бути реалізовані такі **організаційні заходи**:

- для всіх осіб, які мають право доступу до засобів комп'ютерної техніки, потрібно визначити категорії допуску, тобто коло службових інтересів певної особи, види інформації, до яких вона має право доступу, а також: вид такого дозволу, правомочність особи, яка уповноважується для здійснення тих або інших маніпуляцій із засобами комп'ютерної техніки;
- слід визначити адміністративну відповідальність за збереження і санкціонування доступу до інформаційних ресурсів, при цьому за кожний вид ресурсів відповідальність повинна нести одна конкретна особа;
- налагодити періодичний системний контроль за якістю захисту інформації шляхом проведення регламентних робіт як особою, відповідальною за безпеку, так і залученням компетентних фахівців (експертів) з інших організацій;
- провести класифікацію інформації відповідно до її важливості, диференціювати на основі цього заходи захисту;
- визначити порядок охорони та знищення інформації;
- організувати фізичний захист засобів комп'ютерної техніки.

Криптографічні методи захисту. З метою захисту інформації при її передачі зазвичай використовують різні методи шифрування даних перед їх введенням до каналу зв'язку або на фізичний носій з наступною розшифровкою. Методи шифрування дають змогу досить надійно захищати комп'ютерну інформацію від злочинних посягань.

Застосування криптографічного захисту, тобто кодування тексту за допомогою складних математичних алгоритмів, завойовує все більшу популярність. Зазвичай жоден з шифрувальних алгоритмів не дає цілковитої гарантії захисту від зловмисників, але деякі методи шифрування настільки складні, що ознайомитися зі змістом зашифрованих повідомлень практично неможливо.

Основні **криптографічні методи захисту**:

- шифрування за допомогою датчика псевдовипадкових чисел, яке полягає у тому, що генерується гамма шифру за допомогою датчика псевдовипадкових чисел і накладається на відкриті дані з урахуванням зворотності процесу;
- шифрування за допомогою криптографічних стандартів шифрування даних (із симетричною схемою шифрування), в основі якого використовуються перевірені та випробувані алгоритми шифрування даних з великою криптостійкістю;
- шифрування за допомогою пари ключів (з асиметричною системою шифрування), в яких один ключ є відкритим і використовується для шифрування інформації, а другий ключ — закритим і використовується для розшифрування інформації.

Потужним та дієвим є криптозахист, тобто система, що дає змогу шифрувати та дешифрувати інформаційні потоки. Традиційна криптографія виходила з того, що для шифрування та дешифрування використовувався один і той самий секретний ключ, який повинен мати відправник повідомлення і отримувач. Одним із поширених сьогодні методів шифрування є алгоритм RSA, в основі якого кожен учасник процесу має власний таємний ключ та відкритий ключ, що не є секретним, за допомогою якого проводиться обмін повідомленнями.

Електронний цифровий підпис (ЕЦП) — це аналог власного підпису посадової особи в електронному вигляді.

Криптографічні методи захисту інформації широко використовуються в автоматизованих банківських системах і реалізуються у вигляді апаратних, програмних чи програмно-апаратних методів захисту. Використовуючи шифрування повідомлень у поєднанні з правильною установкою комунікаційних засобів, належними процедурами ідентифікації користувача, можна добитися високого рівня захисту інформаційного обміну.

Криптографія є одним з найкращих засобів забезпечення конфіденційності та контролю цілісності інформації. Вона займає центральне місце серед програмно-технічних регулювальників безпеки, є основою реалізації багатьох з них і водночас останнім захисним рубежем.

Отже, підкреслимо, що деякі фахівці з інформаційної безпеки пов'язують надійність фінансових інформаційних систем із засобами їх зовнішнього захисту, тобто системою паролів для входу не тільки у саму комп'ютерну мережу, а й до різних рівнів інформації системи залежно від допуску користувачів. Коло працівників, які за технологією виконання операцій мають доступ до широкого діапазону такої інформації, дуже великий. Тому система захисту, яка базується на кодуванні входів до різних видів інформації, малоефективна. Потрібно знайти принципово нові підходи для розробки та впровадження відносно надійних систем захисту національної діяльності від комп'ютерних злочинів. Така система повинна будуватися згідно із технологією документообігу та особливостями форм операцій.

Підсумовуючи практичні поради щодо захисту інформації споживачів, варто пригадати такий величезний масив даних, як мобільні **месенджери** або власні **онлайн акаунти**.

Кожен користувач може дізнатись про **витоки його даних** із онлайн акаунтів та месенджерів через шахраїв та злочинців, скануючи даркнет або на таких сайтах:

- Have I been pwned?;
- Google password manager;
- Google dark web check.

Доступ до месенджерів та онлайн акаунтів власником можна втратити через:

- перехоплення коду з СМС, який користувач пересилає на вимогу зловмисників, що маскуються під інтернет-магазини або акції;
- злам за допомогою фішингу, отримання персональних даних через онлайн аукціони, сервісів із переказу або обміну валюти;

- втрату доступу до власного пристрою шляхом переходу до шкідливих посилань, передаючі керування пристрою зловмисникам.

Захист месенджерів та онлайн акаунтів повинен складатися із таких складників, що можуть застосовуватись усі разом або окремо (поодинці):

- двофакторна автентифікація запровадження;
- використання унікального паролю;
- впровадження резервної електронної пошти;
- використання пристроїв або активних сесій;
- фізичний захист або збереження мобільного пристрою;
- не обов'язково, можна створювати резервні копії даних із месенджеру.

Проте власні паролі краще зберігати ніж запам'ятовувати. Для цього варто використовувати: парольний менеджер, браузер, нотатки під паролем, записник та ін.

Контрольні питання

1. Які етапи включає процес захисту інформації?
2. Чому аналіз ризиків є першочерговим у процесі захисту?
3. Які заходи входять до етапу впровадження системи захисту?
4. У чому полягає моніторинг інцидентів безпеки?
5. Що таке аудит інформаційної безпеки та які його цілі?
6. Чому важливою є безперервність процесу захисту інформації?

Практичне питання

Мета

Засвоїти процеси, етапи та інструменти захисту.

Практичні завдання

1. Побудувати модель процесу захисту інформації (аналіз ризиків → планування → впровадження → моніторинг → аудит).

2. Проаналізувати роль аудиту ІБ у безперервності процесу захисту (на прикладах).
3. Скласти перелік заходів для етапу моніторингу інцидентів.
4. Розробити приклад політики реагування на порушення безпеки (інцидент).

Питання для обговорення

Який з етапів процесу захисту є найскладнішим у реалізації?

Тема 19. Аналіз об'єктів захисту інформації

З огляду на основні складові процесу захисту інформації, додатково потрібно ознайомитися з об'єктами такого захисту. До стандартного **переліку об'єктів** включені:

Класифікація	Характеристика
Усі різновиди популярних ресурсів	Інформаційні ресурси або документована інформація – спеціальні дані, які зафіксовані на відповідному матеріальному носії. Причому цей носій обов'язково повинен мати конкретні реквізити для майбутнього процесу ідентифікації конфіденційної інформації
Системи, що впливають на формування громадської думки	До цього переліку відносяться ЗМІ, соціальні інститути та інші інстанції, які взаємодіють з широкою аудиторією
Права громадян, держави	Йдеться про юридичних та фізичних осіб, які отримали право на подальше використання, поширення інформаційних даних з конкретною метою.
Система, що дає змогу працювати з інформацією	Така система допомагає обробляти, збирати, поширювати і всіляко використовувати інформацію. Під цими системами прийнято розглядати архіви, бібліотеки, інформаційні технології та ін.

Однією з відмінних, визначних ознак сучасного світового соціального прогресу є зростання значимості інформації у суспільних відносинах.

Суспільні інформаційні відносини постійно розвиваються, особливо з удосконаленням техніки та технологій збирання, обробки, зберігання та передавання інформації. Зазначені процеси визначають сутність інформаційного суспільства. Поряд із позитивними здобутками в інформаційному суспільстві виникли соціальні проблеми криміногенного характеру, які потребують вирішення.

На сучасному етапі можна виокремити **три підходи** до рішення проблем інформаційної безпеки:

- **приватний**, який ґрунтується на рішенні приватних завдань забезпечення інформаційної безпеки. Цей підхід є малоефективним, але досить часто використовується, оскільки не вимагає значних фінансових та інтелектуальних витрат;
- **комплексний**, який ґрунтується на рішенні комплексу приватних завдань єдиної програми. Цей підхід наразі є основним;
- **інтегральний**, який заснований на інтеграції різних підсистем зв'язку, підсистем забезпечення безпеки в єдину систему із загальними технічними засобами, каналами зв'язку, програмним забезпеченням і базами даних.

Інтегральний підхід спрямований на досягнення інтегральної інформаційної безпеки. Поняття **інтегральної безпеки** припускає обов'язкову безперервність процесу забезпечення безпеки як у часі, так і просторі (за всім технологічним циклом діяльності) з обов'язковим обліком усіх можливих видів загроз (несанкціонований доступ, знімання інформації, тероризм, пожежа, стихійні лиха та ін.).

Застосування інтегрального підходу пов'язане з рішенням низки складних різнопланових окремих завдань у їх тісному взаємозв'язку. Найбільш очевидними з них є завдання обмеження доступу до інформації, технічного й криптографічного

закриття інформації, обмеження рівнів паразитних випромінювань технічних засобів, технічної захищеності об'єктів, охорони й оснащення їх тривожною сигналізацією. Однак необхідні рішення й інших, не менш важливих завдань.

Так, наприклад, виведення з ладу керівників держави, членів їхніх родин або ключових управлінців може поставити під сумнів саме існування даної країни. Цьому ж можуть сприяти стихійні лиха, аварії, тероризм та ін.

Необхідною умовою реалізації інтегрального підходу є блокування всіх технічних каналів витоку й несанкціонованого доступу до інформації. Тому для створення ефективних систем безпеки насамперед необхідно досліджувати можливі канали витоку та їх характеристики, тобто проводити аналіз загроз (ризиків) як реальних (діючих у цей момент), так і потенційних (здатних у майбутньому).

Захист інформації — це сукупність організаційних, технічних та правових заходів, спрямованих на запобігання нанесенню збитків інтересам власника інформації. Основними об'єктами захисту інформації є:

1. **Інформація з обмеженим доступом** (ІзОД), тобто інформаційні ресурси, що містять відомості, які належать або до таємної, або до конфіденційної інформації.
2. **Технічні засоби приймання, обробки, зберігання та передання інформації** (ТЗПІ), а саме:
   - системи та засоби інформатизації (обчислювальна техніка, інформаційно-обчислювальні комплекси, мережі та системи);
   - програмні засоби (операційні системи, системи керування базами даних та інше загально системне і прикладне програмне забезпечення);
   - автоматизовані системи керування;
   - системи зв'язку;
   - технічні засоби отримання, передання та обробки ІзОД (звукозапис, звукопідсилення, звукосупроводження, переговорні та телевізійні пристрої);

- засоби тиражування і виготовлення документів та інші технічні засоби обробки графічної, алфавітно-цифрової та текстової інформації), їх інформативні фізичні поля.

3. **Допоміжні технічні засоби і системи** (ДТЗС), тобто технічні засоби і системи, які не належать до ТЗПІ, але розташовані в приміщеннях, де оброблюється ІзОД. До них відносять технічні засоби відкритого телефонного або гучномовного зв'язку, системи пожежної та охоронної сигналізації, система енергопостачання, радіотрансляційна мережа, система годинофікації, енергопобутові прилади тощо, а також самі приміщення, де циркулює ІзОД.

За результатами аналізу матеріалів вітчизняних і закордонних досліджень узагальнимо схему можливих каналів витоку і несанкціонованого доступу до інформації, оброблюваної в типовому одноповерховому приміщенні.

1. Витік за рахунок структурного звуку в стінах і перекриттях.
2. Знімання інформації зі стрічки принтера, погано стертих дискет і т. п.
3. Знімання інформації з використанням відеозакладок.
4. Програмно-апаратні закладки в ПЕОМ.
5. Радіозакладки в стінах і меблях.
6. Знімання інформації з системи вентиляції.
7. Лазерне знімання акустичної інформації з вікон.
8. Виробничі й технологічні відходи.
9. Комп'ютерні віруси, логічні бомби й т. п.
10. Знімання інформації за рахунок наведень і нав'язування.
11. Дистанційне знімання відеоінформації (оптика).
12. Знімання акустичної інформації з використанням диктофонів.
13. Розкрадання носіїв інформації.
14. Високочастотний канал витоку в побутовій техніці.
15. Знімання інформації спрямованим мікрофоном.
16. Внутрішні канали витоку інформації (через обслуговуючий персонал).
17. Несанкціоноване копіювання.

18. Витік за рахунок побічного випромінювання термінала.
19. Знімання інформації за рахунок використання “телефонного вуха”.
20. Знімання з клавіатури й принтера акустичним каналом.
21. Знімання з дисплея по електромагнітному каналу.
22. Візуальне знімання з дисплея й принтера.
23. Наведення на лінії комунікацій і сторонні провідники.
24. Витік через лінії зв’язку.
25. Витік мережею заземлення.
26. Витік мережею годинофікації.
27. Витік трансляційною мережею й гучномовним зв’язком.
28. Витік охоронно-пожежною сигналізацією.
29. Витік мережею електроживлення.
30. Витік мережею опалення, газо- і водопостачання.

Розглянемо більш докладно особливості каналів витоку і несанкціонованого доступу до інформації. Як елементи каналів витоку інформації найбільший інтерес становлять ТЗПІ та ДТЗС із виходом за межі контрольованої зони (КЗ), тобто зони, де виключена можливість появи осіб чи транспортних засобів без постійних чи тимчасових перепусток. Окрім з’єднувальних ліній ТЗПІ та ДТЗС за межі КЗ можуть виходити дроти та кабелі, які їх не стосуються, але проходять через приміщення, де встановлено такі технічні засоби, а також металеві труби опалення, водопостачання та інші струмопровідні металоконструкції. Такі дроти, кабелі та струмопровідні елементи називають сторонніми провідниками.

Перехоплення інформації, оброблюваної на об’єктах ТЗПІ, здійснюється технічними каналами. Під **технічнім каналом витоку інформації** (ТКВІ) розуміють сукупність об’єкта розвідки, **технічного засобу розвідки** (ТЗР), за допомогою якого отримують інформацію про цей об’єкт, та фізичного середовища, в якому поширюється інформаційний сигнал.

По суті, **ТКВІ** — це спосіб отримання за допомогою ТЗР інформації про об’єкт розвідки. При цьому форма подання інформації може бути довільною.

Сигнали є матеріальними носіями інформації. За своєю фізичною природою вони можуть бути електричними, електромагнітними, акустичними, оптичними тощо. Залежно від природи сигнали поширюються у визначених фізичних середовищах – газових, рідинних, твердих (наприклад, у повітрі, конструкціях будівель, струмопровідних кабелях та дротах, заземленому ґрунті тощо). Принцип утворення небезпечних сигналів у технічних засобах полягає в тому, що кожний технічний засіб містить ті чи інші фізичні перетворювачі, функції яких засновані на різних фізичних принципах дії. Лише маючи уявлення про принцип дії кожного з таких перетворювачів, можна виявити неконтрольовані вияви фізичних полів, що утворюють канали витоку.

Розглянемо спочатку електромагнітні, електричні й параметричні технічні канали витоку інформації. Через електромагнітні ТКВІ перехоплюють:

- побічні електромагнітні випромінювання (ПЕМВ) елементів ТЗПІ;
- ПЕМВ на частотах роботи високочастотних генераторів ТЗПІ й ДТЗС;
- ПЕМВ на частотах самозбудження низької частоти підсилювачів (ТЗПІ).

Побічні електромагнітні випромінювання ТЗПІ перехоплюють засобами радіотехнічної розвідки, розміщеними за межами КЗ. Електричні ТКВІ слугують для знімання:

- наведених сигналів ПЕМВ ТЗПІ зі з'єднувальних ліній ДТЗС і сторонніх провідників;
- інформаційних сигналів з ліній електроживлення ТЗПІ;
- інформаційних сигналів з мереж заземлення ТЗПІ і ДТЗС;
- інформації шляхом розміщення у ТЗПІ електронних пристроїв перехоплення інформації.

Останні іноді називають закладними пристроями або апаратними закладками. Вони є мініпередавачами, сигнали від яких модулюються інформаційними сигналами.

Параметричні ТКВІ створюють ВЧ опроміненням ТЗПІ. Для перехоплення інформації цими каналами потрібні ВЧ генерато-

ри з антенами, що мають вузьку діаграму спрямованості, а також спеціальні радіоприймальні пристрої.

У повітряних (прямих акустичних) ТКВІ середовищем поширення є повітря. Для перехоплення акустичних сигналів використовують мікрофони. Сигнали з мікрофонів або записуються на пристрої звукозапису, або транслюються передавачами на пункти приймання.

Для перехоплення акустичної (мовної) інформації використовують:

- портативні диктофони та дротові мікрофони для прихованого звукозапису;
- спрямовані мікрофони;
- акустичні радіозакладки для передавання інформації по радіоканалу;
- акустичні мережні закладки для передавання сигналів по лініях силових мереж електроживлення;
- акустичні ІЧ закладки для передавання інформації по оптичному каналу в ІЧ діапазоні;
- акустичні телефонні закладки для передавання інформації по телефонних лініях зв'язку на підвищених частотах;
- акустичні телефонні закладки типу "електронне вухо" для передавання інформації по телефонній лінії "телефону-спостерігачу" на низькій частоті.

У вібраційних (віброакустичних) ТКВІ середовищем поширення акустичних сигналів є конструкційні елементи споруд і будівель (стіни, перекриття, підлога), труби водопостачання, каналізації та інші тверді тіла.

Для перехоплення акустичних коливань через вібраційні ТКВІ використовують ТЗР із контактними мікрофонами:

- електронні стетоскопи;
- радіостетоскопи (для передавання інформації радіоканалом).

Акустичні ТКВІ виникають за рахунок перетворення акустичних сигналів у електричні (акустоелектричні перетворення) і

дають змогу перехоплювати акустичні коливання через ДТЗС із мікрофонним ефектом, а також ВЧ нав'язуванням. Наприклад, приєднуючи такі ДТЗС до ліній зв'язку телефонних апаратів з електромеханічним дзвінком виклику, можна підслуховувати розмови у приміщеннях, де розміщені такі апарати.

Створити ТКВІ методом ВЧ нав'язування можна шляхом несанкціонованого контактного введення ВЧ струму від генератора, підключеного до лінії (кола), яка має функціональний зв'язок з нелінійним чи параметричним елементом ДТЗС, на яких здійснюється модуляція ВЧ сигналу інформаційним. Останній в елементах ДТЗС з'являється внаслідок акусто-електричного перетворення акустичних сигналів у електричні.

У зв'язку з тим, що нелінійні або параметричні елементи ДТЗС для ВЧ сигналу зазвичай являють собою неузгоджені навантаження, промодульований ВЧ сигнал буде випромінюватися або відбиватися від нього і поширюватись у зворотному напрямку по лінії. Для приймання випроменених або відбитих ВЧ сигналів використовують спеціальні високочутливі приймачі.

Оптико-електричний (лазерний) ТКВІ утворюється під час опромінення лазерним променем вібруючих в акустичному полі тонких відбиваючих поверхонь — скляних вікон, картин, дзеркал і т. п. Для перехоплення мовної інформації таким каналом використовують складні лазерні акустичні локаційні системи (ЛАЛС). Іноді їх називають лазерними мікрофонами.

Параметричні ТКВІ утворюються під час ВЧ опромінення приміщення, де вмонтовані напівактивні закладні пристрої або технічні засоби з елементами, деякі параметри яких змінюються за законом зміни акустичного (мовного) сигналу. Для перехоплення інформації таким каналом потрібен спеціальний передавач із направленим променем і приймач.

Необхідно зазначити, що акустичний канал може бути джерелом витоку не тільки мовної інформації. У літературі описані випадки, коли за допомогою статистичної обробки акустичної інформації з принтера або клавіатури вдавалося перехоплюва-

ти комп'ютерну текстову інформацію, у тому числі здійснювати знімання інформації із системи вентиляції.

Особливий інтерес представляє перехоплення інформації при її передачі каналами зв'язку. Зазвичай у цьому випадку є вільний несанкціонований доступ до переданих сигналів.

Залежно від виду каналів зв'язку, **технічні канали перехоплення інформації можна розділити на електромагнітні, електричні й індукційні**. Електромагнітні випромінювання передавачів засобів зв'язку, які модульовані інформаційними сигналами, можуть перехоплюватися з використанням стандартних технічних засобів. Цей електромагнітний канал перехоплення інформації широко використовується для прослуховування телефонних розмов, що ведуться за допомогою радіотелефонів, стільникових телефонів або радіорелейними і супутниковими лініями зв'язку. Електричний канал перехоплення інформації, що передається кабельними лініями зв'язку, припускає контактне підключення до цих ліній. Цей канал найчастіше використовується для перехоплення телефонних розмов, при цьому перехоплюється інформація, що може бути записана на диктофон або передана радіоканалом.

Безпосереднє електричне підключення апаратури перехоплення є компрометуючою ознакою, тому частіше використовується індукційний канал перехоплення, що не потребує контактного підключення до каналів зв'язку. Сучасні індукційні датчики здатні знімати інформацію з кабелів, захищених не тільки ізоляцією, а й подвійною бронею зі сталевих стрічки й дроту, що щільно обвивають кабель.

Останнім часом значну увагу становлять канали витоку графічної інформації, що реалізуються технічними засобами у вигляді зображень об'єктів або копій документів, які одержуються шляхом спостереження за об'єктом, зйомкою об'єкта та зйомкою (копіюванням) документів. Залежно від умов спостереження використовуються відповідні технічні засоби, у тому числі: оптика (біноклі, підзорні труби, телескопи, монокуляри), телекамери, прилади нічного бачення, тепловізори та ін.

Для документування результатів спостереження проводиться зйомка об'єктів, для чого використовуються фотографічні й телевізійні засоби, що відповідають умовам зйомки. Для зняття копій документів використовуються електронні й спеціальні (закамуфльовані) фотоапарати. Для дистанційного знімання видової інформації використовують відеозакладки.

Розглянуті методи одержання інформації засновані на використанні **зовнішніх каналів витоку**.

Необхідно, однак, коротко зупинитися й на **внутрішніх каналах витоку інформації**, тим більше, що їм не приділяють належної уваги. **Внутрішні канали витоку** зв'язані зазвичай з адміністрацією та обслуговуючим персоналом, з якістю організації режиму роботи. З них насамперед слід зазначити такі канали, як розкрадання носіїв інформації, знімання інформації зі стрічки принтера й погано стертих дискет, використання виробничих і технологічних відходів, візуальне знімання інформації з дисплея й принтера, несанкціоноване копіювання та ін.

Методи й засоби блокування каналів витоку інформації. Захист інформації від витоку технічними каналами забезпечують проєктно-архітектурними рішеннями, проведенням організаційних і технічних заходів, а також виявленням портативних закладних пристроїв.

Організаційні заходи — це спрямовані на захист інформації заходи, проведення яких не потребує спеціально розроблених технічних засобів. До основних організаційних заходів відносять:

- залучення до робіт для захисту інформації організацій, що мають ліцензії відповідних органів на діяльність у сфері технічного захисту інформації (ТЗІ);
- категорування й атестацію об'єктів ТЗПІ та приміщень, виділених для проведення секретних заходів (виділених приміщень) щодо відповідності вимогам забезпечення захисту інформації під час проведення робіт з відомостями відповідного ступеня секретності;
- використання на об'єкті сертифікованих ТЗПІ та ДТЗС;

- встановлення КЗ навколо об'єкта;
- залучення до робіт із монтування апаратури, будування чи реконструкції об'єктів ТЗПІ організацій з відповідними ліцензіями;
- організацію контролю та обмеження доступу на об'єкти ТЗПІ та у виділені приміщення;
- введення територіальних, частотних, енергетичних, просторових і часових обмежень у режимах використання технічних засобів, що підлягають захисту;
- відключення технічних засобів, що мають елементи властивостей електроакустичних перетворювачів, від ліній зв'язку на період проведення секретних заходів.

Технічні заходи — це спрямовані на захист інформації заходи, проведення яких передбачає використання спеціальних технічних засобів, а також реалізацію технічних рішень. Технічні заходи слугують для закриття каналів витоку інформації за рахунок ослаблення рівня інформаційних сигналів або зменшення відношення сигнал/завада у місцях можливого розміщення ТЗР або їх датчиків до рівнів, що унеможливлюють виділення інформаційних сигналів засобами розвідки. Під час проведення таких заходів використовують активні та пасивні методи.

До технічних заходів із використанням пасивних методів відносять такі:

- контроль і обмеження доступу на об'єкти ТЗПІ та у виділені приміщення (установлення на об'єктах ТЗПІ та у виділених приміщеннях технічних засобів та систем обмеження і контролю доступу);
- локалізація випромінювання:
  - екранування ТЗПІ та з'єднувальних ліній;
  - заземлення ТЗПІ та екранів їх з'єднувальних ліній;
  - звукоізолювання виділених приміщень;
- розв'язування інформаційних сигналів:
  - установлення спеціальних захисних засобів типу Граніт, Рікас у ДТЗС із мікрофонним ефектом і таких, що мають вихід за межі КЗ;

- установлення спеціальних діелектричних вставок в обплетення кабелів електроживлення, труб систем опалення, водозабезпечення і каналізації, що виходять за межі КЗ;
- установлення автономних або стабілізованих пристроїв електроживлення ТЗПІ (наприклад, мотор-генераторів);
- установлення у мережах електроживлення ТЗПІ, а в лініях освітлювальної та розеткової мережі виділених приміщень
- завадоподавляючих фільтрів типу ФП, ФСП, ФС-2.

До технічних заходів із використанням активних методів належать такі:

- просторове зашумлення:
  - просторове електромагнітне зашумлення з використанням генераторів шуму або створення прицільних завад відповідними засобами (за умови виявлення та з'ясування частоти випромінювання закладного пристрою або ПЕМВ ТЗПІ);
  - створення акустичних і вібраційних завад із використанням генераторів акустичного шуму — шумотронів;
  - подавлення працюючих у режимі запису диктофонів за допомогою подавляючих пристроїв;
- лінійне зашумлення:
  - мереж електроживлення та кіл заземлення;
  - сторонніх дротів та з'єднувальних ліній ДТЗС, що виходять за межі КЗ;
- знешкодження підключених до лінії закладних пристроїв за допомогою спеціальних генераторів імпульсів (випалювачів "жучків").

Виявити закладні пристрої можна завдяки спеціальним обстеженням (візуальний огляд без залучення технічних засобів) і спеціальним перевіркам (із використанням технічних засобів) об'єктів ТЗПІ та виділених приміщень.

Для виявлення закладних пристроїв використовують:

- пасивні методи:
  - установлення засобів і систем виявлення лазерного випромінювання (підсвітлення скла на вікнах);
  - установлення стаціонарних детекторів диктофонів;
  - розшук закладних пристроїв за допомогою індикаторів поля, інтерсепторів, частотомірів, сканувальних приймачів та програмно-апаратних комплексів контролю;
  - організація радіоконтролю (постійно або на час проведення конфіденційних заходів) побічних електромагнітних випромінювань ТЗПІ;
- активні методи:
  - спеціальна перевірка виділених приміщень із використанням нелінійних локаторів;
  - спеціальна перевірка виділених приміщень, ТЗПІ та ДТЗІ з використанням рентгенівських комплексів.

Таким чином, ефективний захист інформації досягається комплексним застосуванням апаратних, програмних, криптографічних методів і засобів захисту, а також організаційних заходів.

Бурхливий розвиток сучасних технологій і технічних засобів сприяє постійному розширенню спектра можливих каналів витоку інформації, тому дослідження каналів витоку стає все більше актуальним і складним завданням. На ефективність систем захисту інформації істотно впливають характеристики каналів витоку інформації, тому створення систем ефективного захисту має відбуватися з урахуванням особливостей реальних каналів.

Цей висновок не є тривіальним, як може здатися на перший погляд. Наприклад, сам факт наявності випромінювання дисплея ще не говорить про витік інформації. Усе визначається конкретним рівнем напруженості поля за межами зони безпеки й технічних можливостей противника, тому остаточний висновок про витік інформації може зробити тільки кваліфікований фахівець, який використовує спеціальні технічні засоби.

Отже, особливості реальних каналів витоку інформації можуть бути успішно використані й противником для забезпечення несанкціонованого доступу до інформації, про що необхідно постійно пам'ятати. Так, знімання інформації з акустичних каналів може бути здійснено через скло вікон, будівельні, сантехнічні, вентиляційні, теплотехнічні й газорозподільні конструкції з використанням для передачі сигналів радіо, радіотрансляційних, телефонних і комп'ютерних комунікацій, антенних і телевізійних розподільних мереж, охоронно-пожежної й тривожної сигналізації, мереж електроживлення й годинофікації, гучномовного й диспетчерського зв'язку, ланцюгів заземлення тощо. Випадковий пропуск хоча б одного можливого каналу витоку може звести до нуля всі витрати й зробити систему захисту інформації неефективною.

Контрольні питання

1. Які об'єкти можуть бути об'єктами захисту інформації?
2. Як визначають критичність об'єктів захисту?
3. У чому полягає аналіз інформаційних потоків?
4. Як класифікують інформаційні ресурси за значимістю?
5. Які методи використовуються для оцінки вразливостей об'єктів?
6. Чому важливо розглядати людський фактор під час аналізу об'єктів захисту?

Практичне питання

Мета

Навчитися визначати об'єкти захисту та аналізувати їх критичність.

Практичні завдання

1. Визначити об'єкти захисту у державному органі (інформаційні ресурси, персональні дані, техніка, мережі, люди).
2. Провести класифікацію об'єктів за важливістю (критичні — важливі — допоміжні).

3. Оцінити вразливості об'єктів (мінімум 5 прикладів).
4. Проаналізувати роль людського фактора як об'єкта і джерела ризику.

Питання для обговорення

Чому правильна класифікація об'єктів визначає ефективність всього захисту?

Тема 20. Класифікація загроз захисту інформації

Інформаційна загроза — загрози викрадення, зміни або знищення інформації.

Безпека інформації — це стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації. Багаторічний досвід захисту інформації в інформаційно-комунікаційних системах (ІКС) дозволив визначити головні властивості інформації, збереження яких дає змогу гарантувати збереження цінності інформаційних ресурсів, — це конфіденційність, цілісність і доступність інформації.

Загроза — будь-які обставини чи події, що можуть спричинити порушення політики безпеки інформації та нанесення збитку ІКС. Тобто загроза — це будь-який потенційно можливий несприятливий вплив.

До можливих загроз захисту інформації відносять:

- стихійні лиха й аварії;
- збої та відмови устаткування;
- наслідки помилок проєктування і розроблення компонентів автоматизованих систем (надалі АС);
- помилки персоналу під час експлуатації;
- навмисні дії зловмисників і порушників.

Класифікація загроз за ознаками

Ознака класифікації	Причина, спрямованість, характеристика загроз
1	2
Природа виникнення	Природні загрози (виникають через впливи на АС та її компоненти об'єктивних фізичних процесів або стихійних природних явищ, що не залежать від людини). Штучні загрози (викликані діяльністю людини)
Принцип несанкціонованого доступу (НСД)	Фізичний доступ: • подолання рубежів територіального захисту і доступ до незахищених інформаційних ресурсів; • розкрадання документів і носіїв інформації; • візуальне перехоплення інформації, виведеної на екрани моніторів і принтерів; • підслуховування; • перехоплення електромагнітних випромінювань. Логічний доступ: доступ із використанням засобів комп'ютерної системи
Мета НСД	Порушення конфіденційності (розкриття інформації). Порушення цілісності (повне або часткове знищення інформації, спотворення, фальсифікація, викривлення). Порушення доступності (наслідок — відмова в обслуговуванні)
Причини появи вразливостей різних типів	Недоліки політики безпеки. Помилки адміністративного керування. Недоліки алгоритмів захисту. Помилки реалізації алгоритмів захисту
Характер впливу	Активний (внесення змін в АС). Пасивний (спостереження)
Режим НСД	За постійної участі людини (в інтерактивному режимі) можливе застосування стандартного ПЗ. Без особистої участі людини (у пакетному режимі) найчастіше для цього застосовують спеціалізоване ПЗ

1	2
Місцезнаходження джерела НСД	Внутрішньосегментне (джерело знаходиться у локальній мережі). У цьому випадку зазвичай ініціатор атаки – санкціонований користувач. Міжсегментне: • несанкціоноване вторгнення з відкритої мережі в закриту; • порушення обмежень доступу з одного сегмента закритої мережі в інший
Наявність зворотного зв'язку	Зі зворотним зв'язком (атакуючий отримує відповідь системи на його вплив). Без зворотного зв'язку (атакуючий не отримує відповіді)
Рівень моделі взаємодії відкритих систем OSI (Open Systems Interconnection)	Вплив може бути здійснено на таких рівнях: фізичному, канальному, мережевому, транспортному, сеансовому, представницькому, прикладному, тобто на всіх рівнях моделі OSI

Класифікація інформаційних атак за кінцевим результатом

Це спрощена класифікація, що відображає найбільш типові атаки на розподілені автоматизовані системи. Цю класифікацію було запропоновано Пітером Меллом (Peter Mell):

- **віддалене проникнення**. Атаки, які дають змогу реалізувати віддалене керування комп'ютером через мережу. Приклади програм, що реалізують цей тип атак: NetBus, BackOrifice;
- **локальне проникнення**. Атаки, що призводять до отримання несанкціонованого доступу до вузлів, на яких вони ініційовані. Приклад програми, що реалізує цей тип атак: GetAdmin;
- **віддалена відмова в обслуговуванні**. Атаки, що дають можливість порушити функціонування системи або перенавантажити комп'ютер через мережу (зокрема через інтернет). Приклади атак цього типу: Teardrop, trinOO;
- **локальна відмова в обслуговуванні**. Атаки, що дають змогу порушити функціонування системи або перена-

вантажити комп'ютер, на якому їх ініційовано. Приклади атак цього типу: аплет, який перенавантажує процесор (наприклад, відкривши багато вікон великого розміру), що унеможливлює оброблення запитів інших програм.

Класифікація атак за способом здійснення:

- **сканування мережі**. Аналіз топології мережі та активних сервісів, доступних для атаки. Атака може бути здійснена за допомогою службового програмного забезпечення, наприклад за допомогою утиліти nmap;
- **використання сканерів уразливостей**. Сканери вразливостей призначені для пошуку вразливостей на локальному або віддаленому комп'ютері. Такі сканери системні адміністратори застосовують як діагностичні інструменти, але їх також можна використовувати для розвідки та здійснення атаки. Найвідоміші з таких програмних засобів: SATAN, SystemScanner, Xspider, nessus;
- **злам паролів**. Для цього використовують програмні засоби, що підбирають паролі користувачів. Залежно від надійності системи зберігання паролів, застосовують методи зламу або підбору пароля за словником. Приклади програмних засобів: LOphtCrack для Windows і Crack для UNIX;
- **пасивне прослуховування мережі**. Пасивна атака спрямована на розкриття конфіденційних даних, зокрема ідентифікаторів і паролів доступу. Приклади засобів: tcpdump, Microsoft Network Monitor, NetXRay, LanExplorer.

Методика STRIDE розроблена, обґрунтована та активно пропагується фахівцями з корпорації Майкрософт. Фактично, це ще один варіант класифікації загроз за їх наслідками. Методику використовують для побудови моделі загроз під час розроблення програмного забезпечення. Назву методики утворено з перших літер назв категорій загроз. До методики загроз відносяться:

- **підміна об'єктів**. Крім згаданих загроз, які виникають через недоліки мережних протоколів, до цього класу на-

лежить також загроза, викликана підміною особи користувача, її здійснюють, скориставшись слабкістю системи автентифікації або здобувши автентифікаційні дані шляхом крадіжки чи шахрайства (так звана соціальна інженерія);

- **модифікація даних**. До цього класу належать загрози впливів (атак), мета яких — навмисне псування даних. Атаки можуть бути спрямовані на інформаційні об'єкти, що перебувають у стані зберігання (файли, бази даних), і такі, що передаються мережею;
- **відмова від авторства**. Загрози цього класу дають змогу порушнику відмовитися від здійснених ним дій (або бездіяльності). Причиною існування такої загрози є відсутність або слабкість механізмів реєстрації подій і слабкі механізми автентифікації;
- **розголошення інформації**. Загрози цього класу не потребують коментарів;
- **відмова в обслуговуванні**. Ми вже обговорювали загрози цього класу. Атаки, що спричиняють відмову в обслуговуванні, порівняно легко здійснити у розподілених системах і дуже важко їм протидіяти. Особливо небезпечними є атаки розподіленої відмови в обслуговуванні (distributed deniai of service), які здійснюють на один об'єкт одразу з кількох вузлів мережі;
- **підвищення привілеїв**. До цього класу належать загрози, які дають можливість порушнику підвищити свої привілеї у системі. Наприклад, звичайний користувач отримує повноваження адміністратора, або порушник, що підключився без автентифікації до будь-якого мережного сервісу, виконує дії як авторизований користувач.

Проаналізувавши наявні загрози, можна створити **модель загроз** та їх абстрактний структурований опис. У Додатку до НД ТЗІ 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі" рекомендовано таку структуру опису загрози.

Властивості інформації або автоматизованих систем (АС), на порушення яких спрямована загроза:

- конфіденційність;
- цілісність;
- доступність інформації;
- спостережність та керованість АС.

Джерела виникнення загрози захисту інформації:

- суб'єкти АС;
- суб'єкти, зовнішні відносно АС (див. далі модель порушника).

Способи реалізації інформаційної загрози:

- технічними каналами, до яких належать канали побічного електромагнітного випромінювання і наведень, а також акустичні, оптичні, радіотехнічні, хімічні та ін.;
- каналами спеціального впливу шляхом формування полів і сигналів із метою руйнування системи захисту або порушення цілісності інформації;
- шляхом несанкціонованого доступу через підключення до засобів та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування програмно-апаратних закладок і впровадження комп'ютерних вірусів.

Загрози, реалізовані першими двома способами, це загрози фізичного рівня, а останнім — логічного.

Щоб розібратися з усіма можливими класифікаціями загроз захисту інформації, спочатку потрібно зрозуміти, про які саме об'єкти йдеться. Адже до **переліку об'єктів**, що охороняються можуть відноситися матеріальні, всілякі абстрактні ресурси:

- різні документи та інші інформаційні носії;
- обладнання, системи;
- приміщення;
- співробітники, партнери.

Класифікувати всі можливі загрози можна одразу за кількома категоріями. Наприклад, **класифікація** загроз захисту

інформації **за видом порушуваних властивостей інформації** представлена у такому вигляді:

Класифікація	Характеристика
Порушення конфіденційності збереженої інформації	Якщо така загроза дійсно виникає, тоді з'являється ризик витоку інформації, яка може стати доступною широкому колу користувачів, яким не обов'язково нею володіти
Порушення доступності інформаційних даних	Це стосується випадкового/навмисного блокування важливої інформації, поломки системи, де міститься вся інформація
Порушення цілісності інформаційних даних	Таким чином, відбувається втрата важливої частини даних, спотворення інформації, модифікація

У результаті ця класифікація безпосередньо пов'язана з основними складовими захисту інформації.

Але якщо узагальнити **всі можливі класифікації загроз** захисту інформації, потрібно виділити декілька найбільш важливих, головних і поширених **видів загроз**:

- розкрадання або копіювання інформаційних даних на всілякі носії;
- спеціальне нав'язування неправдивої інформації співробітникам, які мають відповідні повноваження;
- знищення інформації;
- заперечення автентичності конкретної інформації;
- зміна (модифікація) інформації;
- блокування інформації (проблеми з доступом).

Найчастіше зловмисники та шахраї **зламують акаунти** користувачів через такі причини:

- слабкий пароль, який складається із анкетних даних власника (прізвище, ім'я, по батькові, дата народження та набір знаків підряд на клавіатурі);
- один пароль на всі поштові адреси та сторінки у соціальних мережах, що використовуються;
- скидання пароля власником за вимогою зловмисників під приводом входу або реєстрації;

- фішинг — вид шахрайства, мета якого — виманювання у довірливих або неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів із переказу або обміну валюти, інтернет-магазинів. Шахраї намагаються змусити користувачів самостійно розкрити конфіденційні дані, наприклад, надсилаючи електронні листи з пропозиціями підтвердити реєстрацію облікового запису, що містять посилання на сайт, зовнішній вигляд якого повністю копіює дизайн відомих ресурсів.

Фішинг — один з різновидів соціальної інженерії, заснований на незнанні користувачами основ мережевої безпеки. Зокрема, багато хто не знає простого факту: сервіси не розсилають листів з проханнями повідомити свої облікові дані, пароль та ін.

Для захисту від фішингу виробники основних інтернет-браузерів домовилися про застосування однакових способів інформування користувачів про те, що вони відкрили підозрілий сайт, який може належати шахраям. Нові версії браузерів вже володіють такою можливістю, яка відповідно має назву "антифішинг".

За даними компанії PhishMe, станом на березень 2016 р. 93 % усіх фішингових листів намагались заразити комп'ютер жертви шкідливими програмами криптографічного здирництва — вони шифрують дані на жорсткому диску та вимагають гроші від жертви за їх розшифрування. Також серед стійких тенденцій до підвищення ефективності фішингових атак було названо випадки підлаштування вмісту листів під певну категорію жертв (за їхнім фахом) та із включенням певних елементів особистої інформації (зокрема звернення до жертви за іменем).

Фішинговий сайт — це шахрайський вебресурс, який виманює реквізити платіжних карток під виглядом надання послуг, що не існують (наприклад, поповнення мобільного рахунку, переказів з картки на картку), або вебресурс організації, якій користувач довіряє (наприклад, клон інтернет-банку), що має на меті збір реквізитів платіжних карток для подальшої крадіжки грошових коштів з рахунків власників платіжних кар-

ток. Більше ніж 90 % фішингових сайтів надають відсутні послуги з поповнення мобільного рахунку та переказу коштів з картки на картку.

Розкручуючи свій злочинний сайт, шахраї експлуатують людські мотиви: допитливість, бажання отримати вигоду, заробити тощо. Найпоширеніші повідомлення фішерів: "Дізнайтеся, чи є ваша картка в базі даних хакерів! Введіть дані, щоб перевірити", "При поповненні рахунку від 20 грн Ви гарантовано отримуєте 10 % від суми поповнення", "Акція! Поповнення рахунку, а також перекази з картки на картку будь-якого банку України без комісії" і т. ін. Крім того, власники шахрайських сайтів просувають їх, використовуючи інструменти вебмаркетингу: SEO-оптимізацію, контекстну й банерну рекламу, рекламу в соцмережах. І ці зусилля, на жаль, дають результат: відвідуваність фішингових сайтів доволі висока. За даними вебаналітиків, у середньому протягом місяця на шахрайський сайт заходить 15–30 тис. відвідувачів.

За даними компанії Phishlabs дедалі більше фішингових сайтів налаштовані на використання протоколу захищеної передачі даних HTTPS: у 3 кварталі 2017 р. таких було близько 25 %, майже удвічі більше, ніж за попередній квартал. Використання сайтом HTTPS створює у жертви хибне відчуття безпеки, адже багато хто вважає, що звичайна для сучасних веббраузерів "зелена позначка" поряд з адресою сайту свідчить про його надійність.

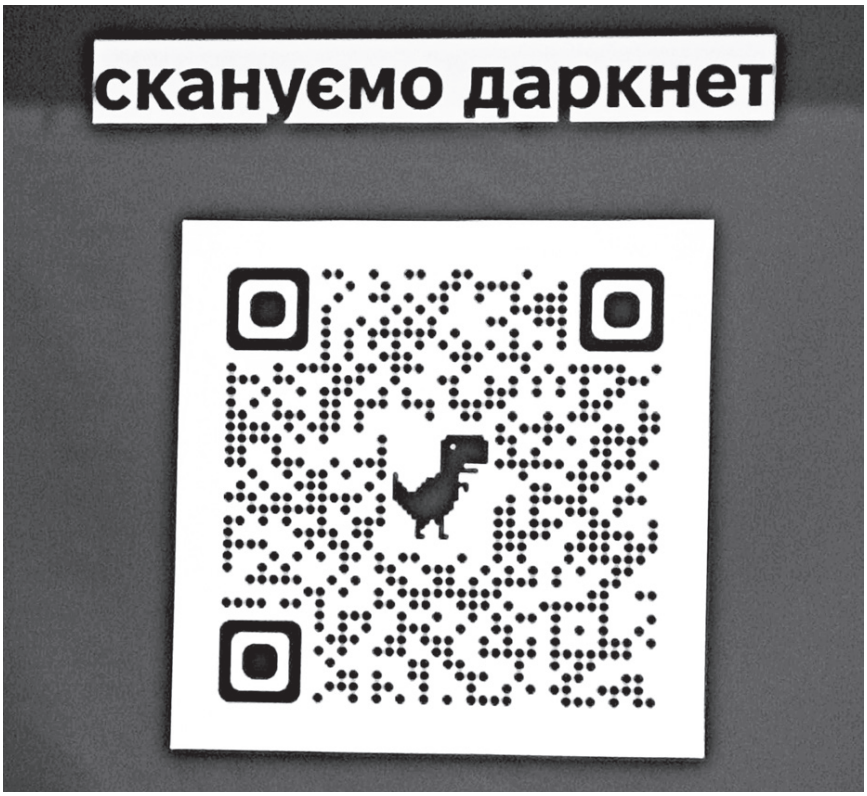
Вид атак, коли у людини намагаються викрасти деякі дані (реквізити банківської карти, реквізити для авторизації на сайті, ...) шляхом видавання себе за іншу людину. Наприклад злодій дзвонить на телефон жертви, представляючись працівником банку, і каже, що треба щось перевірити, або що його карта заблокована, і просить, наприклад, пройти авторизацію чи назвати дані карти, які розголошувати не можна.

Проведення **фішингової атаки** за допомогою СМС. Зловмисник надсилає СМС від імені якоїсь компанії або банку, де просить перейти на фішинговий сайт або надати якісь дані.

Діпфейк фішинг — це новий вид фішингових атак через засоби відео та аудіокомунікацій. Цей вид атак набув популярності під час коронавірусного локдауну.

Водночас основними носіями загроз захисту інформації є потенційні джерела таких загроз. Зазвичай запуск цих джерел здійснюється з однією метою: отримати вигоду при незаконному знищенні інформаційних ресурсів або при завданні істотної шкоди інформаційним даним. Але водночас трапляються ситуації, коли відзначають і випадковий вплив загроз, що відбувається з причини недостатньо високого ступеня безпеки інформації.

Як практичну пораду для виявлення інформаційних загроз та витоку персональної інформації власника онлайн акаунтів або месенджерів можна сканувати Даркнет за цим:



Контрольні питання

1. Як класифікують загрози інформації за джерелами походження?
2. Чим внутрішні загрози відрізняються від зовнішніх?

3. Які технічні загрози є найбільш поширеними?
4. Які організаційні загрози можуть виникнути у державних установах?
5. Як цифровізація впливає на виникнення нових загроз?
6. Що таке комбіновані загрози?

Практичне питання
Мета
Сформувати розуміння видів і джерел загроз.

Практичні завдання
1. Скласти класифікацію загроз (внутрішні, зовнішні, природні, техногенні, організаційні, людські).
2. Проаналізувати реальний інцидент (DDoS-атака, фішинг, саботаж, помилка користувача) й визначити тип загрози.
3. Побудувати "дерево причин" загрози (вибрати одну).
4. Оцінити вплив цифровізації на появу нових загроз.

Питання для обговорення
Чи можна уникнути всіх загроз при високому рівні кіберзахисту?

Тема 21. Основані засади вразливостей захисту

Усі **вразливості** прийнято ділити на три основні класи:
- об'єктивні;
- випадкові;
- суб'єктивні.

Щоб усунути повноцінну загрозу, потрібно послабити вплив зазначених вразливостей, а тому важливо більш детально ознайомитися з кожним класом.

Представлені учасники безпосередньо пов'язані з непередбаченими обставинами. Попри те, що їх наявність і вплив складно передбачити, завжди важливо бути готовим до відповідних загроз.

Для оперативного усунення подібних неполадок рекомендується скористатися організацією інженерно-технічних процесів і нанесенням удару **загрозі захисту інформації (ЗІ)**:

- збої, відмова в роботі системи. Це стосується поломки окремих інформаційних носіїв (дискети, мікросхеми, цілих ліній), ПЗ, що підтримує важливі ланки у ланцюгу зберігання/обробки інформаційних даних, сервісні програми, встановлені антивіруси;
- чинники, які всіляко послаблюють ЗІ. Таке трапляється з причини пошкодження комунікаційних мереж, під час поломки огороджувальних конструкцій — парканів, перекриттів, корпусів обладнання, де зберігається важлива інформація.

Усі перелічені фактори вимагають негайного реагування. В іншому випадку виникають серйозні ризики пошкодження важливої інформації.

Цей вид вразливостей безпосередньо пов'язаний з технічним аспектом організації всього обладнання у конкретному суспільстві. Повністю позбавитися від подібних факторів досить складно, але для часткової компенсації можна скористатися такими перевіреними **методами**:

- застосування технічних засобів випромінювання. Це можуть бути електромагнітні методики, представлені у вигляді випромінювання і сигналів від кабельних ліній; звукові методики у вигляді вібросигналів і акустичних варіантів, а також електричні методики у вигляді моментального прослизання сигналів по електромережі;
- керуючі способи. До цього переліку включені: шкідливе ПЗ; нелегальні програми і апаратура, що впроваджується у телефонні; електричні мережі тощо;
- створені з урахуванням особливостей конкретного об'єкта, перебувають під його захистом. Це вібро, звуковідбивні елементи, радіоканали, частоти.

Усе це дає змогу забезпечити 100 % безпеку інформації, виключаючи її пошкодження або навмисне розкрадання.

Такий вид є логічним результатом неправильно організованої роботи співробітників інформаційної безпеки, компанії, які припустилися серйозних помилок під час зберігання і захисту інформаційних даних.

Тому **позбутися від подібних факторів можна** тільки із застосуванням спеціального ПЗ і сучасної апаратури:

- різні неточності, допущені грубі помилки, що стали результатом порушення інформаційної безпеки. Такі проблеми могли статися на етапі виконання завантаження важливих файлів, при використанні даного ПЗ, при розробці алгоритмів, необхідних для майбутньої діяльності компанії;
- порушене функціонування в інформаційному просторі. Це стосується зміни захисних функцій інформаційних даних, режимів зберігання, захищеності інформації, під час експлуатації технічних пристроїв або ж під час роботи з такими даними.

Припуститися серйозних помилок користувачі інформації можуть також під час управління всіма програмами, системами.

Захист інформації у мережах вкрай необхідний кожному суспільству, організації та компанії незалежно від того, у якій саме галузі працюють ці об'єкти. До **переліку телекомунікаційних мереж** прийнято відносити:

- комп'ютерні мережі — використовуються для передачі всіляких інформаційних даних;
- телефонні мережі — використовуються для передачі голосової інформації.

Зазвичай навмисні дії зловмисники скоюють виключно з конкретною метою. Часто трапляються ситуації, коли розкраданням інформації цікавляться власні співробітники, гості, партнери, а також професіонали — спеціально найняті працівники.

Причому мотиви навмисного впливу можуть бути найрізноманітнішими: починаючи з незадоволеності своїм керів-

ництвом і закінчуючи бажанням завдати матеріальної шкоди країні.

Державні інформаційні ресурси (ДІР) являють собою систематизовану інформацію, що є доступною за допомогою інформаційних процесів, що використовують засоби обчислювальної техніки та забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування. Під обробкою ДІР розумітимемо виконання однієї або кількох операцій, а саме: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація, приймання, отримання, передавання, які здійснюються у системі за допомогою технічних і програмних засобів. Від надійного виконання зазначених операцій та рівня захищеності ДІР у значній мірі залежить функціонування ІТС та ефективна робота державних установ та організацій.

Порушення рівня захищеності у сфері використання електронно-обчислювальних засобів, телекомунікаційних систем і комп'ютерних мереж розподіляються на такі **види**:

- несанкціонований доступ до роботи автоматизованих систем, комп'ютерних мереж, баз даних;
- створення з метою використання, поширення або збуту шкідливих програмних продуктів або технічних засобів, а також їх розповсюдження або збут;
- несанкціонований збут або поширення інформації з обмеженим доступом, яка зберігається в автоматизованих системах, комп'ютерних мережах або на носіях такої інформації;
- злочини, що здійснені шляхом використання комп'ютерної системи як засобу досягнення злочинної мети тощо.

Атаки реалізуються зловмисниками для порушення конфіденційності, цілісності або доступності ДІР, що зберігається, обробляється та циркулює в ІТС. З цією метою зазвичай використовують вразливості ІТС, тобто нездатність системи протистояти реалізації певної загрози або сукупності загроз.

Проведемо аналіз таких характеристик безпеки ДІР, як: загрози на ДІР, аналіз можливих вразливостей ДІР та атак на ДІР. Також розглянемо сучасні бази даних, які містять детальний опис вразливстей атак та загроз, які взаємодіють між собою на рівнях моделі OSI.

У межах моделі OSI, **взаємодія** між системами відбувається фактично у вигляді **двох моделей — горизонтальної та вертикальної (ієрархічної та розподільної)**:

- у межах горизонтальної (розподільчої) моделі розглядається пряма взаємодія (обмін даними) однакових рівнів у двох кінцевих точках (хостах); для організації такої взаємодії у кожній з кінцевих точок повинні підтримуватися однакові протоколи для даного рівня;
- у вертикальній (ієрархічній) моделі розглядається обмін інформацією (взаємодія) між сусідніми рівнями однієї системи з використанням інтерфейсів; у цій моделі кожен рівень може надавати свої послуги вищому рівню і користуватися послугами нижчого рівня (крайні рівні моделі у цьому сенсі є винятком – прикладний рівень надає свої послуги користувачу, а фізичний рівень не користується сервісом інших рівнів).

Перші інциденти порушення захисту інформації, офіційно зареєстровані в базах даних вразливостей, з'явилися у 1988 р. З тих пір ведеться постійний пошук вразливостей та їх реєстрація як у межах різних відкритих проєктів, так і комерційними компаніями, дослідницькими інститутами та дослідниками. Серед лідерів детектування вразливостей можливо зазначити таких **розробників відповідних баз даних вразливостей**:

- компанія MITRE та її база вразливосей Common Vulnerabilities and Exposures (CVE);
- National Institute of Standardsand Technology та база National Vulnerabilities Database (NVD);
- United State Computer Emergency Readiness Team та база Vulnerability Notes Database (VND), компанія IBM та база вразливостей X-Force та ін.

Розглянемо більш детально деякі із зазначених **баз вразливостей**:

1. **CVE – довідково-пошукова система посилань та позначень вразливостей.** Важливою складовою системи є CVE-ідентифікатори — унікальні ідентифікатори, що надаються кожній відомій вразливості у сфері інформаційної безпеки. Система містить більше 98 тис. записів про окремі вразливості. Основна відмінність полягає у тому, що вона є найбільш повною та систематизованою, тому її використовують як основу для визначення відповідності записів вразливостей в інших базах. До основних елементів структури записів вразливостей відносяться:

- статус — у цьому полі може міститися або значення Entry (перевірений запис), або значення Candidate (ще не перевірена вразливість);
- фаза — у цьому полі міститься значення етапу розвитку вразливості, а також дата присвоєння зазначеного етапу. Можуть бути такі значення: Proposed — фаза пропозиції вразливості; Interim — проміжна фаза вразливості; Modified — фаза модифікації вразливості; Assigned — фаза встановлення вразливості;
- опис — поле містить опис вразливості;
- посилання — у даному полі містяться посилання на інші джерела із зазначенням конкретної адреси інтернет-ресурсу опису вразливості й ідентифікатора джерела;
- голоси — поле містить імена членів голосування, які прийняли рішення про занесення вразливості у базу;
- коментарі — вноситься ім'я автора коментаря та його текстовий зміст.

Також в елементах записів вразливостей міститься тип вразливості, ім'я та ідентифікатор. Ім'я вразливості має формат "CVE-YYYYNNNN", де YYYY — це рік виявлення вразливості, а NNNN — її порядковий номер.

Процес додавання вразливості у базу містить три етапи:

- обробку — аналіз, дослідження і процес приведення вразливості до формату CVE;

- присвоєння — призначення конкретному запису вразливості ідентифікатора CVE;
- публікацію — створення нового запису і публікація його на інтернет-ресурсі CVE, як тільки ідентифікатор CVE офіційно присвоєно.

До недоліків бази CVE слід віднести відсутність механізму опису належності вразливостей до конкретних продуктів, а також присвоєння вразливостям метрик і розрахунку ступеня небезпеки.

2. **Національна база даних вразливостей США (NVD)** — сховище даних вразливостей, засноване на стандартах протоколу автоматизації змісту безпеки. База NVD об'єднала в собі опис вразливостей, назви програмного забезпечення з цими вразливостями і оцінки небезпеки вразливостей. На 2017 р. база даних вразливостей NVD мала близько 70 тис. записів вразливостей.

Структура запису вразливості у базі NVD є розширеною формою подання запису в базі CVE за рахунок наявності таких полів: конфігурація вразливих продуктів з урахуванням залежностей; список вразливих продуктів; показники, що характеризують вразливість у форматі "Загальної системи оцінки вразливостей"; тип доступу для реалізації вразливості.

Встановлено, що 82,77 % вразливостей належать додаткам, 12,28 % — операційним системам і 3,59 % — апаратному забезпеченню.

Відмінною особливістю бази NVD є використання Common Platform Enumeration, що є одним із кращих словників продуктів серед відомих аналогів за рахунок великої кількості записів і уніфікованого формату імен програмно-апаратного забезпечення.

Однак у цього формату представлення записів продуктів є недоліки, а саме:

- неоднозначність значень різних полів формату;
- недостатнє використання записів даного словника базою NVD.

3. **База вразливостей OSVDB створена для спільноти фахівців у сфері безпеки.** Мета проєкту полягає в тому, щоб забезпечити точну, деталізовану, актуальну інформацію про вразливість для систем забезпечення безпеки. Ця база містить понад 110 тис. вразливостей.

Структура цієї бази не суттєво відрізняється від раніше розглянутої бази NVD, однак варто відзначити наявність основних полів, таких як:

- "Ідентифікатор OSVDB";
- "Дата виявлення";
- "Ім'я виробника";
- "Ім'я продукту";
- "Версія продукту";
- "Посилання";
- "Рішення";
- "Метрики вразливості".

4. **База вразливостей X-Force** є проєктом компанії IBM, що знаходиться у відкритому доступі у мережі Інтернет. Поля даних, що описують записи вразливостей цієї бази, не суттєво відрізняються від полів баз вразливостей, описаних раніше. Однак в їх склад входять елементи, що вказують на перевагу бази X-Force — це:

- поле "Наслідки", які представляють у формалізованому вигляді можливий результат експлуатації вразливості;
- поле TemporalScore, що є елементом системи метрик CVSS, використовуваної для оцінювання тимчасових характеристик вразливості.

Також слід відзначити наявність у даній базі описів і висновків про можливі вразливості.

Зазначена база містить більше 70 тис. записів вразливостей, які поділяються на вразливості вищого, середнього та низького рівнів. Вразливості низького рівня небезпеки становлять всього 12 %, середнього і високого — 62 та 26 % відповідно.

Зазначені вразливості можуть бути використані зловмисником для здійснення вторгнень у ІТС з метою порушення ці-

лісності, доступності та конфіденційності інформації, яка передається в ІТС, або для деструктивного впливу на сам процес функціонування ІТС.

Таким чином, у ІТС має бути передбачена можливість щодо виявлення та запобігання вторгнень, які реалізуються множиною різнонаправлених за своїм фізичним змістом атак. Для забезпечення такої можливості система управління містить у своєму складі підсистему управління безпекою, функціонування якої повинно здійснюватися на основі відповідних методів виявлення атак або вторгнень (МВА).

Під **вторгненням** розуміємо несанкціонований вхід в ІТС у результаті дій, що порушують політику безпеки або обходять систему захисту. Питання захисту будь-якої ІТС від вторгнень та атак є завдання, забезпечення якого покладається на МВА. Внаслідок цього при побудові МВА необхідно враховувати широкий спектр атак, які здатні впливати на ІТС практично на всіх рівнях мережевої моделі OSI.

Під атакою розуміємо спробу реалізації загрози. У свою чергу загроза є будь-якою обставиною або подією, що може бути причиною порушення функціонування інформаційним, програмним та апаратним складовим інформаційної системи, політиці безпеки, нанесення збитків тощо.

Розглянемо **типи атак на ІТС обробки ДІР та їх параметри**, що використовуються.

1. **Пасивні**. Атаки, що не мають безпосереднього впливу на роботу системи, але можуть порушувати її політику безпеки. Атаку практично неможливо виявити. Після атаки не залишається ніяких слідів. Приклад: прослуховування каналу зв'язку в мережі.

2. **Активні**. Атаки, що безпосередньо впливають на роботу системи (зміна конфігурації ІТС, порушення працездатності тощо) і порушують прийняту в ній політику безпеки. Практично всі типи віддалених атак є активними. Існує можливість виявлення, оскільки у результаті здійснення атаки в системі відбуваються певні зміни.

3. **Порушення конфіденційності**. Перехоплення інформації. Приклад: прослуховування каналу в мережі.

4. **Порушення цілісності**. Спотворення інформації. Приклад: впровадження помилкового об'єкта в ІТС.

5. **Порушення доступності**. Не відбувається несанкціонованого доступу (зберігається цілісність і конфіденційність), проте доступ до інформації легальних користувачів неможливий. Приклад: відмова в обслуговуванні (DoS).

6. **Атака на запит від об'єкта, що атакується**. У разі запиту атакуючий очікує передачі від потенційної мети атаки запиту певного типу, який і буде умовою початку здійснення впливу. Ініціатором здійснення початку атаки є об'єкт, що атакується. Приклад: DNS- і ARP-запити у стеці TCP / IP.

7. **Атака з настанням події, що очікується на об'єкті**. У разі настання події, атакуючий здійснює постійне спостереження за станом операційної системи віддаленої цілі атаки і при виникненні певної події у цій системі починається вплив. Ініціатором здійснення початку атаки є об'єкт, що атакується. Приклад: переривання сеансу роботи користувача з сервером у мережевих операційних системах без видачі команди LOGOUT.

8. **Безумовна атака**. У разі безумовної атаки її початок по відношенню до мети атаки і до стану системи здійснюється негайно. Ініціатором здійснення початку атаки є атакуючий.

9. **Атака зі зворотним зв'язком**. Це атака, під час якої атакуючий отримує відповідь від об'єкта на частину своїх дій. Такі відповіді потрібні, щоб мати можливість продовжити атаку і/або здійснювати її більш ефективно, реагуючи на зміни, що відбуваються у системі.

10. **Без зворотного зв'язку (односпрямована атака)**. Атака без зворотного зв'язку – атака, яка відбувається без реакції на поведінку системи, що атакується. Приклад: відмова в обслуговуванні (DoS).

11. **Внутрісегментна**. Атака, при якій суб'єкт і об'єкт атаки знаходяться всередині одного сегменту мережі (сегмент — фі-

зичне об'єднання станцій за допомогою комунікаційних пристроїв не вище канального рівня).

12. **Міжсегментна**. Міжсегментна атака — атака, при якій суб'єкт і об'єкт атаки знаходяться у різних сегментах мережі.

13. **Розподілена**. Атака, вироблена двома або більше атакуючими на одну і ту саму обчислювальну систему, об'єднаними єдиним задумом і в часі.

14. **Нерозподілена**. Нерозподілена атака проводиться одним атакуючим.

У свою чергу база даних про атаки та модель для оцінки поведінки зловмисників при здійсненні вторгнень є матрицею ATT@CK, яка описує **найбільш небезпечні фази атаки на ІТС**, а саме:

- отримання початкового доступу (Initial Access) — являє собою вектори, які використовують зловмисники для отримання доступу до мережі;
- виконання (Execution) – застосування методів, що призводять до виконання коду зловмисника в локальній або віддаленій системі;
- закріплення в атакуємій системі (Persistence) — будь-які зміни доступу або конфігурації системи, що забезпечують постійну присутність зловмисника у цій системі;
- підвищення привілеїв (Privilege Escalation) — зловмисник має скористатись слабкими місцями системи для отримання прав локального адміністратора або рівня system/root;
- обхід захисту (Defense Evasion) — набір атрибутів, які застосовує зловмисник для ухилення від виявлення;
- отримання облікових даних (Credential Access) — методи отримання доступу або контролю обліковими даними системи, домена або служби, що використовуються у системі;
- огляд (Discovery) — методи отримання зловмисником відомостей про систему і внутрішню мережу;

- горизонтальне просування (Lateral Movement) — методи збору інформації із системи без використання додаткових інструментів;
- збір даних (Collection) — методи збору інформації;
- витік (Exfiltration) — методи та атрибути видалення файлів та інформації з цільової системи;
- управління і контроль (Command and Control) — взаємодія зловмисника з підконтрольними системами.

Аналіз останніх публікацій свідчить про те, що **існуючі атаки**, які застосовуються **для проведення вторгнень в ІТС, поділяються на 5 категорій**. Кожна з категорій містить множину типів атак, які використовуються для реалізації мети вторгнення. У свою чергу кожен тип атаки несе загрозу мережі на відповідних рівнях мережевої моделі OSI та виконує свою функцію щодо здійснення деструктивного впливу на мережу.

До **вказаних категорій атак** відносять:

1. **Side-channel атаки** (атаки сторонніми каналами) — атаки, спрямовані на вразливості у практичній реалізації криптосистеми. На відміну від теоретичного криптоаналізу, атаки по сторонніх каналах використовують інформацію про фізичні процеси в пристрої, які не розглядаються у теоретичному описі криптографічного алгоритму. До найчастіше застосованих Side-channel атак належать: probing attack, timing attack, fault-induction attack, power analysis attack, electromagnetic analysis attacks та ін.

2. **DoS-атаки** — це мережеві атаки, спрямовані на створення ситуацій, коли у системі, що піддається вторгненню, відбувається відмова в обслуговуванні.

Вказані атаки характеризуються генерацією великого обсягу трафіка, що призводить до перенавантаження та блокування сервера. До найчастіше застосованих DoS-атак належать: back, land, neptune, pod, smurf, teardrop attacks та ін.

3. **U2R-атаки** — пропонують отримання зареєстрованим користувачам привілеїв адміністратора. До U2R-атак відносять такі типи: buffer_overflow, loadmodule, perl, rootkit.

4. **R2L-атаки** — характеризуються отриманням доступу незареєстрованого користувача до мережі з боку віддаленої станції. Поділяють R2L-атаки на: ftp_write, guess_passwd, imap, multihop, phf, spy, warezclient, warezmaster та ін.

5. **Probe-атаки** — сканування мережевих портів з метою отримання конфіденційної інформації. Probe-атаки поділяються на такі типи: ipsweep, nmap, portsweep, satan та ін.

Кожна атака характеризується наявністю множини параметрів, при ідентифікації яких можливо співвіднести до окремого типу атак.

Атаки — це послідовність параметрів з'єднання, таких як: тривалість з'єднання, тип протоколу, послуга мережі, кількість байтів у повідомленні, стан з'єднання, кількість термінових пакетів, кількість невдалих спроб встановлення з'єднання тощо.

Зазвичай атака поступає на інформаційно-телекомунікаційний ресурс у вигляді повідомлення з мовою, відео-, аудіоінформацією або даними. Дане повідомлення складається з таких елементів: передзаголовок, заголовок, контрольна сума, текст повідомлення, завершення повідомлення, що ідентифікується системою виявлення атак на предмет встановлення атаки.

Вказані типи атак за своєю функцією можуть впливати на: управління ІТС, розмежування доступу, обмін пакетами, енергетичні характеристики, доступ до кодування, управління інформацією та ін.

З урахуванням особливостей функціонування ІТС, які обробляють ДІР, доцільно висунути **перелік вимог до МВА з метою їх застосування у ІТС**:

- інтелектуалізація процесу встановлення вразливостей та виявлення атак;
- висока точність виявлення атак;
- висока швидкість виявлення атак;
- можливість виявлення нових атак;
- робота в умовах непередбачуваності;
- можливість самонавчання та ін.

Системи виявлення атак (СВА) служать механізмами моніторингу та спостереження підозрілої активності. Вони можуть виявити атакуючих, які змогли обійти Firewall, і видати звіт про це адміністратору, який у свою чергу зробить подальші кроки щодо запобігання атаки.

Проведений аналіз вразливостей та атак на ДІР, що обробляються засобами ІТС, показав різноманіття підходів до побудови баз вразливостей, кожен має свої переваги та недоліки, але найбільш вагомим є орієнтованість сучасних баз вразливистей для використання в експертних системах. Сучасні ІТС обробки ДІР мають велику кількість зовнішніх і внутрішніх вразливостей, а реалізація їх відбувається за допомогою множини різнонаправлених атак. Поширення вразливостей окремого вузла ІТС може викликати появу додаткових загроз безпеці ДІР, що в ній оброблюються. Тому для визначення множини параметрів при оцінюванні захищеності ДІР загалом та виявлення нових вразливостей доцільно забезпечити функціонування СВА з урахуванням зазначених вимог, параметрів даних та характеристичних особливостей сучасних СВА.

Контрольні питання

1. Що таке вразливість в інформаційній системі?
2. Які типи вразливостей існують (програмні, апаратні, організаційні)?
3. Як людський фактор формує вразливості?
4. Які методи виявлення вразливостей використовують сучасні служби безпеки?
5. Чим відрізняється zero-day вразливість від відомої вразливості?
6. Чому регулярне оновлення систем знижує ризик експлуатації вразливостей?

Практичне питання

Мета

Розуміти сутність вразливостей та способи їх усунення.

Практичні завдання

1. Скласти класифікацію вразливостей (технічні, програмні, організаційні, людські).
2. Проаналізувати приклад zero-day вразливості та її наслідки.
3. Створити таблицю “Вразливість – загроза – наслідки – контрзахід”.
4. Розробити заходи щодо усунення 5 поширених вразливостей в установі.

Питання для обговорення

Чому людський фактор залишається головною вразливістю?

Тема 22. Загальні принципи захисту інформації у мережах

Розвиток нових інформаційних технологій, загальна комп’ютеризація та різке збільшення кількості інформаційно-комунікаційних систем і мереж (ІКСМ) призвели до того, що захист інформації стає обов’язковим, він також є однією з характеристик інформаційних систем. Фактор безпеки інформаційних ресурсів і послуг при розробці та експлуатації сучасних ІКСМ відіграє першорядну роль. При організації систем захисту потрібно керуватися низкою принципів, які забезпечать якісний захист та протидію від існуючих загроз.

Ціль захисту інформації в ІКСМ — це процес протидії впливу на інформаційні ресурси та послуги, якщо даний вплив виконується з метою порушення конфіденційності, цілісності та доступності, а саме: знищення, крадіжка, зниження ефективності функціонування або несанкціонований доступ.

Для захисту документів, які знаходяться на паперових носіях, а також інформації в електронному вигляді, потрібно ознайомитися з основними принципами захисту інформації (ЗІ).

У результаті повноцінна **система захисту інформації** передбачає виконання таких **обов'язкових кроків**:

1. Поділ усіх інформаційних ресурсів на дві основні категорії — конфіденційна і неконфіденційна інформація. Таким чином, можна точно зрозуміти, які саме файли і папки потрібно захищати від зловмисників.

2. Виключити вільний доступ до всієї інформації, що відноситься до категорії конфіденційної. Для захисту даних у комп'ютерній мережі команда фахівців вдається до різних сучасних методів: DLP-системи, ОС, засоби криптографічного захисту тощо.

3. Організувати ретельний контроль за переміщенням носіїв з конфіденційною інформацією. Вирішити таку проблему дає змогу спеціальний модуль DLP-системи.

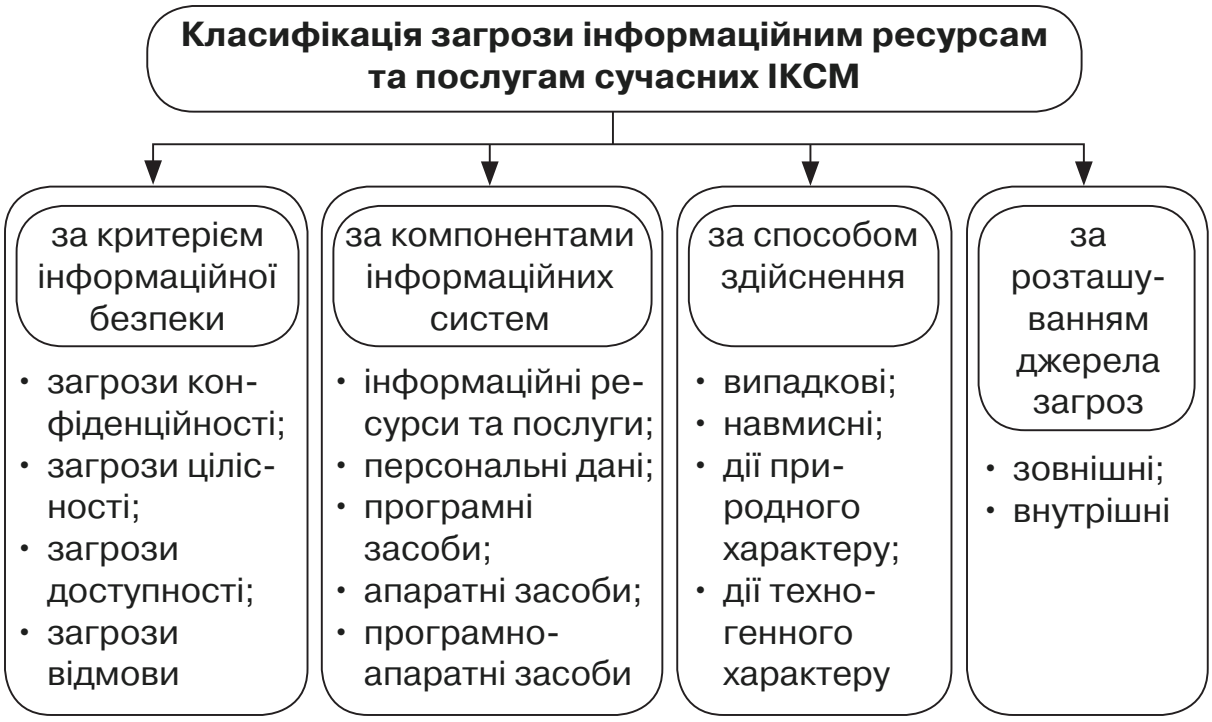
4. Крім того, потрібно обов'язково провести роз'яснювальну роботу та інструктажі з усіма користувачами, які мають вільний доступ до подібних інформаційних ресурсів.

Побудова надійного та ефективного захисту інформаційної системи неможлива без попереднього **аналізу можливих загроз** безпеки системи. Цей аналіз повинен складатися з таких **етапів**:

- виявлення характеру інформації, яка зберігається у системі;
- оцінка цінності інформації, яка зберігається у системі;
- побудова моделі зловмисника;
- визначення та класифікація загроз інформації у системі (несанкціоноване зчитування, несанкціонована модифікація та ін.);

Під **загрозою безпеки інформаційним ресурсам** розуміють дії, які можуть призвести до спотворення, несанкціонованого використання або навіть до руйнування інформаційних ресурсів керованої системи, а також програмних і апаратних засобів.

Загрози інформаційним ресурсам та послугам можна **класифікувати за такими критеріями** (див. рисунок):



Класифікація базових загроз інформаційним ресурсам та послугам у сучасних системах і мережах

- інформаційна безпека (загрози конфіденційності даних і програм; загрози цілісності даних, програм, апаратури; загрози доступності даних; загрози відмови від виконання операцій);
- за компонентами інформаційних систем, на які загрози націлені (інформаційні ресурси та послуги, персональні дані, програмні засоби, апаратні засоби, програмно-апаратні засоби);
- за способом здійснення (випадкові, навмисні, дії природного та техногенного характеру);
- за розташуванням джерела загроз (внутрішні та зовнішні).

Усі загрози безпеки, спрямовані проти програмних і технічних засобів інформаційної системи, впливають на безпеку інформаційних ресурсів і призводять до порушення основних властивостей інформації, що зберігається і обробляється в інформаційній системі. Зазвичай загрози інформаційній безпеці розрізняються за способом їх реалізації.

Дослідження й аналіз численних випадків впливів на інформацію і несанкціонованого доступу до неї показують, що їх можна розділити на випадкові та навмисні.

Якщо розглядати класичну систему організації впливу на ІКСМ, то всі загрози поділяються на випадкові, ненавмисні та навмисні.

Джерелом ненавмисних загроз інформаційних систем можуть бути: вихід з ладу апаратних чи програмних засобів, неправильні дії працівників або її користувачів, ненавмисні помилки в програмному та програмно-апаратному забезпеченні тощо. Такі загрози можуть нанести значний збиток. Однак більш значними, з точки зору ефективності функціонування ІКСМ, є навмисні загрози, які на відміну від випадкових, мають на меті завдання збитків інформаційній системі або користувачам.

Навмисні загрози реалізуються шляхом довготривалої масованої атаки несанкціонованими запитами або вірусами тощо. Наслідками можуть бути: руйнування (втрата) інформації, модифікація (зміна інформації на помилкову, яка коректна за формою і змістом, але має інший сенс) і ознайомлення з нею сторонніх осіб. Ціна вказаних подій може бути досить високою.

Для вирішення поставленої задачі й створення ефективної системи захисту інформації, розроблення та вдосконалення існуючих методів захисту доцільно навести найбільш повну класифікацію загроз і шляхів їх реалізації в ІКСМ.

Можна виокремити **актуальні загрози безпеці**, які спрямовані проти інформаційних ресурсів у сучасних інформаційно-комунікаційних системах та мережах:

- протиправне збирання і використання інформації;
- порушення технології обробки інформації;
- впровадження в апаратні та програмні вироби компонентів, що реалізують функції, не передбачені документацією на ці вироби;
- розробка і поширення програм, що порушують нормальне функціонування інформаційних та інформаційно-те-

лекомунікаційних систем, у тому числі систем захисту інформації;
- радіоелектронний вплив з метою виведення з ладу, пошкодження чи руйнування засобів і систем обробки інформації, телекомунікації зв'язку;
- вплив на парольно-ключові системи захисту автоматизованих систем обробки і передачі інформації;
- витік інформації технічними каналами;
- впровадження електронних пристроїв для перехоплення інформації у технічні засоби обробки, зберігання і передачі інформації з каналів зв'язку, а також у службові приміщення органів державної влади, підприємств, установ та організацій усіх форм власності;
- знищення, пошкодження, руйнування чи розкрадання машинних та інших носіїв інформації;
- перехоплення інформації у мережах передачі даних та лініях зв'язку, дешифрування цієї інформації і нав'язування хибної інформації;
- використання несертифікованих вітчизняних і закордонних інформаційних технологій, засобів захисту інформації, засобів інформатизації, телекомунікації зв'язку при створенні та розвитку інформаційної інфраструктури України;
- несанкціонований доступ до інформації, що знаходиться у банках і базах даних;
- порушення законних обмежень на поширення інформації.

Основні принципи організації захисту інформаційних систем

При організації ефективного та надійного захисту потрібно керуватися системою принципів. Під **принципами захисту інформації** розуміються основні ідеї і найважливіші рекомендації з питань організації та здійснення робіт для ефективного захисту інформаційних ресурсів ІКСМ. Використання даних

принципів дає змогу ефективно організувати роботу із захисту інформації.

Принципи захисту інформації можна умовно розділити на дві основні групи:

- правові принципи;
- організаційні принципи.

Правові принципи захисту інформації. Правове регулювання захисту інформації спирається на принципи інформаційного права. Дані принципи, що базуються на положеннях основних конституційних норм, закріплюють інформаційні права і свободи, а також гарантують їх здійснення. Крім того, основні правові засади захисту інформації ґрунтуються на особливостях і юридичних властивостях інформації як повноцінного об'єкта правовідносин.

Загалом до правових принципів захисту інформації відносяться:

- легітимність (законність);
- пріоритет міжнародного права над внутрішньодержавним;
- економічна доцільність.

Організаційні принципи захисту даних. Роль організаційного захисту інформації у системі заходів безпеки визначається своєчасністю та правильністю прийнятих управлінських рішень, способів і методів захисту інформації на основі діючих нормативно-методичних документів.

Організаційні методи захисту передбачають проведення організаційно-технічних та організаційно-правових заходів, а також включають такі принципи захисту інформації:

- науковий підхід до організації захисту інформації;
- планування захисту;
- керування системою захисту;
- безперервність процесу захисту інформації;
- мінімальна достатність організації захисту;
- системний підхід до організації та проєктування систем та методів захисту інформації;

- комплексний підхід до організації захисту інформації;
- відповідність рівня захисту цінності інформації;
- гнучкість захисту;
- багатозональність захисту, що передбачає розміщення джерел інформації в зонах з контрольованим рівнем її безпеки;
- багаторубіжність захисту інформації;
- обмеження числа осіб, які допускаються до захищеної інформації;
- особиста відповідальність персоналу за збереження довіреної інформації.

Відкриті системи володіють властивостями самоорганізації та інтелекту (розуму). Під інтелектом (у даному випадку) розуміється здатність мислення, раціонального пізнання, яке реалізується в процесі взаємодії у трійці: суб'єкт – управляюча дія – об'єкт, або (у загальному випадку) в послідовності суб'єкт – управляюча дія – суб'єкт – управляюча дія ... – об'єкт. Назвемо таку взаємодію суб'єктно-об'єктною взаємодією. Інтелектуальна система "інженерно" виникає лише тоді, коли в процесі пізнання суб'єкт і об'єкт періодично міняються місцями: суб'єкт переходить у стан об'єкта, а об'єкт стає відповідаючим джерелом активності — суб'єктом. Безперервно необхідне підтвердження — суб'єкт повинен ставати об'єктом для сприйняття правильності контекстного розуміння його повідомлення. Для планування наступної команди необхідно, як мінімум, бути впевненим у правильному контекстному розумінні попередньої. Інтелектуальна система подібна генератору, який виробляє управляючу інформацію.

Поняття відкритої системи відрізняється від класичного визначення системи тим, що воно враховує важливу роль в існуванні відкритої системи взаємодії з оточуючим середовищем. Відкрита система безперервно взаємодіє зі своїм оточенням. Взаємодія забезпечується як у силовій формі, так і у "несиловій" інформаційній формі. Крім того, відкрита система існує як безперервний процес взаємодії. Сприйняття відкритої системи

можливе на основі технологічних правил цього процесу. Це віддалено нагадує процес виконання комп'ютерної програми, який перетворює комп'ютер у функціонуючу автоматизовану систему.

Відкрита система взаємодіє із зовнішнім оточенням, обмінюючись інформацією, енергією, матеріальними об'єктами. Безпека взаємодії складається із взаємопов'язаних між собою інформаційної безпеки, енергетичної безпеки, фізичної безпеки тощо. У процесі взаємодії з інформаційних, енергетичних, матеріальних потоків мають вибиратися ті, які відповідають цільовій функціональності існування відкритої системи.

Відкриті системи мають органічно притаманні їм властивості самозбереження, самоорганізації, саморозвитку та інтелекту. Самозбереження, як буде показано далі, є однією з цілей і забезпечується самим принципом інтелектуального управління у відкритій системі. Властивість самоорганізації виявляється у процесі еволюції відкритої системи як процесу.

Еволюція системи має бути керована у "критичних точках", зокрема у початковій точці при пуску системи. Цільова неспонтанна самоорганізація є однією з обов'язкових вимог до багатьох сучасних систем. Властивість саморозвитку забезпечує системам можливість адаптуватись до змін у зовнішньому середовищі. Вважається, що цілі існування штучних відкритих систем знаходяться поза цими системами. Інколи їх не можна чітко сформулювати. Саморозвиток може стати можливим тоді, коли цілі існування формулюються ("усвідомлюються") самою відкритою системою. Дані властивості при їх розгляді під кутом зору забезпечення інформаційної безпеки відкритої системи ставлять проблеми і умови постійної керованості, спостережності, а також повсюдності цих властивостей для тотожності визначення контексту в однакових умовах.

Основу захисту інформації відкритих систем складає умова спостережності всіх систем, явищ, процесів або об'єктів. Відкриті системи описуються за допомогою контекстно-залежної мови. Тому, по-перше, відкриті системи моделювати не можна,

складні системи не можна моделювати інакше, як повторивши всю історію їх виникнення, а по-друге, необхідна якість управління системно-складними об'єктами може бути досягнута лише за рахунок використання контекстно-залежних мов їх представлення та системи управління, яка працює з такими мовами.

Управління у загальному випадку повинне починатись з попередньої оцінки об'єкта, який управляється, і вибору мови управління, яка відповідає об'єкту. Для замкнутих об'єктів ці мови мають математичну або алгоритмічну реалізацію. Для відкритих систем, при збереженні досить високого рівня своєї комунікативної функції відносно оточення, мови описання і управління стають контекстно-залежними.

Відкриту систему можна представити як сукупність кількох підсистем інформаційно зв'язаних з деякими серверами, їх базами, і які користуються їх обчислювальними потужностями. Підсистеми зв'язані між собою інформаційними потоками, які замикаються через окрему підсистему з динамічною реконфігурацією структурних зв'язків. З оточуючим середовищем взаємодія відбувається через шумові та керуючі (командні) інформаційні потоки. Точка підключення кожного користувача або окремої автоматизованої системи до інформаційного середовища оформлюється у вигляді термінала — робочого місця, яке має програмне забезпечення, що базується на нормативно-правовій та нормативно-методичній інформації та визначає права доступу до інформаційних ресурсів. Для прийняття рішень щодо управління та захисту необхідна інформація про інформацію, тобто метаінформація, або відомості, які характеризують динаміку інформаційної взаємодії. Мають бути враховані параметри, які характеризують інформаційні потоки: обсяги за одиницю часу, адресація і напрям, швидкість обробки, ідентифікація та персоніфікація джерела та обробника тощо, які характеризують конкретику ситуації.

Про підсистему треба мати всі прямі та контекстні відомості щодо поточного стану підсистеми, фактів і динаміки отриман-

ня або передачі інформації чи матеріальних об'єктів тощо. Внутрішня семантика інформації потрібна також при прийнятті рішень щодо захисту.

Для управління відкритою системою та забезпечення безпеки необхідно створити систему роботи з інформацією у вигляді структури взаємодії управляючої системи (і, зокрема, її підсистеми інформаційної безпеки) з об'єктом. Ця структура має забезпечити можливість накопичення і використання метаінформації для можливості прийняття рішень щодо управління і захисту.

Остаточно нас цікавить забезпечення захищеного обміну. Мають контролюватись процеси, які можуть привести систему до саморуйнування або до стану, близького до такого, при якому стає неможливим виконання їх функцій. Якщо попередити таке руйнування неможливо, то необхідно провести саморуйнування (реструктуризацію) у "безпечній формі". Тим самим мають забезпечуватись замикання інформаційних потоків джерел і споживачів інформації всередині об'єкта, а також у можливому ступеню потоків взаємодії із зовнішнім середовищем через деяке контрольне середовище, яке виконує функції контролю та семантичного аналізу всіх інформаційних потоків та стає єдиним дозволеним каналом для обміну інформацією і невід'ємною частиною об'єкта. Це означає, що у контрольному середовищі постійно працює програма адресного збору інформації динамічних характеристик потоків інформації і характеристик захищеності та безпеки інформації.

Кожна підсистема повністю і постійно відслідковується за цими характеристиками. Будь-яка зміна динаміки і семантики інформаційних потоків, які не передбачені технологією роботи, має генерувати сигнал для початку вироблення управляючих та захисних рішень. Саме таке повне і постійне слідкування за характеристиками усіх інформаційних потоків не реалізоване у сучасних комп'ютерних системах, які класифікуються як автоматизовані або інформаційно-телекомунікаційні системи. Це зумовлює нескінченну множину вразливостей, які продо-

вжують експлуатувати зловмисники. Витрати на додаткову обробку інформації можуть бути значними, але тільки вони дають контекстну інформацію, необхідну для досягнення безпечного інтелектуального управління.

У безпечній інтелектуальній системі управління наявна практично вся інформація, що може бути зібрана і використана при автоматичному прийнятті управлінських та захисних рішень. При цьому характеристики динаміки вже дають спостережність системи та інформаційного продукту, який вона виробляє.

Система захисту інформації вимагає визначення діапазонів свого стану стійкості, набору дозволених станів, частотних, статичних і динамічних оцінок. Повноцінний захист відкритої системи забезпечується завдяки вбудованому перехопленню й контролю всіх інформаційних потоків. Врахування динаміки інформаційних потоків необхідне за двома базовими складовими: інформації-продукту та інформації-сировини.

Інформація-продукт виробляється у підсистемі, наприклад на робочому місці оператора, і має цінність новизни.

Інформація-сировина та команди споживаються від джерел наявної інформації і служать для вироблення нової інформації.

Тут потрібна також інформація про інформацію. Крім базових інформаційних потоків необхідно виділяти інформацію, що регламентує зміст цих потоків з точки зору управління та безпеки. Для надійного захисту інформаційного середовища, яке має цінність для системи, від шумового впливу програмне забезпечення робочих місць має проводити фільтрацію потоків інформації як за внутрішньою несуперечністю, так і на узгодженість з наявною інформацією, використовуючи методи семантичного аналізу. У відкритій системі управління може бути лише інтелектуальним і здійснюватись за допомогою інтелектуальних інформаційних баз.

Управління — це посилання повідомлень, які ефективно впливають на поведінку керованої системи. **Інтелектуальна система управління** — це система управління, що заснована на виробленні, структуризації та обміні інформацією. **Інтелекту-**

альна база управління — це активна система оцінювання результатів, яка основана на двосторонній контекстуальній взаємодії. Інтелектуальна база складається з машини бази даних, машини бази знань та системи управління.

Машина баз знань — це механізм забезпечення управління для відкритих систем, орієнтований на практичну задачу сприйняття семантики інформації як управління з урахуванням всіх необхідних умов контекстного аналізу та реструктуризації зв'язків при роботі зі знаннями. У машині бази знань вхідна інформація є і управлінням, і водночас командою для організації дій з її обробки.

Система захисту інформації накладає на систему обмеження у ресурсах, виконуваних функціях. Класична система захисту інформації робить систему, що захищається, закритою, яка знижує її ефективність. Задача полягає у максимальному збереженні можливостей взаємодії з оточуючим середовищем та ефективності свого функціонування в умовах взаємодії з навколишнім оточенням, тобто побудувати систему захисту інформації на законах функціонування відкритих систем, зберігаючи і не зменшуючи ефективність функціонування, а також зберігаючи необхідну свободу взаємодії.

Захист інформації як і управління треба проводити на самому інформаційному потоці взаємодії з навколишнім оточенням. Забезпечення безпеки проводиться у процесі управління, коли в системі, що управляється, треба відчути направлений і "розумний з її точки зору" опір керованого об'єкта, треба одержати які-небудь підтвердження факту освоєння нею отриманої інформації і деякі гарантії правильності, з точки зору управителя, її засвоєння.

Для знаходження місця процесам забезпечення інформаційної безпеки в інтелектуальній системі корисно врахувати відому теорію ієрархії потреб Маслоу, відповідно до якої усі потреби інтелектуальної системи може бути подано у вигляді піраміди: фізіологічні, безпеки, причетності, визнання, самовираження. З позицій теорії відкритих систем цю піраміду по-

треб можна коментувати таким чином. Насамперед повинні забезпечуватись потреби фізіологічні: енергетичні, продовольчі тощо. Потреби другого рівня піраміди пов'язані з бажанням та прагненням суб'єктів до стабільного й безпечного стану: фізичної, енергетичної, інформаційної безпеки. Після задоволення первинних потреб першого та другого рівнів у суб'єкта виникає необхідність у задоволенні потреб причетності, прийнятної взаємодії з навколишнім середовищем. Потреби визнання реалізуються у взаємодії з іншими суб'єктами, які можуть виступати об'єктами й управляючими суб'єктами. П'ятий рівень ієрархії потреб можна трактувати як потребу виконувати функції управляючого суб'єкта.

З теорії потреб Маслоу випливає, що процеси забезпечення безпеки є однією з пріоритетних задач системи інтелектуального управління. Звідси також випливає ієрархічність системи інтелектуального управління. На задоволення потреб кожного рівня необхідний відповідний контур управління. Мінімальна кількість контурів управління становить чотири, якщо об'єднати контури, що близькі за функціями й цілями.

Процеси безпеки мають реалізуватись кожним рівнем інтелектуального управління, при цьому пріоритет належить першим контурам управління. Тепер можна почати формулювати цілі інформаційної безпеки відкритої системи. У сфері захисту інформації такі цілі визначені новою парадигмою інформаційної безпеки інформаційних систем. У цій парадигмі для повноцінної роботи або збереження мінімального набору критично важливих функцій система має володіти цілком визначеним запасом стійкості до зовнішніх дестабілізуючих впливів середовища. При цьому порушення цілісності системи на фоні зниження активності її елементів тягне за собою дезорганізацію управління, одночасне зниження активності елементів та їх живучості — втрату гнучкості, а зниження живучості та порушення цілісності системи — втрату найважливіших функцій. Тут виявляється принципова схожість цілей безпеки й управління у відкритих системах.

У відкритій системі існують не менше ніж три “управління” — внутрішнє, зовнішнє і компенсація непрогнозованих впливів зовнішнього світу. Три цикли управління мають таке призначення:

I — управління для підтримання гомеокінетичної стабільності системи як деякий процес “внутрішнього переосмислення”, внутрішньої реструктуризації, зміни цільових установок, зміни в процесі аналізу власної внутрішньої структури;

II — управління для компенсації збурень від зовнішнього світу;

III — зовнішнє управління як цілеспрямована дія деякої зовнішньої системи, яка в даний момент виступає як суб’єкт.

Усі ці управління реалізуються як однотипні на основі парадигми узгодження структури зв’язків даних і в повній логічній схемі передбачаються відповідно три цикли, три процедури суб’єктно-об’єктної взаємодії, які відповідають особливостям і смислу вказаних процесів управління.

Найбільш складним щодо управління, безпеки і небезпечним для існування системи є зовнішнє управління. Поставити фільтр на вході зовнішнього інформаційного потоку буває важко, бо засоби семантичного аналізу та інші механізми прийняття рішень знаходяться далі у середині системи. Тому зовнішнє управління завжди має сприйматись через порівняння наявної структури з тією, яка повинна виникнути при позитивній реакції на управління. Кінцева структура має бути “осмислена” через сприйняття накопиченого образу та логічних висновків щодо безпеки наслідків пропонованої реструктуризації даних. Відкрита система не має сприймати “самовбивчі” для неї команди.

При виробленні логічних висновків із можливих наслідків запропонованої реструктуризації даних результат має попередити можливі катастрофічні наслідки. Складною є також компенсація збурень за рахунок збурень від зовнішнього світу. Вони виявляються через зміну динаміки інформаційних потоків в об’єкті, що управляється. Компенсація зовнішніх збурень

можлива, здебільшого, лише за рахунок розімкнутої системи управління. Дійсно, відновлення динаміки інформаційного потоку, що необхідне для повернення об'єкта в усталений стан, можливе лише за рахунок перебудови його структури, зміни внутрішніх відносин між підсистемами, а вже потім — за рахунок впливу на зовнішній світ.

Управління динамікою інформаційних потоків та забезпечення безпеки передбачає безперервний контроль пересилок інформаційних потоків між підсистемами як за семантикою повідомлень, так і за темпами їх проходження та обробки. Такий контроль є необхідною складовою семантичного аналізу інформації у системі інформаційної безпеки й управління. Без цього частина семантики інформації буде втрачена, а направленість рішень із захисту й управління буде не відповідати цілям управління. Система зі зворотним зв'язком тут не підходить. Для вироблення прийнятних угод між суб'єктом і об'єктом у процесах захисту й управління необхідні структури даних і апарат їх узгодження. Кількісних оцінок тут не може бути, структурні перетворення у базах знань не характеризуються якоюсь метрикою.

Таким чином, узагальнене інтелектуальне управління може бути визначене через:

- задачу стабілізації досягнутого стану як внутрішню функцію певної внутрішньої реструктуризації системи, направлену на утримання системи на гомеокінетичному плато протягом максимально можливого часу;
- задачу переходу у новий стан, коли необхідно забезпечувати перехід системи з одного гомеокінетичного плато на інше, або з однієї групи плато на деяку іншу групу;
- задачу забезпечення функцій, які відносяться до фізичної та інформаційної безпек.

Для кожної системи існує оптимальне дозування управляючих впливів. Недостатнє управління може вивести систему у нестабільний стан з причини "зриву динаміки її існування". У цьому випадку система немовби знаходиться у сфері дії "пози-

тивного зворотного зв'язку", який може призвести систему до повного руйнування.

Введення в систему надмірних управляючих впливів пригнічує смисл інтелектуального управління, веде до насильницької перебудови структур без процесу їх осмислення. У відкритих системах управління зв'язане зі змінами та перетвореннями структури інтелектуальної бази у циклі суб'єктно-об'єктної взаємодії.

В інтелектуальній системі управління є система вводу та оцінки інформаційних потоків для сприйняття зовнішніх управляючих повідомлень і повідомлень із зовнішнього світу. Вихідним потоком інформації треба вважати кінцевий стан зв'язків даних, які встановлюються в інтелектуальній базі після всіх структурних узгоджень і перетворень. Структури об'єкта в кожен момент часу є "вихідним сигналом" для обробки наступної або поточної інформаційної посилки.

Для безпеки пріоритет завжди віддається внутрішньому управлінню, тобто підтриманню стабільності своєї структури. Реакцією інтелектуальної системи може бути відмова від виконання зовнішнього управління, або адекватна реакція на небезпечне управління, яке призводить до втрати стабільного стану. Таким чином, наявна система інтелектуального управління передбачає механізми забезпечення стійкості існування самої системи, тобто її живучості та фізичної безпеки. Залишається вияснити питання забезпечення стабільності функціонального призначення системи з урахуванням вимог до інформаційної безпеки.

Інтелектуальна система управління та безпеки повинна складатись не менше ніж із трьох здвоєних інтелектуальних баз, які відповідають управляючому суб'єкту, зовнішньому світу й об'єкту. Крім того, в ній присутні підсистеми, які приймають і контролюють інформаційні потоки від управляючого суб'єкта й зовнішнього світу, а також підсистема забезпечення безпеки та внутрішнього управління. Приймаючи інформаційні потоки від зовнішнього світу, відповідна підсистема забезпечує синтаксичний та семантичний контроль, а також іденти-

фікацію об'єктів зовнішнього світу. На базі цих інформаційних потоків формуються в інтелектуальній базі даних структури, які відповідають знанням, "образам" зовнішнього світу і які використовуються далі в контурі управління компенсацією впливів зовнішнього світу.

Аналогічні процеси проходять з інформаційними потоками від управляючого суб'єкта за винятком того, що додатково проводиться персоніфікація (автентифікація) суб'єкта. Здвоєні інтелектуальні бази поділяються на ліву половину, де виконується накопичення і коригування знань, та праву половину, де зберігаються накопичені раніше знання (образи) та виробляються реакції на управління і впливи зовнішнього світу за допомогою логіки взаємодії.

Логіка взаємодії побудована таким чином. Інтелектуальна база (ІБ) "Суб'єкт", прийнявши інформацію від зовнішнього управляючого суб'єкта негайно перебудовує всі свої зв'язки. Далі у правій половині ІБ "Суб'єкт" здійснюється порівняння наявної і нової структури для визначення збереження захищеності та стійкості системи, якщо вона згодна на таке управління.

Аналогічно відбувається реструктуризація і контроль захищеності й стійкості у ланцюгу сприймання управління впливом від зовнішнього світу. Наслідки цього нецільового випадкового впливу менші й мають більшу невизначеність. З метою забезпечення безпеки система ІБ "Об'єкт" ізольована від безпосередніх інформаційних потоків зовнішнього світу. Вона структурно залежить від прийнятого рішення й отримує нову інформацію лише в контурі внутрішнього управління після аналізу і вироблення реакції на зовнішні управління для утримання системи на гомеокінетичному плато.

До складу інтелектуальної бази "Об'єкт" входить SIB — security information base (інформаційна база захисту), яка використовується у циклі контролю стану та управління безпекою. Усі три половинки інтелектуальних баз приводяться до нової структури відповідно до вироблених рішень, які враховують усі структурні перетворення в ієрархії та відповідають

вибраній політиці безпеки та управління. Врешті-решт, кожна з правих половинок інтелектуальних баз повідомляє лівій свій узгоджений стан і процес генерації нової інформації завершується, щоб початись далі спочатку.

Цілі захисту інформації, що співпадають з цілями інтелектуального управління. Виходячи з розглянутих властивостей відкритих систем та враховуючи нову парадигму інформаційної безпеки інформаційно-телекомунікаційних систем, цілі захисту інформації у відкритих системах можуть ставитись таким чином. Відкриті системи принципово повинні постійно взаємодіяти з оточуючим зовнішнім середовищем, у яке вони занурені, з метою адаптації до енергетичних та інформаційних потоків нерівноважного світу. Закриття системи, обмеження її зв'язків зменшує її можливості розвитку і може призвести до деградації.

Необхідно розробити систему інформаційної безпеки відкритої системи, яка забезпечила б інформаційно безпечне існування та розвиток відкритої системи в умовах взаємозв'язку з динамічними інформаційними процесами. Система інформаційної безпеки повинна забезпечити певний баланс між певною мірою закритості та збереженням можливостей для адаптації і розвитку. Збалансованість досягається забезпеченням стану стійкої рівноваги (гомеостазу) відкритої інформаційної системи, тобто балансу ентропії зовнішнього середовища та запасу живучості системи. У відкритій системі управління як процес мають включатися процеси забезпечення інформаційної безпеки. Інтелектуальне управління слід перетворювати на безпечне інтелектуальне управління.

Принципи забезпечення інформаційної безпеки

- Процеси забезпечення інформаційної безпеки, як і управління, повинні проводитись на інформаційних потоках внутрішньої і зовнішньої взаємодії з навколишнім оточенням та носіях цих інформаційних потоків.
- Система інформаційної безпеки та механізми безпеки повинні бути не окремо виділеною системою, а органічно

вбудованою невід'ємною складовою системи обробки динамічних потоків інформації.

- Відповідно до поділу управління в інтелектуальній системі на внутрішнє, зовнішнє та компенсацію непрогнозованих впливів зовнішнього світу, система забезпечення інформаційної безпеки відкритої системи теж має складатись з не менш ніж трьох процесів, цілі та механізми дії яких можуть відрізнятись.
- Проблема обмеження зростання кількості контрольованих сутностей і потоків вирішується разом із системою інтелектуального управління шляхом реструктуризації, а саме створенням структур наступних рівнів.

Рішення щодо реструктуризації приймаються з урахуванням вимог до інформаційної безпеки. Доречно зробити зауваження щодо проблеми цінності інформації, що розглядалась у першій частині цієї роботи. У відкритих системах об'єктивної оцінки чи функції цінність інформації не існує, бо оцінка інформації локалізована у конкретній взаємодії. Можна сказати, що "цінність інформації", а не сама інформація, завжди існує лише у контексті, який розглядається, і є породженням трійки: "користувач – задача – вміст бази".

У відкритих системах цінність, корисність, функція старіння конкретних даних, знань, інформації, структур інформації існують у конкретній взаємодії, класифікуються за типами взаємодій і можуть розглядатись як контекстно-залежні функції від поточного контексту. Це співпадає з управляючою функцією інформаційного потоку. Тому мають розглядатись як параметри інтелектуального управління. Цінність належить до категорії управляючих функцій інформації.

Задачі інформаційної безпеки. Класична система інформаційної безпеки робить систему, яка захищається, закритою, що знижує її ефективність. Одна з головних задач полягає у максимальному збереженні можливостей взаємодії з оточуючим середовищем, в ефективному функціонуванні в умовах взаємодії з навколишнім оточенням, тобто створення системи

інформаційної безпеки згідно з законами відкритих систем, зберігаючи при цьому ефективність функціонування і необхідну свободу взаємодії. Процеси забезпечення безпеки є однією з пріоритетних задач системи інтелектуального управління. Пріоритет завжди віддається внутрішньому управлінню, тобто підтриманню стабільності власної структури.

Задачі системи інформаційної безпеки можуть бути класифіковані у такому порядку: забезпечити стійкість і поведінкові (цільові) аспекти системи, що управляється; компенсувати випадкові впливи, які збурюють систему; досягти стану, при якому скомпенсовані випадкові впливи, виявлені, а також блоковані зовнішні впливи, що не відповідають цільовій направленості функціонування системи. Будь-які завчасно не передбачені відхилення практичного стану об'єкта від його теоретичного описання, повинні бути заблоковані таким чином, щоб вони не призвели до катастрофічних наслідків. Система інформаційної безпеки інтелектуальних систем повинна використовувати можливості й засоби роботи з контекстно-залежною інформацією, передбачати підтримку контекстної залежності даних у SIB, забезпечити роботу системи управління на різних контекстах інформаційних потоків у різних ситуаціях.

Системи безпеки майбутнього повинні не тільки і не стільки обмежувати допуск користувачів до програм і даних, скільки визначати і делегувати їх повноваження у корпоративному вирішенні задач, виявляти аномальне використання ресурсів, прогнозувати аварійні ситуації й усувати їх наслідки, гнучко адаптуючи структуру в умовах відмов, часткової втрати або тривалого блокування ресурсів. Вирішення такої задачі дасть можливість оптимізувати також й існуючі системи інформаційної безпеки закритих систем, сучасна теорія яких частково вирішує задачу захисту відкритих систем.

Важливим напрямом досліджень є розробка принципів і реалізація адаптивних систем захисту інформації та розробки систем інформаційної безпеки у зовнішньому контурі управління відкритою системою.

Таким чином, на основі проведеного аналізу сучасних загроз інформаційним ресурсам систем та мереж передачі даних проведено їх класифікацію за базовими критеріями. На основі проведених досліджень запропоновано систему принципів організації захисту інформаційних систем.

Контрольні питання

1. Які принципи лежать в основі системи захисту інформації?
2. У чому полягає принцип мінімальних привілеїв?
3. Як реалізується принцип багаторівневого (комплексного) захисту?
4. Що означає принцип безперервності контролю безпеки?
5. Чому важливий принцип персональної відповідальності користувачів?
6. Які принципи забезпечують баланс між безпекою та доступністю інформації?

Практичне питання

Мета

Сформувати розуміння принципів і правил побудови системи захисту.

Практичні завдання

1. Назвати й пояснити основні принципи захисту (комплексність, безперервність, мінімальні привілеї, багаторівневість тощо).
2. Проаналізувати приклад порушення принципу мінімальних привілеїв.
3. Розробити політику доступу до інформації з використанням принципів захисту.
4. Порівняти принципи захисту інформації та принципи кібербезпеки.

Питання для обговорення

Який принцип є визначальним для державних органів у воєнний час?

ПЕРЕЛІК КЛЮЧОВИХ ІНФОРМАЦІЙНИХ СИСТЕМ ТА РЕЄСТРІВ УКРАЇНИ

1. **Системи соціальної сфери**

   Ключовою системою у соціальній сфері є Єдина інформаційна система соціальної сфери (ЄІССС), яка об'єднує різні підсистеми та реєстри для автоматизації процесів надання соціальної підтримки.

   Регулюючий документ:

   • Про Єдину інформаційну систему соціальної сфери: Закон України від 24.06.2024 р. № 11377 (набрав чинності 18.09.2025). URL: https://ips.ligazakon.net/document/ji11303a

   Основні компоненти та системи, що інтегруються з ЄІССС:

   • Єдиний соціальний реєстр (ЄСР). Основна база даних про отримувачів соціальної підтримки.
   • Реєстр надавачів та отримувачів соціальних послуг. Містить дані щодо суб'єктів, які надають та отримують соціальні послуги.
   • Інтегрована комплексна інформаційна система Пенсійного фонду України (ІКІС ПФУ). Взаємодіє з ЄІССС для обміну даними про пенсійне забезпечення та облік застрахованих осіб.
   • Автоматизована система реєстрації гуманітарної допомоги. Система, що використовується Мінсоцполітики.
   • Електронний кабінет особи з інвалідністю. Сервіс для забезпечення доступу до послуг, зокрема протезування.

2. **Ключові державні реєстри загального призначення**

   Ці реєстри забезпечують роботу більшості державних послуг та інтегруються із соціальною та іншими сферами:

   • Єдиний державний демографічний реєстр. Містить інформацію про особу та її біометричні дані.
   • Державний реєстр фізичних осіб — платників податків. Використовується для ідентифікації громадян.

- Державний реєстр актів цивільного стану громадян. Містить дані про народження, шлюби, розлучення тощо.
- Єдиний державний реєстр юридичних осіб, фізичних осіб — підприємців та громадських формувань (ЄДР). Керується ДП “Національні інформаційні системи” (НАІС).
- Державний земельний кадастр. Система обліку інформації про землі України.
- Державний реєстр речових прав на нерухоме майно. Містить дані про власність на нерухомість.

3. **Галузеві інформаційні системи**
   - Електронна система охорони здоров’я (ЕСОЗ). Центральна база даних, яка взаємодіє з численними (понад 30) приватними медичними інформаційними системами (МІС).
   - Єдина судова інформаційно-телекомунікаційна система (ЄСІТС). Забезпечує автоматизацію судових процесів.
   - Інформаційна система Національної програми інформатизації. Визначає завдання та функціонал для управління державними проєктами інформатизації.
   - Національний реєстр електронних інформаційних ресурсів. Включає всі державні електронні ресурси суб’єктів владних повноважень.
4. **Регулюючі документи (загальні)**
   - Про затвердження переліку інформаційних систем органів виконавчої влади : Постанова Кабінету Міністрів України від 15.09.2023 р. № 1004. URL: https://zakon.rada.gov.ua/go/1004-2023-%D0%BF (дата звернення: 25.11.2025 р.).
   - Про затвердження Положення про Єдину інформаційну систему Національної програми інформатизації: Постанова Кабінету Міністрів України від 27.12.2023 р. № 1406. URL: zakon.rada.gov.ua (дата звернення: 25.11.2025 р.).

АЛГОРИТМ ДІЙ ЩОДО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ У СФЕРАХ СУСПІЛЬНОЇ ДІЯЛЬНОСТІ

Алгоритм призначений для використання відповідальними особами органів, підприємств, установ та організацій, які є власниками або адміністраторами соціальних інформаційних систем (наприклад, ЄІССС, Реєстр ВПО, системи ПФУ тощо).

ЕТАП 1. Аудит, ідентифікація та оцінка ризиків

Мета

Зрозуміти поточний стан безпеки, визначити слабкі місця та можливі загрози.

Ідентифікація активів

Скласти повний перелік усіх інформаційних активів (сервери, бази даних, мережеве обладнання, програмне забезпечення, дані, користувачі).

Визначити власників активів та відповідальних за їх безпеку.

Класифікація інформації

Визначити тип інформації, що обробляється (персональні дані, службова інформація, відкрита інформація, державна таємниця). Класифікація здійснюється відповідно до Закону України “Про захист персональних даних” та інших НПА.

Аналіз загроз та вразливостей

Проаналізувати типові загрози для соціальних систем (фішинг, програми-вимагачі, витік даних, відмова в обслуговуванні).

Оцінити існуючі технічні та організаційні уразливості.

Оцінка ризиків

Визначити ймовірність реалізації загроз та потенційний вплив (збитки) на систему та суб’єктів даних.

Скласти Матрицю ризиків.

ЕТАП 2. Розробка та впровадження політики безпеки та організаційних заходів

Мета

Встановити правила, процедури та розподілити відповідальність для управління безпекою.

Розробка Політики інформаційної безпеки (ПІБ)

Створення офіційного документа, який визначає загальні цілі, принципи та підходи до забезпечення ІБ в організації.

Розробка внутрішньої нормативної документації

Положення про захист персональних даних.

Інструкції користувачів. Правила роботи з інформацією, використання паролів, дії у надзвичайних ситуаціях.

План реагування на інциденти інформаційної безпеки

Призначення відповідальних осіб

Призначення адміністратора безпеки, адміністратора системи, особи, відповідальної за захист персональних даних (DPO).

Навчання персоналу

Регулярне проведення тренінгів та інструктажів з питань кібергігієни, виявлення фішингу та роботи з конфіденційною інформацією.

ЕТАП 3. Побудова комплексної системи захисту інформації (КСЗІ)

Мета

Впровадження технічних засобів для мінімізації ідентифікованих ризиків.

Забезпечення фізичної безпеки

Контроль доступу до серверних приміщень, обладнання, носіїв інформації.

Забезпечення мережевої безпеки

Використання міжмережевих екранів (firewalls), систем виявлення та запобігання вторгненням (IDS/IPS).

Сегментація мережі для ізоляції критично важливих даних.

Захист кінцевих точок (endpoint protection)

Встановлення антивірусного програмного забезпечення та систем захисту робочих станцій.

Криптографічний захист інформації

Застосування шифрування для даних, що зберігаються (at rest) та передаються (in transit), зокрема при використанні віддаленого доступу (VPN).

Використання кваліфікованого електронного підпису (КЕП) для забезпечення цілісності та автентичності даних. Закон України "Про електронні довірчі послуги".

Управління доступом

Впровадження принципу найменших привілеїв (надання доступу лише до необхідної інформації).

Використання надійної автентифікації (багатофакторна автентифікація — MFA).

ЕТАП 4. Моніторинг, аудит та управління інцидентами

Мета

Підтримка актуального рівня безпеки, постійний контроль та готовність до реагування.

Постійний моніторинг

Моніторинг журналів подій безпеки (SIEM-системи) для виявлення підозрілої активності в режимі реального часу.

Використання систем моніторингу доступності сервісів.

Резервне копіювання та відновлення

Регулярне створення резервних копій критичних даних.

Тестування процедур відновлення даних (Disaster Recovery Plan).

Реагування на інциденти

При виявленні інциденту — активація Плану реагування.

Локалізація загрози, її усунення, аналіз причин та відновлення роботи систем.

Повідомлення про інциденти до Урядової команди реагування на комп'ютерні надзвичайні події України (CERT-UA).

Регулярний аудит та тестування

Проведення внутрішніх та зовнішніх аудитів безпеки.

Періодичне тестування на проникнення (penetration testing) для виявлення нових уразливостей.

Мета

Забезпечення легітимності функціонування соціальних систем.

Дотримання законодавства України

Регулярний перегляд та оновлення внутрішньої документації відповідно до змін у Законах України “Про кібербезпеку” та “Про захист персональних даних” тощо.

Сертифікація КСЗІ

Отримання Атестату відповідності на КСЗІ від уповноваженого органу (Держспецзв’язку), що є обов’язковим для державних інформаційних систем.

Взаємодія з регуляторами

Співпраця з Держспецзв’язку, СБУ та Офісом Омбудсмана (у частині захисту ПДн) з питань забезпечення ІБ.

СПИСОК ЛІТЕРАТУРИ

Нормативно-правові акти

1. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650.
2. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР. *Відомості Верховної Ради України*. 1994. № 31. Ст. 286.
3. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.
4. Про Національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241.
5. Про державну таємницю : Закон України від 21.01.1994 р. № 3855-XII. *Відомості Верховної Ради України*. 1994. № 16. Ст. 93.
6. Концепція забезпечення національної безпеки України у сфері інформаційної безпеки : Указ Президента України від 28.12.2016 р. № 47/2017.

Стандарти, міжнародні документи

7. ISO/IEC 27001:2022. Information security management systems — Requirements. Geneva : ISO, 2022.
8. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls. Geneva : ISO, 2022.
9. NIST SP 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations. Gaithersburg : NIST, 2020.
10. NIST SP 800-30 Rev. 1. Guide for Conducting Risk Assessments. Gaithersburg : NIST, 2012.

11. NIST Cybersecurity Framework (CSF). National Institute of Standards and Technology. Washington, 2018.
12. ENISA Threat Landscape 2023. European Union Agency for Cybersecurity. Athens : ENISA, 2023.

Монографії та навчальні посібники

13. *Бойко А. В.* Захист інформації: теорія і практика : навч. посіб. Київ : Кондор, 2020. 312 с.
14. *Герасименко В. А., Гнатюк С. О.* Інформаційна безпека: основи теорії. Київ : НАУ, 2019. 256 с.
15. *Дубов Д. В.* Гібридні війни і безпека інформаційного простору. Київ : НІСД, 2016. 328 с.
16. *Додонов О. Г., Плєснєвич О. В.* Інформаційна безпека та криптографія : підручник. Київ : Ліра-К, 2021. 384 с.
17. *Коваленко І. В.* Методи і засоби захисту інформації : навч. посіб. Харків : ХНЕУ, 2018. 290 с.
18. *Морозов А. В.* Основи кібербезпеки та інформаційного захисту. Дніпро : УДХТУ, 2022. 204 с.
19. *Семенченко А. І., Петрик В. М.* Національна інформаційна безпека: методологія, стратегія, управління. Київ : КНЕУ, 2017. 416 с.
20. *Шеховцов В. В.* Захист інформації в інформаційних системах. Київ : ВД “Славутич-Дельта”, 2020. 288 с.

Наукові статті

21. *Гнатюк С. О.* Криптографічні засоби захисту інформації: сучасний стан та перспективи розвитку. *Інформаційна Безпека*. 2022. № 1. С. 22–33.
22. *Грищенко І. О.* Правові засади інформаційної безпеки держави. *Право України*. 2019. № 7. С. 95–104.
23. *Гусєв В. Є.* Вразливості інформаційних систем: класифікація та методи виявлення. *Кібербезпека та IT-інфраструктура*. 2021. № 2. С. 41–49.
24. *Кохан О. І.* Організаційні методи захисту інформації в державному секторі. *Державне управління та безпека*. 2020. № 3. С. 56–64.

25. *Левченко В. О.* Загрози інформаційній безпеці: тенденції та класифікація. *Військова безпека*. 2020. № 4. С. 78–87.
26. *Чекмарьов Д. Є.* Моделі комплексного захисту інформації в інформаційних системах. *Техніка і засоби зв'язку*. 2021. № 2. С. 12–21.

Звіти, доповіді міжнародних організацій

27. Cybersecurity Report 2023. World Economic Forum. Geneva : WEF, 2023.
28. Global Risks Report 2024. World Economic Forum. Geneva : WEF, 2024.
29. Internet Crime Report 2023. Federal Bureau of Investigation. Washington : FBI, 2023.
30. Data Breach Investigations Report 2023. Verizon. New York, 2023.

Електронні ресурси

31. CERT-UA. Аналіз кіберінцидентів та рекомендації. Режим доступу: https://cert.gov.ua (дата звернення: 20.11.2025 р.).
32. Державна служба спеціального зв'язку та захисту інформації України. Режим доступу: https://www.dsszzi.gov.ua (дата звернення: 20.11.2025 р.).
33. NIST Computer Security Resource Center. Режим доступу: https://csrc.nist.gov (дата звернення: 20.11.2025 р.).

ЗМІСТ

ДЛЯ НОТАТОК

Методичний посібник містить лекційний та практичний матеріали, контрольні питання для перевірки знань студентів, наявні інформаційні ресурси держави, а також список рекомендованої літератури.

Для слухачів курсу "Інформаційна безпека держави та захист інформації у сферах суспільної діяльності", науково-педагогічних працівників, студентів, адвокатів, працівників правоохоронних органів та спеціальних служб.

Навчальне видання

МЕТОДИЧНИЙ ПОСІБНИК
щодо забезпечення практичної роботи
слухачів курсу

"ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ ТА ЗАХИСТ ІНФОРМАЦІЇ У СФЕРАХ СУСПІЛЬНОЇ ДІЯЛЬНОСТІ"

Редактор *Т. К. Валицька*
Коректор *А. А. Тютюнник*
Комп'ютерне верстання *Н. В. Коваленко*

Формат 60×84/16.
Ум. друк. арк. 11,47. Обл.-вид. арк. 7,38. Наклад 30 пр.

Міжрегіональна Академія управління персоналом (МАУП)
03039 Київ-39, вул. Фрометівська, 2

Свідоцтво
про внесення суб'єкта видавничої справи до державного реєстру видавців, виготовлювачів і розповсюджувачів видавничої продукції
ДК № 7066 від 04.06.2020

Виготовлювач: ТОВ "Видавництво Ліра-К"
Свідоцтво № 3981, серія ДК.
03115, м. Київ, вул. С. Чобану, 24
тел.: (050) 462-95-48; (067) 820-84-77
Сайт: lira-k.com.ua, редакція: zv_lira@ukr.net