ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Система захисту від витоку даних на підприємстві»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Вячеслав ОЧЕРЕТЯНИЙ
(підпис)

Виконав: здобувач вищої освіти групи БСД-41
ОЧЕРЕТЯНИЙ Вячеслав
(прізвище, ім'я)

Керівник к.т.н., доцент, Борсуковський Ю.В.
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Систем та технологій кібербезпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
"___" _____ 2025 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Очеретяному Вячеславу Олександровичу
(прізвище, ім'я)

1. Тема кваліфікаційної роботи:
Система захисту від витоку даних на підприємстві

керівник кваліфікаційної роботи Борсуковський Ю.В, к. т. н., доцент
(прізвище, ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «___» _____ 2025 року № ____.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 06.06.2024 р.

3. Вихідні дані до кваліфікаційної роботи
Інформаційні ресурси підприємства;
рішення щодо впровадження системи захисту від витоку даних;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти у сфері інформаційної безпеки.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1.Дослідження основних понять захисту від витоку даних на підприємстві.
2.Аналіз методів та засобів захисту інформації для запобігання витоку даних.
3.Розробка рекомендацій щодо впровадження системи захисту від витоку даних на підприємстві.

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 28.02.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми захисту від витоку даних на підприємстві.	03.03.2025 р.	
2.	Аналіз наукової та технічної літератури з питань інформаційної безпеки та методів захисту даних.		
3.	Аналіз нормативної бази та сучасних технологій захисту від витоку даних на підприємствах.		
4.	Практична оцінка існуючих засобів та методів захисту від витоку даних у підприємствах.		
5.	Розробка рекомендацій щодо впровадження системи захисту від витоку даних на підприємстві.		
6.	Оформлення результатів дослідження.		
7.	Підготовка доповіді до захисту.	06.06.2025 р.	

Здобувач вищої освіти _____ Вячеслав ОЧЕРЕТЯНИЙ
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Юрій БОРСУКОВСЬКИЙ
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача ОЧЕРЕТЯНОГО Вячеслава
на тему: «Система захисту від витоку даних на підприємстві»

Актуальність:

. Забезпечення захисту від витоку даних є критично важливим завданням для будь-якого сучасного підприємства, особливо в умовах зростання кіберзагроз та збільшення обсягів оброблюваної інформації. Надійні системи захисту допомагають запобігати несанкціонованому доступу, втратам і викраденню конфіденційних даних. Тема кваліфікаційної роботи є актуальною та відповідає сучасним викликам інформаційної безпеки.

Позитивні сторони:

1. У роботі наведено огляд нормативно-правової бази та технічних аспектів захисту від витоку даних на підприємстві.
2. Проаналізовано сучасні методи та технології запобігання витоку даних, а також їх реалізацію у різних програмних і апаратних рішеннях.
3. Надано практичні рекомендації щодо впровадження системи захисту від витоку даних у підприємстві.
4. Матеріал викладено логічно, послідовно, з дотриманням норм наукового стилю. Використані джерела є актуальними, а висновки — обґрунтованими.

Недоліки:

1. Було б доцільно розширити аналіз конкретних випадків витоку даних та заходів реагування на них у реальних підприємствах.
2. В роботі варто було б окремо розглянути потенційні ризики і обмеження впровадження систем захисту у контексті сучасних гібридних загроз.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **“добре”**, а здобувач(ка) **ОЧЕРЕТЯНИЙ Вячеслав** – присвоєння кваліфікації бакалавр з кібербезпеки за освітньою програмою Інформаційна та кібернетична безпека**.**

Рецензент:

(науковий ступінь, вчене звання)	*(підпис)*	*(ім’я, прізвище)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на здобуття освітнього ступеня бакалавра

Направляється здобувач ОЧЕРЕРЕТЯНИЙ Вячеслав до захисту кваліфікаційної роботи
(прізвище, ім'я)

спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: «Система захисту від витоку даних на підприємстві».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Євгенія ІВАНЧЕНКО
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач ***ОЧЕРЕТЯНИЙ Вячеслав*** обрав тему роботи, метою якої було дослідити методи та засоби захисту кінцевих точок організації та розробка рекомендацій щодо її реалізації. Перелік використаних джерел свідчить про вміння здобувачем розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***ОЧЕРЕТЯНИЙ Вячеслав*** показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***ОЧЕРЕТЯНОГО Вячеслава*** на оцінку "**добре**" та присвоїти йому кваліфікацію бакалавр з кібербезпеки за освітньою програмою Інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Юрій БОРСУКІВСЬКИЙ
(підпис) *(ім'я, прізвище)*
"____" _____ 2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **ОЧЕРЕТЯНИЙ Вячеслав** допускається до захисту
даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Систем та технологій кібербезпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 58 сторінок, 6 рисунків, 18 джерел.

Об'єкт дослідження – Система захисту від витоку даних на підприємстві.

Предмет дослідження – Методи та засоби забезпечення захисту інформації для запобігання витоку даних на підприємстві.

Мета роботи – дослідити існуючі системи та методи захисту від витоку даних на підприємствах, визначити основні принципи їх впровадження, а також розробити рекомендації щодо ефективного впровадження такої системи для підвищення рівня інформаційної безпеки.

Методи дослідження – опрацювання наукових джерел з обраної тематики, аналіз нормативної документації, вивчення сучасних технологій захисту інформації, проведення порівняльного та функціонального аналізу.

Система захисту від витоку даних є ключовим інструментом для забезпечення конфіденційності, цілісності та доступності інформації на підприємстві. Впровадження таких систем дозволяє виявляти та запобігати несанкціонованому доступу, викраденню або втраті важливої інформації під час її обробки та зберігання.

У роботі проаналізовано основні компоненти систем захисту від витоку даних, методи контролю доступу, технології моніторингу та запобігання інцидентам безпеки. Розглянуто нормативно-правові вимоги щодо захисту інформації в Україні.

Розроблено рекомендації для підприємств щодо вибору та впровадження ефективних систем захисту від витоку даних з урахуванням існуючих інформаційних систем та організаційних процесів.

Застосування систем захисту від витоку даних значно підвищує рівень інформаційної безпеки, дозволяє контролювати витоки інформації та забезпечує відповідність вимогам законодавства.

На основі проведеного дослідження запропоновано покрокову методику впровадження системи захисту від витоку даних на підприємстві для підвищення безпеки та цілісності інформації.

Галузь використання – інформаційна безпека, захист даних у підприємницькій діяльності..

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

DLP – Data Loss Prevention

IDS – Intrusion Detection System

IPS – Intrusion Prevention System

MFA – Multi-Factor Authentication

SIEM – Security Information and Event Management

UEBA – User and Entity Behavior Analytics

IAM- Identity and Access Management

BYOD – Bring Your Own Device

VPN – Virtual Private Network

GDPR – General Data Protection Regulation

ВСТУП

У сучасну епоху цифрових технологій інформація є одним із найважливіших ресурсів, що забезпечують ефективне функціонування будь-якого підприємства. Гарантування її безпеки, цілісності та конфіденційності є основним завданням у сфері інформаційної безпеки. Зі зростанням обсягів оброблюваної та збереженої інформації виникає нагальна потреба у впровадженні комплексних систем захисту від витоку даних, які здатні запобігати несанкціонованому доступу, втратам та викраденню інформації.

Система захисту від витоку даних на підприємстві являє собою сукупність технічних, організаційних та програмних заходів, які спрямовані на забезпечення контролю за переміщенням конфіденційної інформації, виявлення потенційних загроз та запобігання витокам даних. Ефективне впровадження таких систем дозволяє мінімізувати ризики втрати важливої інформації, підвищити рівень довіри до інформаційних процесів і відповідати вимогам законодавства щодо захисту персональних та комерційних даних.

Тема дослідження є актуальною у зв’язку із збільшенням кількості кібератак, спрямованих на викрадення корпоративної інформації, а також необхідністю дотримання сучасних нормативних вимог у сфері інформаційної безпеки. Ефективна система захисту від витоку даних є ключовою складовою загальної стратегії безпеки підприємства.

Виникає потреба у розробці комплексних, практичних рекомендацій щодо впровадження систем захисту від витоку даних, які враховують особливості функціонування конкретних підприємств, наявність технологічних рішень та рівень підготовки персоналу. Це дозволить підвищити ефективність захисту інформаційних активів та мінімізувати ризики, пов’язані з витоком даних.

Метою даної роботи є дослідження існуючих підходів до захисту від витоку даних, аналіз технічних, організаційних та правових аспектів систем захисту, а також формування практичних рекомендацій щодо їх впровадження в умовах конкретного підприємства.

Вищевказане визначає актуальність теми кваліфікаційної роботи, основний

зміст якої становлять методи та засоби захисту від витоку даних з метою забезпечення цілісності, конфіденційності та доступності інформації на підприємстві.

Сучасна практика свідчить, що традиційні методи захисту інформації вже не є достатніми в умовах зростання кількості кібератак та складності інформаційних систем. Системи захисту від витоку даних активно впроваджуються у фінансовому секторі, державних установах та комерційних організаціях. Важливим фактором є не лише технологічна складова, а й нормативне регулювання, підготовка персоналу та інтеграція систем у загальну інформаційну інфраструктуру підприємства.

Успішне впровадження систем захисту вимагає комплексного підходу до технічних, організаційних та правових аспектів безпеки.

1. АНАЛІЗ ПРОБЛЕМИ ВИТОКУ ДАНИХ НА ПІДПРИЄМСТВІ

1.1 Види та джерела витоку даних

З розвитком цифрових технологій, розширенням використання хмарних сервісів та віддаленого доступу до корпоративних ресурсів, питання збереження конфіденційності інформації стало ключовим для кожного сучасного підприємства. Витік даних (Data Leak або Data Breach) — це процес несанкціонованого розголошення або передачі інформації, яка повинна залишатися в межах організації. Такий інцидент може бути як навмисним, так і ненавмисним, але в будь-якому випадку він загрожує серйозними наслідками для бізнесу.

Види витоку даних

У загальному випадку витоки даних можна класифікувати за кількома ознаками:

1. **За способом реалізації:**
    - **Фізичний витік.** Передбачає копіювання даних на фізичні носії інформації (наприклад, флешки, диски) без належного контролю або дозволу. Сюди ж входять фотографування екранів, виведення конфіденційної інформації на друк.
    - **Цифровий витік.** Здійснюється через інформаційні системи — передачу даних електронною поштою, через хмарні сервіси, програми для обміну повідомленнями (месенджери), веб-інтерфейси, API тощо.
    - **Пасивний витік.** Має місце, коли конфіденційна інформація потрапляє до зловмисників через прослуховування мереж, перехоплення пакетів, недосконалу конфігурацію серверів або відсутність шифрування.
    - **Активний витік.** Це цілеспрямовані дії з копіювання, збереження, передавання або публікації конфіденційних даних.
2. **За каналами передачі:**
    - **Електронна пошта.** Один із найчастіших каналів витоку, особливо у випадках, коли конфіденційна інформація пересилається неавторизованим одержувачам.

- **Месенджери та соціальні мережі.** Популярні сервіси обміну повідомленнями (Viber, Telegram, WhatsApp, Facebook Messenger) часто використовуються для несанкціонованої передачі даних.
- **Знімні носії.** USB-накопичувачі, зовнішні жорсткі диски тощо, при неналежному контролі використовуються для виведення даних за межі організації.
- **Хмарні сервіси.** Google Drive, Dropbox, OneDrive — популярні, але потенційно небезпечні ресурси, якщо не впроваджено DLP або політики доступу.
- **Фізичний друк.** Документи, виведені на принтер, можуть бути втрачені або передані стороннім особам.

3. **За навмисністю:**
   - **Навмисні витоки.** Здійснюються із корисливою або шкідливою метою: продаж інформації конкурентам, саботаж, промислове шпигунство.
   - **Ненавмисні витоки.** Виникають внаслідок помилок користувачів, неправильного налаштування прав доступу, використання застарілого програмного забезпечення.

Джерела витоку даних

До основних джерел витоку даних на підприємствах належать:

- **Інсайдери** — співробітники або підрядники, які мають законний доступ до інформації, але з різних причин зловживають цим доступом. Часто саме внутрішній персонал становить найбільшу загрозу безпеці, адже має прямий доступ до даних і знає слабкі місця в системах безпеки.
- **Користувачі з низькою безпековою культурою.** Вони можуть ненавмисно надіслати файл не тому адресату, використовувати прості паролі, завантажувати підозрілі вкладення тощо.
- **Зловмисники (аутсайдери).** Вони отримують доступ до інформації через фішинг, шкідливе програмне забезпечення, експлуатацію вразливостей, атаки на мережеву інфраструктуру.

- **Автоматизовані системи.** Налаштовані з помилками або без урахування політик доступу, вони можуть ненавмисно викладати дані в загальний доступ.
- **Партнери та контрагенти.** У деяких випадках витік відбувається через сторонні організації, які мають доступ до внутрішніх систем або даних підприємства.

Приклади реальних інцидентів

- **Equifax (2017):** Внаслідок уразливості в веб-додатку витекли персональні дані понад 147 млн осіб.
- **Facebook (2019):** Незахищені бази даних користувачів виявилися у відкритому доступі, що призвело до витоку понад 540 млн записів.
- **Укрпошта (2023):** Під час внутрішньої перевірки виявлено передачу клієнтських даних співробітником у месенджері сторонній особі.

Особливої уваги потребує класифікація витоків даних відповідно до намірів суб'єкта, який спричинив витік:

- **Умисний витік** відбувається внаслідок навмисних дій зловмисника, часто з фінансовою або конкурентною мотивацією. Прикладом є продаж клієнтських баз стороннім особам або завантаження конфіденційної інформації до публічних ресурсів. Такі витоки здебільшого реалізуються інсайдерами, включно зі співробітниками, які мають легальний доступ до критичних ресурсів.
- **Ненавмисний витік** зазвичай є результатом помилки працівника або недосконалості процесів. Найпоширеніші ситуації — відправлення листа не тому адресатові, збереження документа в незахищеному публічному каталозі, використання слабких паролів тощо. В умовах недостатньої підготовки персоналу ризик таких витоків зростає.

Іншим важливим аспектом є типи інформації, що можуть бути об’єктами витоку. До найпоширеніших належать:

- персональні дані працівників або клієнтів;
- фінансові звіти та платіжні реквізити;

- комерційна таємниця (наприклад, технічна документація, внутрішні звіти, стратегії);
- результати наукових або маркетингових досліджень;
- логіни, паролі, сертифікати доступу до інформаційних систем.

Також класифікація витоків даних передбачена у низці міжнародних стандартів і рекомендацій, зокрема:

- **ISO/IEC 27001** – визначає вимоги до систем управління інформаційною безпекою (СУІБ), де витоки ідентифікуються як інциденти безпеки.
- **NIST SP 800-53** – містить набір контролів для запобігання витоку, особливо в контексті державного та критичного інфраструктурного секторів.
- **GDPR (ЄС)** – передбачає обов'язкове повідомлення про витік персональних даних регулятору упродовж 72 годин.

Таким чином, розуміння джерел та видів витоку даних дозволяє не лише ефективно реагувати на інциденти, а й розробляти превентивні політики безпеки з урахуванням специфіки підприємства, його структури, сфери діяльності та рівня цифрової зрілості.

1.2 Основні причини та наслідки витоку

Аналіз інцидентів інформаційної безпеки, зафіксованих упродовж останніх років, свідчить про те, що витік даних найчастіше зумовлений не одним, а комплексом взаємопов'язаних факторів. Ці фактори можна умовно розділити на людські, технічні, організаційні та зовнішні впливи.

Людські причини

1. Ненавмисні помилки співробітників.

Найчастіше працівники, не усвідомлюючи рівень конфіденційності даних, допускають помилки під час роботи з ними. Наприклад:

- надсилання листа з вкладенням на неправильну електронну адресу;
- публікація файлів у відкритому хмарному сховищі без налаштування обмежень доступу;
- передача логінів і паролів у незахищеному вигляді через месенджери.

2.Низький рівень кіберграмотності.

Більшість користувачів не володіють достатніми знаннями з основ інформаційної безпеки. Вони можуть відкривати фішингові посилання, використовувати прості або однакові паролі на різних ресурсах, не звертати уваги на підозрілу активність на своїх облікових записах.

3. Зловмисні дії інсайдерів.

Співробітники з доступом до критичних систем і даних можуть навмисно здійснювати витік інформації. Причинами таких дій часто є конфлікти на роботі, звільнення, фінансова мотивація або підкуп конкурентами. Інсайдерські витоки найважче виявляти та контролювати.

Технічні причини

1. Недосконалість технічної інфраструктури.

Використання застарілих операційних систем, непатчених програмних рішень або відсутність систем виявлення вторгнень (IDS/IPS) відкриває численні вектори атак. У багатьох компаніях немає шифрування даних на носіях або у каналах зв’язку, що робить їх вразливими до перехоплення.

2. Погане адміністрування.

Приклади включають:

- неправильне налаштування прав доступу (надмірні права);
- публічний доступ до відкритих папок чи баз даних;
- залишення сервісів або портів відкритими для Інтернету.

3. Відсутність моніторингу і журналювання.

Без журналів подій та систем моніторингу адміністратори не можуть вчасно виявити витік, що вже стався. Це ускладнює реагування, і зловмисники мають більше часу для розвитку атаки.

Організаційні причини

1. Відсутність політик безпеки.

Якщо в компанії не визначено правила поводження з конфіденційними даними (класифікація інформації, політики доступу, політики BYOD), кожен працівник діє на власний розсуд, що підвищує ризики витоку.

2. Відсутність контролю над третіми сторонами.

Підрядники, аутсорсингові команди, зовнішні консультанти часто мають доступ до важливої інформації, але їхня діяльність не регулюється або не перевіряється належним чином. У разі витоку через третю сторону компанія несе повну відповідальність.

3. Відсутність навчання персоналу.

Навіть при наявності технічних засобів захисту, без навчання працівники залишаються найслабшою ланкою у системі безпеки. Один невірно відкритий лист або завантаження зараженого файлу може нівелювати всі інші заходи.

Зовнішні фактори

1. Атаки з боку хакерських угруповань.

Особливо небезпечними є атаки з використанням вразливостей нульового дня або складних багатовекторних стратегій (APT-атаки), спрямованих на поступове проникнення до внутрішньої мережі організації.

2. Промислове шпигунство.

В умовах жорсткої конкуренції деякі компанії вдаються до незаконного добування інформації про своїх конкурентів, що включає зломи, підкуп співробітників, використання шкідливих програм.

Наслідки витоку даних

Витік даних має різнорівневі наслідки, які зачіпають всі напрями діяльності підприємства:

1. Фінансові збитки.

   Прямі втрати включають штрафи регуляторів (наприклад, згідно з GDPR), судові витрати, витрати на розслідування інциденту, оновлення інфраструктури, а також непрямі втрати — втрата клієнтів, падіння акцій, зниження продажів.

2. Репутаційні ризики.

   Довіра клієнтів і партнерів може бути зруйнована назавжди. Після публічного скандалу організації доводиться витрачати значні ресурси на відновлення іміджу.

3. Юридичні наслідки.

   Компанія може зіткнутися з позовами, відкриттям кримінальних проваджень проти посадових осіб, перевірками контролюючих органів.

4. Операційні порушення.

   Внаслідок інциденту може бути втрачено критично важливі дані або зупинено основні бізнес-процеси, що загрожує простоєм виробництва або недоступністю сервісів для клієнтів.

5. Витрати на реагування та відновлення.

   Організації змушені інвестувати у дорогі рішення для аудиту, резервного копіювання, тестування безпеки, навчання персоналу, укріплення інфраструктури.

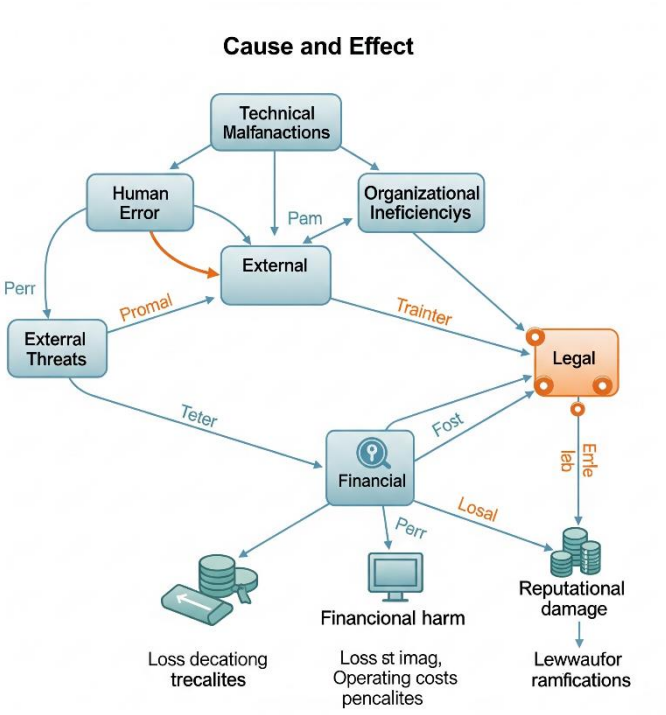

Рис 1.2 Діаграма "Причини та наслідки"

Поглиблений аналіз причин витоку: сучасні виклики

У сучасному цифровому середовищі все частіше трапляються комбіновані інциденти, коли технічні та організаційні недоліки поєднуються з діями людини. Наприклад, відсутність двофакторної автентифікації (технічна причина) у поєднанні з фішинговою атакою (людський фактор) призводить до компрометації облікового запису з правами доступу до бази клієнтів.

Зростання популярності мобільної роботи та використання особистих пристроїв у робочих цілях (модель BYOD — *Bring Your Own Device*) створює нові ризики витоку даних. Дані, які опиняються на особистих смартфонах або ноутбуках, часто не шифруються, а знищення їх після завершення роботи не контролюється. У таких умовах особливої актуальності набуває впровадження політик мобільної безпеки, а також DLP-рішень, які можуть виявляти підозрілу активність на пристроях користувачів.

Ще один виклик — використання хмарних сервісів без узгодження з IT-відділом (так званий *shadow IT*). Користувачі самостійно зберігають документи в особистих Google Drive чи Dropbox, не замислюючись про безпеку або контроль доступу. У таких випадках витік може бути випадковим, але дуже небезпечним, оскільки компанія навіть не підозрює про загрозу.

Роль керівництва у формуванні причин

Часто однією з глибинних причин витоку є недостатнє розуміння значення інформаційної безпеки з боку керівництва. Якщо менеджмент не ініціює або не підтримує впровадження стандартів безпеки, політик доступу, процедур реагування на інциденти — підрозділи безпеки залишаються ізольованими і не мають інструментів впливу на бізнес-процеси. Такий підхід призводить до того, що захист будується формально або фрагментарно, без комплексного охоплення.

Статистичні приклади

Відповідно до звіту IBM Security «Cost of a Data Breach Report 2023»:

- У середньому компанії виявляють витік через 204 дні після його виникнення, а реагують — ще через 73 дні.
- 83% організацій повідомили, що хоча б один витік даних був пов'язаний з людським фактором.
- Компанії, які мали автоматизовані системи захисту даних (наприклад, DLP або SIEM), зменшили середню вартість інциденту на понад 1,5 мільйона доларів.

Ці дані підтверджують критичну необхідність запровадження проактивного моніторингу та швидкого реагування, адже чим довше компанія не знає про витік,

тим більшими будуть збитки.

1.3 Класифікація загроз витоку даних

У сучасних умовах кіберзагроз захист даних є критично важливою складовою діяльності будь-якого підприємства. Одним із перших етапів у побудові системи запобігання витоку є ідентифікація можливих загроз, які можуть спричинити порушення конфіденційності, цілісності або доступності інформації. Для цього використовується класифікація загроз — процес систематизації потенційних інцидентів за певними ознаками. Такий підхід дозволяє структурувати інформацію про джерела небезпеки, способи реалізації атак, об’єкти впливу та інші важливі параметри.

Одним із основних критеріїв класифікації є джерело загрози. У загальному випадку загрози можуть походити як ізсередини організації (внутрішні інсайдери), так і ззовні (зовнішні зловмисники). Внутрішні загрози є особливо небезпечними через наявність у користувачів доступу до внутрішніх ресурсів, знання архітектури IT-систем і обхідних шляхів захисту. Зовнішні загрози, своєю чергою, переважно реалізуються через фішинг, шкідливе програмне забезпечення, мережеві атаки, використання вразливостей тощо.

Ще одним важливим аспектом є спосіб витоку даних. Найбільш поширеними каналами є електронна пошта, зовнішні накопичувачі, хмарні сервіси, веб-інтерфейси, системи обміну миттєвими повідомленнями та навіть фізичні засоби (друк, фото, сканування). У багатьох випадках витік може відбутися і через пасивні або побічні канали, наприклад, залишені тимчасові файли, лог-файли, помилково надані публічні посилання тощо.

Щодо об’єкта впливу, загрози класифікуються за типами даних, які можуть бути скомпрометовані. Це можуть бути персональні дані співробітників або клієнтів, комерційна таємниця, інтелектуальна власність, фінансові документи, технічні конфігурації, облікові дані доступу тощо. Кожен тип інформації має свою критичність і регулюється відповідними нормативними актами. Наприклад, витік персональних даних підпадає під регулювання загального регламенту ЄС із захисту даних (GDPR), українського Закону «Про захист персональних даних» та ряду

інших стандартів.

Також загрози витоку класифікують за наміром суб’єкта. У цьому контексті розрізняють умисні та ненавмисні загрози. Умисні загрози, як правило, пов’язані з корисливою або шкідливою мотивацією — це може бути саботаж, зрада, шантаж, фінансова вигода або конкуренція. Ненавмисні загрози часто виникають через необізнаність, неуважність або порушення процедур співробітниками, які не усвідомлюють значення захисту даних.

Важливо також враховувати властивість інформації, яку порушує загроза. Це може бути порушення конфіденційності (незаплановане розкриття або передача інформації), цілісності (несанкціонована модифікація або підміна) або доступності (втрата доступу до даних через знищення, блокування або відмову системи). Найбільш критичними є загрози, які впливають одночасно на кілька властивостей, наприклад, зловмисне програмне забезпечення, яке спершу викрадає, а потім шифрує дані.

Додатково загрози можуть класифікуватися за ступенем наслідків: незначні (локальні інциденти без суттєвого впливу), середні (що потребують внутрішнього розслідування та мають вплив на процеси), критичні (завдають значної шкоди репутації, фінансам, юридичному стану компанії). Важливою також є класифікація за фазою реалізації — завершені (коли витік вже відбувся) та потенційні (загрози, що можуть виникнути в майбутньому за наявності вразливостей).

У сучасних міжнародних стандартах, таких як ISO/IEC 27005 (управління ризиками інформаційної безпеки), NIST SP 800-30 (управління ризиками інформаційних систем), загрози класифікуються з урахуванням контексту організації, її активів та ймовірності реалізації загрози. Такий підхід дозволяє не лише систематизувати знання, але й створювати адаптивні моделі захисту, що відповідають реальним умовам бізнесу.

Отже, детальна та багатовимірна класифікація загроз витоку даних є ключовим елементом у процесі побудови ефективної системи захисту інформації на підприємстві. Вона дозволяє не лише розуміти можливі сценарії інцидентів, але й проєктувати запобіжні заходи, адаптовані до конкретної IT-інфраструктури,

політик компанії та зовнішніх викликів інформаційного середовища.

Ефективна побудова системи кіберзахисту підприємства, зокрема системи запобігання витоку даних (Data Loss Prevention, DLP), неможлива без повного розуміння й класифікації загроз, що можуть призвести до компрометації конфіденційної інформації. Класифікація загроз є критично важливим етапом у процесі оцінювання ризиків, розробки політик інформаційної безпеки, а також формування архітектури захисту.

У сучасних умовах загрози витоку даних мають складну багатовимірну природу, і лише інтегральний підхід до їх класифікації дає змогу виявити справжні джерела та сценарії реалізації атак. Це особливо важливо в умовах цифрової трансформації бізнесу, впровадження віддаленої роботи, мультихмарної інфраструктури, використання сторонніх постачальників послуг (SaaS, IaaS, PaaS) та інтеграції зі сторонніми інформаційними системами.

Одним із базових підходів є класифікація за походженням загрози. За цим критерієм виділяють внутрішні та зовнішні загрози. До внутрішніх загроз належать дії співробітників або партнерів, які мають авторизований доступ до систем. Це може бути як свідоме порушення (шпигунство, саботаж, викрадення інформації), так і ненавмисні дії (помилкова відправка документів, недотримання політик безпеки, неправильне використання хмарних сховищ тощо). Зовнішні загрози надходять ззовні організації і реалізуються хакерами, конкурентами, організованими злочинними угрупованнями або навіть державами. Їх реалізація може охоплювати цілеспрямовані атаки, фішинг, соціальну інженерію, злам систем, використання шкідливого програмного забезпечення, експлуатацію вразливостей.

Класифікація за каналом витоку розкриває способи фізичної чи логічної передачі інформації за межі контрольованого середовища. Найпоширенішими каналами є:

- **Електронна пошта** — найбільш використовуваний і ризикований канал. Часто співробітники надсилають конфіденційні файли не тим адресатам або через неконтрольовані сервіси.
- **Знімні носії інформації** — USB-флешки, SD-карти, зовнішні диски. Без

належного контролю можуть бути легко використані для копіювання й винесення інформації.

- **Хмарні сервіси** — Google Drive, Dropbox, iCloud та інші, які використовуються працівниками для зручного зберігання, але можуть містити уразливі конфігурації (наприклад, публічний доступ до файлів).
- **Месенджери та соціальні мережі** — WhatsApp, Telegram, Viber, Facebook Messenger активно використовуються для ділового спілкування, але водночас мають обмежені можливості контролю з боку служби безпеки.
- **Веб-браузери** — передача даних через форми, веб-пошта, публікації на форумах, блоги, особисті сайти.

Інформація, яка піддається витоку, також класифікується за типом. Серед найбільш цінних і чутливих даних:

- **Персональні дані** (ПІБ, паспортні дані, банківська інформація, геолокація);
- **Комерційна таємниця** (клієнтські бази, маркетингові стратегії, договори);
- **Фінансова інформація** (звіти, бюджети, банківські операції);
- **Інтелектуальна власність** (технічна документація, патенти, алгоритми);
- **Інформація ІТ-рівня** (паролі, конфігурації мереж, доступи до серверів).

Ще один принциповий підхід — класифікація за мотивацією порушника:

- **Умисні загрози** — реалізуються навмисно заради особистої вигоди, помсти, конкурентної боротьби, ідеологічних переконань або фінансової винагороди. Прикладами є співробітник, що виносить клієнтську базу для передачі новому роботодавцеві, або сторонній хакер, який зламує сервери з метою продажу даних у даркнеті.
- **Ненавмисні загрози** — виникають унаслідок необережних або помилкових дій користувачів. Наприклад, неуважність під час вибору адресата листа або завантаження конфіденційного документа у відкритий доступ.

Класифікація за властивістю інформації, що порушується, базується на моделі CIA (Confidentiality, Integrity, Availability), яка є основою інформаційної безпеки:

- **Порушення конфіденційності** — несанкціоноване розкриття даних.
- **Порушення цілісності** — спотворення, модифікація або підміна даних.
- **Порушення доступності** — блокування доступу до даних або втрата їх назавжди.

У деяких випадках порушуються одночасно кілька властивостей, наприклад, коли після крадіжки даних зловмисники видаляють або шифрують їх, вимагаючи викуп (атаки типу ransomware).

Крім того, загрози класифікують за ступенем завершеності (реалізовані, спроби, потенційні) та за масштабом впливу (локальні, широкі, критичні). Наприклад, витік документа одного працівника — локальний інцидент, а компрометація всієї бази клієнтів з адресами, телефонами і номерами карт — масова критична загроза.

У сучасній практиці кібербезпеки використовуються стандартизовані методології оцінювання загроз, серед яких:

- **ISO/IEC 27005** — рекомендації щодо аналізу ризиків та загроз інформаційній безпеці;
- **NIST SP 800-30** — керівництво з управління ризиками інформаційних систем;
- **MITRE ATT&CK Framework** — таксономія технік, які використовуються зловмисниками на різних етапах атак, включно з ексфільтрацією даних.

Класифікація загроз витоку даних не є статичною. Вона повинна постійно оновлюватися відповідно до змін у технологіях, поведінці користувачів, моделі бізнесу, вимогах регуляторів та поточному стану кіберзагроз у світі. Наприклад, із розвитком штучного інтелекту виникають нові ризики витоку через автоматизоване генерування контенту, а з поширенням хмарних сервісів актуальними стають витоки через некоректну інтеграцію API або загальнодоступні S3-бакети в Amazon Web Services.

Таким чином, глибоке розуміння природи, форм прояву та класифікації загроз витоку даних є основою формування стратегії інформаційної безпеки підприємства. Саме систематизований підхід до загроз дає змогу оцінити ймовірність, потенційні наслідки та обрати релевантні заходи захисту з

урахуванням галузевої специфіки, технологічної інфраструктури та організаційної структури.

На додаток до традиційних класифікацій, у сучасній практиці кібербезпеки все частіше застосовується класифікація загроз витоку даних за сценарієм атаки. Це дає змогу детальніше аналізувати поведінку порушника на кожному етапі інциденту — від первинного проникнення до ексфільтрації інформації. Так, згідно з моделлю Cyber Kill Chain, розробленою Lockheed Martin, витік даних найчастіше є результатом завершального етапу складної багаторівневої атаки, яка включає:

- розвідку (розпізнавання цілей),
- експлуатацію вразливостей (наприклад, через фішинг),
- встановлення шкідливого програмного забезпечення (бекдорів),
- внутрішнє горизонтальне переміщення в мережі (lateral movement),
- збір цільової інформації та її витік через заздалегідь підготовлений канал.

Також дедалі частіше враховуються галузеві особливості загроз. Наприклад:

- У **банківському секторі** — найбільш небезпечним є витік даних клієнтів, реквізитів платіжних карток, схем внутрішнього аудиту та регламентів.
- У **медичній сфері** — витоки стосуються персональних медичних записів, історій хвороб, що регулюються міжнародними стандартами типу HIPAA.
- У **виробничій галузі** — загрозу становить компрометація технологічної документації, креслень, рецептур тощо.
- У **державному секторі** — витоки персональних даних громадян, службових документів, інформації з обмеженим доступом можуть мати національну або навіть міжнародну загрозу.

Крім того, при класифікації загроз слід враховувати рівень контролю, який організація має над джерелами загроз:

- **Контрольовані загрози** — наприклад, витік через локального працівника, чия діяльність моніториться, або з внутрішніх серверів із DLP.
- **Неконтрольовані загрози** — це витоки через зовнішніх підрядників, хмарні сервіси без належного захисту, сторонні додатки, інтеграції з API.

Особливу категорію становлять так звані "повільні витоки" (slow exfiltration),

коли інформація виводиться частинами, тривалий час, у незначних обсягах, щоб не викликати підозру. Такі витоки часто здійснюються за допомогою маскування — наприклад, викрадена інформація кодується в DNS-запити або приховується в непримітних файлах типу зображень (техніка стеганографії).

У розрізі методів формалізації загроз, сучасні системи оцінювання інформаційних ризиків (наприклад, OCTAVE, STRIDE, DREAD) пропонують формальні моделі для опису загроз із зазначенням:

- **мотиву** (наприклад, фінансова вигода, політична мета),
- **способу реалізації** (через API, незахищений Wi-Fi, тощо),
- **впливу** (на фінанси, репутацію, юридичні зобов'язання),
- **ймовірності** реалізації,
- **можливостей реагування** (чи можна виявити, зупинити, відстежити джерело).

Ці підходи особливо важливі для створення каталогів загроз та ризик-орієнтованих моделей безпеки, які застосовуються в рамках ISO 27001, GDPR, PCI DSS, а також національних вимог до критичної інфраструктури.

Важливо також зазначити, що класифікація загроз повинна адаптуватися до мінливого цифрового середовища. Наприклад, із поширенням ChatGPT-подібних систем та генеративного ШІ з'явилися нові загрози, коли конфіденційна інформація вводиться користувачами у відкриті ШІ-інтерфейси без розуміння наслідків. Це створює нову категорію витоків — інформаційна недбалість у взаємодії з системами штучного інтелекту, яку важко відстежити через відсутність централізованого контролю.

Отже, класифікація загроз витоку даних повинна бути багатофакторною, динамічною та практично орієнтованою. Вона має враховувати не лише технічні й людські аспекти, але й стратегічний контекст функціонування підприємства, міжнародні регуляторні вимоги, технологічну архітектуру та специфіку бізнесу. Лише така систематизація дозволяє побудувати ефективну модель інформаційної безпеки, здатну реагувати на сучасні загрози витоку даних.

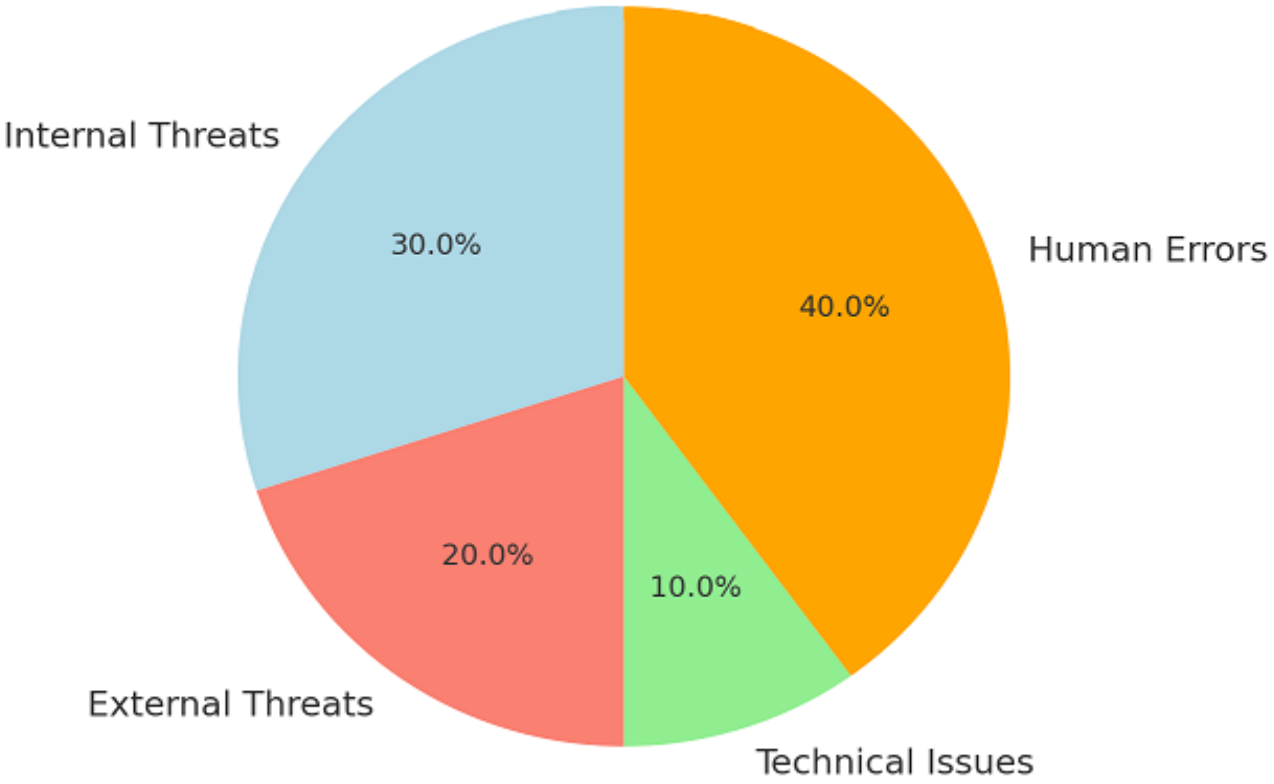

Рис.1.3 Діаграма, що класифікує загрози на основі різних категорій

2. Методи та засоби запобігання витоку даних

2.1. Підходи до побудови систем захисту

Сучасна інформаційна безпека підприємств вимагає комплексного і системного підходу до захисту конфіденційної інформації від несанкціонованого доступу, зловживань та витоків. Для ефективного запобігання витоку даних необхідно застосовувати багаторівневі заходи, що охоплюють як технічні, так і організаційні аспекти безпеки.

Комплексний підхід до захисту даних

Перш за все, побудова системи захисту від витоку даних базується на інтеграції кількох компонентів: технологічних засобів контролю, політик і процедур, навчання персоналу, а також моніторингу і реагування на інциденти. Цей підхід передбачає, що жоден окремий захід не є достатнім сам по собі, а тільки їх поєднання дозволяє ефективно мінімізувати ризики.

Основні принципи побудови системи

1. Принцип найменших привілеїв.

   Доступ до інформаційних ресурсів має надаватись виключно тим користувачам і процесам, які потребують його для виконання своїх функцій. Обмеження прав мінімізує можливості випадкового або умисного витоку.

2. Сегментація мережі та ізоляція критичних систем.

   Розділення корпоративної мережі на зони з різним рівнем довіри і доступу дозволяє локалізувати потенційні загрози та ускладнює зловмиснику пересування внутрішніми системами.

3. Впровадження політик безпеки.

   Чітко сформульовані і доведені до кожного працівника правила роботи з інформацією, правила поводження з конфіденційними даними, використання корпоративних пристроїв і додатків.

4. Використання технологій шифрування.

   Шифрування даних у стані спокою (на дисках, носіях) і при передачі (мережеві канали) гарантує, що навіть у разі витоку інформація залишатиметься недоступною для зловмисника.

5. Моніторинг і аудит.

   Впровадження систем журналювання, моніторингу подій безпеки (SIEM) та аналізу поведінки користувачів дозволяє виявляти підозрілі дії в режимі реального часу та своєчасно реагувати на інциденти.

6. Автоматизація контролю та реагування.

   Використання рішень класу DLP, систем виявлення вторгнень, автоматизованих засобів ізоляції уражених систем і блокування шкідливих операцій.

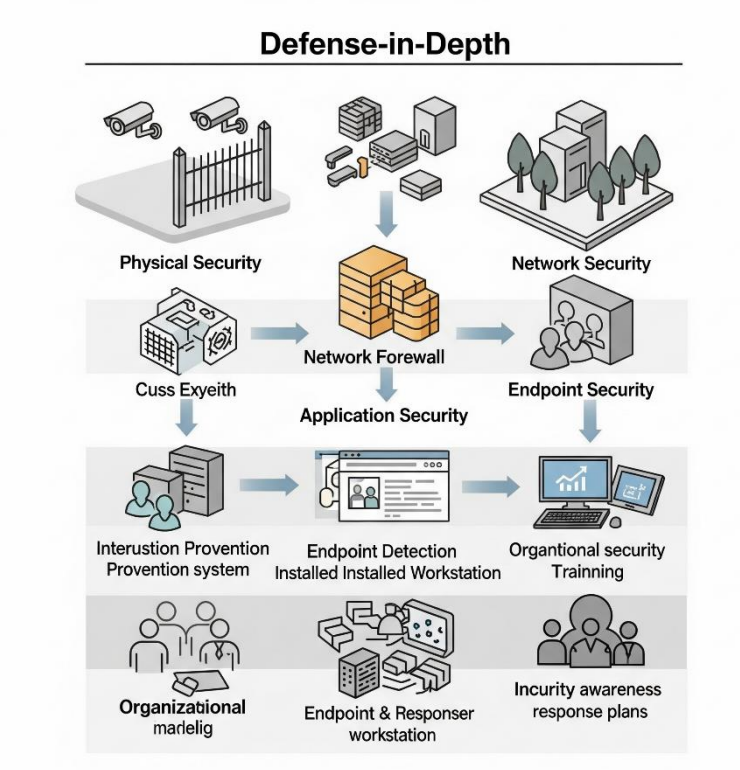

Рис 2.1 Схема багаторівневого захисту (Defense-in-Depth)

Технологічні компоненти систем захисту

Серед ключових технологічних засобів, що формують сучасну систему захисту від витоку даних, можна виділити:

- Data Loss Prevention (DLP) — технологія, яка контролює рух даних по корпоративній мережі, на кінцевих точках і в хмарних сервісах. DLP-системи аналізують зміст файлів і повідомлень, застосовують політики відповідно до типу і важливості інформації, блокують або попереджають про спроби передачі конфіденційних даних.

- Ідентифікація і аутентифікація користувачів — впровадження систем багатофакторної аутентифікації (MFA), єдиного входу (SSO), а також управління правами доступу (IAM) забезпечує надійність контролю за тим, хто має доступ до інформації.
- Шифрування даних — реалізується на рівні файлових систем, баз даних, електронної пошти, а також у мережевих протоколах (TLS, VPN). Це обов'язкова умова для захисту від перехоплення і несанкціонованого використання даних.
- Системи моніторингу та аналізу поведінки (UEBA) — застосовують алгоритми машинного навчання для виявлення аномальної активності користувачів, що може свідчити про потенційний витік.
- Технології ізоляції і сегментації мережі — застосування VLAN, DMZ, Zero Trust Architecture, що вимагає перевірки кожного доступу до ресурсів незалежно від місця користувача.

Організаційні заходи

Важливою складовою є підготовка персоналу, формування культури безпеки, регулярне навчання і перевірка знань. Окрім того, підприємство має впроваджувати процеси внутрішнього аудиту, оцінки відповідності політикам безпеки, а також мати розроблені плани реагування на інциденти.

Взаємодія з нормативними вимогами

Побудова системи захисту також має враховувати міжнародні та національні нормативні документи, такі як GDPR, ISO/IEC 27001, NIST, PCI DSS, які визначають вимоги до захисту даних і рекомендовані практики. Відповідність цим стандартам підвищує довіру партнерів і клієнтів та мінімізує ризики юридичної відповідальності.

Таким чином, системний і комплексний підхід до побудови захисту від витоку даних є запорукою збереження цінної інформації та забезпечення безперервності бізнесу.

Захист від витоку даних є ключовим напрямком інформаційної безпеки підприємств у сучасному цифровому середовищі. Враховуючи постійне зростання

обсягів оброблюваної інформації, розповсюдження мобільних і хмарних технологій, а також еволюцію кібератак, системи захисту мають бути багатошаровими, гнучкими та адаптивними.

Багаторівневий захист: концепція Defense-in-Depth

Одним із фундаментальних підходів у побудові систем безпеки є концепція **Defense-in-Depth** (багаторівневого захисту). Вона передбачає створення послідовних, взаємодоповнюючих механізмів захисту на різних рівнях інформаційної системи — від фізичного рівня і мережі до прикладного програмного забезпечення і користувацького рівня. Основна ідея — якщо один рівень захисту буде скомпрометований, інші залишаться активними, зменшуючи ймовірність успішного витоку даних.

Архітектура системи захисту від витоку даних

Побудова системи захисту від витоку передбачає інтеграцію наступних ключових компонентів:

- **Політики безпеки** — чітко визначені правила та норми поводження з інформацією, права та обов’язки співробітників, вимоги до захисту конкретних типів даних.
- **Технологічні рішення**, які реалізують контроль та моніторинг за дотриманням політик. Це системи Data Loss Prevention (DLP), системи управління ідентифікацією та доступом (IAM), шифрування, системи управління подіями безпеки (SIEM).
- **Організаційні заходи** — навчання і підвищення обізнаності співробітників, формування культури безпеки, внутрішні аудити, регулярне тестування системи захисту.
- **Процеси реагування на інциденти** — плани дій у разі виявлення порушень, координація між IT-відділом, службою безпеки і керівництвом підприємства.

Ключові принципи побудови системи захисту від витоку даних

1. **Принцип найменших привілеїв**

   Забезпечення мінімального необхідного рівня доступу до інформації для кожного користувача або процесу. Це дозволяє обмежити масштаби

можливого витоку та зменшити ризик зловживання.

2. **Захист даних на всіх етапах їх життєвого циклу**

   Від моменту створення і обробки до зберігання, передачі і знищення. Система має контролювати всі ці етапи, запобігаючи витоку на будь-якому з них.

3. **Автоматизація контролю та моніторингу**

   Використання сучасних засобів автоматизації (DLP, SIEM, UEBA) дозволяє виявляти аномалії, порушення політик, потенційні загрози у реальному часі і оперативно реагувати.

4. **Інтеграція систем захисту з бізнес-процесами**

   Безпека не повинна гальмувати роботу підприємства. Важливо, щоб захисні механізми були прозорими для користувачів, мінімізували навантаження і не створювали зайвих бар'єрів.

5. **Контроль і захист на кінцевих точках (Endpoint Security)**

   Оскільки більшість витоків здійснюються через робочі станції, ноутбуки і мобільні пристрої, застосування EDR (Endpoint Detection and Response) і антивірусних рішень є необхідною складовою.

6. **Сегментація мережі та архітектури Zero Trust**

   Перехід від традиційної моделі довіри всередині корпоративної мережі до моделі «нікому не довіряй, завжди перевіряй» (Zero Trust) дозволяє ефективно контролювати доступ до ресурсів і знижувати ризики внутрішніх витоків.

Основні технології, що використовуються у системах захисту від витоку даних

- **Data Loss Prevention (DLP)**

  DLP-системи аналізують зміст і контекст інформації, що передається через мережу, або зберігається на кінцевих точках, з метою запобігання передачі конфіденційних даних за межі організації. Вони підтримують політики, які визначають, які дані є захищеними, кому дозволено з ними працювати, і які дії є забороненими (копіювання, пересилання, друк).

- **Шифрування**

Захист інформації у стані спокою (на дисках, базах даних) та під час передачі (мережеві протоколи SSL/TLS, VPN). Навіть у разі фізичного вилучення носіїв чи перехоплення мережевого трафіку інформація залишається недоступною.

- **Ідентифікація, аутентифікація і управління доступом (IAM)**
  Сучасні системи дозволяють реалізовувати багатофакторну аутентифікацію, єдиний вхід (SSO), динамічне визначення прав доступу на основі ролей або атрибутів користувачів.
- **Моніторинг і аналіз поведінки користувачів (UEBA)**
  Використання штучного інтелекту і машинного навчання для виявлення аномалій у поведінці користувачів, які можуть свідчити про зловмисні дії або витік даних.
- **Системи управління інформаційною безпекою (ISMS)**
  Комплексний підхід, що включає політики, процедури, стандарти, технології і людські ресурси для управління ризиками безпеки інформації.

Організаційні аспекти

Одним із важливих елементів є постійне навчання і підвищення обізнаності персоналу. Соціальна інженерія та людський фактор залишаються одними з головних причин витоків, тому регулярні тренінги, тестування на фішинг, а також формування культури безпеки є незамінними.

Підприємство має також розробити і підтримувати в актуальному стані плани реагування на інциденти, які передбачають швидке виявлення витоку, локалізацію, мінімізацію наслідків і відновлення нормальної роботи.

Відповідність нормативам і стандартам

Реалізація системи захисту від витоку даних також повинна відповідати вимогам національного і міжнародного законодавства, а також галузевих стандартів. Це не лише забезпечує правову безпеку підприємства, а й підвищує довіру партнерів і клієнтів. Наприклад:

- **GDPR** регламентує захист персональних даних;
- **ISO/IEC 27001** визначає вимоги до систем управління інформаційною

безпекою;

- **PCI DSS** регламентує захист даних платіжних карток.

Таким чином, побудова системи захисту від витоку даних є багатокомпонентним процесом, що включає взаємодію технологічних, організаційних та управлінських заходів. Тільки комплексний підхід забезпечує необхідний рівень безпеки та мінімізує ризики витоків, що загрожують стабільності та репутації підприємства.

обудова ефективної системи захисту від витоку даних вимагає застосування інтегрованого підходу, що охоплює комплекс технічних, організаційних та процедурних заходів. Сучасні виклики у сфері кібербезпеки — зростання складності атак, багатоканальні витоки, розвиток хмарних технологій і мобільних робочих середовищ — вимагають від підприємств не лише стандартних рішень, але й впровадження інноваційних методів захисту.

Комплексний багаторівневий захист

Одним із фундаментальних принципів побудови системи захисту від витоку даних є реалізація багаторівневого захисту (Defense-in-Depth). Цей принцип полягає в тому, що інформація захищається не одним механізмом, а рядом взаємопов’язаних технологій і політик, що охоплюють усі етапи життєвого циклу даних.

Кожен рівень має власні методи і засоби контролю, наприклад:

1)Фізичний рівень: контроль доступу до приміщень, серверних кімнат, захист апаратного забезпечення.

2)Мережевий рівень: використання міжмережевих екранів (firewalls), систем виявлення і запобігання вторгнень (IDS/IPS), сегментація мережі.

3)Рівень доступу: управління ідентифікацією та доступом (IAM), багатофакторна аутентифікація, політики найменших привілеїв.

4)Прикладний рівень: системи контролю і моніторингу дій користувачів, DLP-рішення, шифрування інформації.

5)Рівень навчання персоналу: регулярне навчання, тестування на фішинг, підвищення культури безпеки.

6)Визначення політик і норм

Успішність системи захисту багато в чому залежить від наявності чітких, задокументованих і впроваджених політик безпеки, що регламентують роботу з інформацією. Ці політики повинні визначати класифікацію інформації (наприклад, публічна, конфіденційна, секретна), правила доступу, порядок обробки, зберігання і знищення даних.

Важливо, щоб політики були зрозумілі і доведені до усіх співробітників, а також щоб існували механізми їх дотримання і контролю. Без цього навіть найсучасніші технології будуть малоефективними.

Технологічні рішення

У структурі системи захисту від витоку даних ключову роль відіграють технологічні інструменти:

- **Data Loss Prevention (DLP):** системи DLP виконують моніторинг, аналіз і контроль інформації, що передається або зберігається, з метою запобігання несанкціонованому копіюванню, пересиланню або викраденню. Вони здатні розпізнавати конфіденційні дані на основі контентного аналізу (ключові слова, регулярні вирази, патерни даних), контексту операцій і поведінкових моделей.
- **Шифрування:** як для збереження інформації у спокої, так і під час передачі. Використання алгоритмів AES, RSA, TLS/SSL забезпечує, що у разі компрометації фізичних носіїв або мережевого трафіку дані залишаться недоступними для зловмисників.
- **Системи управління ідентифікацією і доступом (IAM):** реалізують принцип найменших привілеїв, контролюють аутентифікацію користувачів (зокрема, багатофакторну), забезпечують аудит і звітність щодо доступу.
- **Моніторинг поведінки користувачів (UEBA):** аналізує типові патерни поведінки та визначає аномалії, які можуть свідчити про компрометацію облікового запису або підготовку витоку.
- **Системи управління подіями інформаційної безпеки (SIEM):** збирають, корелюють і аналізують лог-файли та події з різних джерел для виявлення

потенційних загроз у режимі реального часу.

- **Технології Zero Trust:** передбачають перевірку кожного запиту на доступ незалежно від розташування користувача, що значно знижує ризики внутрішніх витоків.

Контроль за кінцевими точками і мобільними пристроями

Оскільки значна частина інформації обробляється на кінцевих пристроях (ПК, ноутбуки, смартфони), особлива увага приділяється захисту цих точок:

- Використання EDR-рішень, які забезпечують постійний моніторинг подій безпеки, швидке виявлення шкідливої активності, ізоляцію уражених пристроїв.
- Впровадження політик BYOD з чітким контролем використання особистих пристроїв для робочих цілей.
- Захист мобільних пристроїв через MDM (Mobile Device Management) із можливістю шифрування, віддаленого блокування і стирання даних.

Організаційні заходи

- Проведення регулярних тренінгів і підвищення обізнаності співробітників, зокрема щодо соціальної інженерії і фішингових атак.
- Встановлення чітких процедур реагування на інциденти, що включають швидке виявлення, локалізацію, повідомлення відповідальних осіб та зовнішніх регуляторів у разі необхідності.
- Розробка внутрішніх аудиторських процедур для контролю дотримання політик безпеки.
- Підтримка культури безпеки, де співробітники розуміють свою роль у запобіганні витокам і активно долучаються до процесу захисту.

Відповідність нормативним вимогам

Побудова системи захисту від витоку даних обов’язково має враховувати міжнародні стандарти (ISO/IEC 27001, NIST), законодавчі акти (GDPR, Закон України «Про захист персональних даних»), а також галузеві вимоги (PCI DSS для фінансових організацій, HIPAA для медичних закладів). Відповідність цим нормам не лише знижує ризики, а й забезпечує юридичний захист підприємства.

Приклади успішної реалізації

Відомі світові компанії, такі як Microsoft, IBM, Cisco, використовують багатошарові системи захисту, що включають власні DLP-рішення, аналітику поведінки користувачів і інтелектуальні системи реагування на інциденти. Це дозволяє їм оперативно виявляти витоки і мінімізувати шкоду.

Таким чином, побудова системи захисту від витоку даних — це складний і багатогранний процес, який вимагає поєднання технологічних, організаційних і процедурних рішень, постійного аналізу загроз і адаптації до нових викликів кібербезпеки.

2.2 Огляд DLP-рішень: архітектура, компоненти, функції

У системах захисту від витоку даних особливе місце займають технології **Data Loss Prevention (DLP)** — комплексні рішення, спрямовані на виявлення, запобігання та контроль несанкціонованого доступу або передачі конфіденційної інформації за межі організації. DLP-системи стали невід'ємною частиною корпоративної безпеки, оскільки вони дозволяють реалізувати політики безпеки на рівні змісту даних, а не лише на рівні мережевої інфраструктури.

Архітектура DLP-систем

Архітектура сучасних DLP-рішень зазвичай включає кілька основних компонентів, що працюють у взаємодії, забезпечуючи моніторинг і контроль даних на різних рівнях:

1. **Агенти кінцевих точок (Endpoint Agents).**

   Встановлюються на робочих станціях, ноутбуках, мобільних пристроях. Вони контролюють локальну активність користувача: збереження файлів, копіювання на зовнішні носії, пересилання через пошту або месенджери. Агенти можуть блокувати спроби витоку і повідомляти адміністраторам про інциденти.

2. **Мережеві сенсори (Network Sensors).**

   Моніторять мережевий трафік, що проходить через корпоративні шлюзи, електронну пошту, веб-трафік, FTP, хмарні сервіси. Вони аналізують пакети даних, виявляють конфіденційну інформацію та блокують спроби її передачі

поза межі дозволеного.

3. **Сервер управління (Management Server).**

   Центральний компонент, який здійснює налаштування політик безпеки, збирає звіти з агентів і сенсорів, проводить кореляцію подій, визначає ризики та координує реагування.

4. **Консолі адміністрування і звітності.**

   Забезпечують інтерфейс для налаштування системи, перегляду інцидентів, генерації звітів для керівництва та аудиторів.

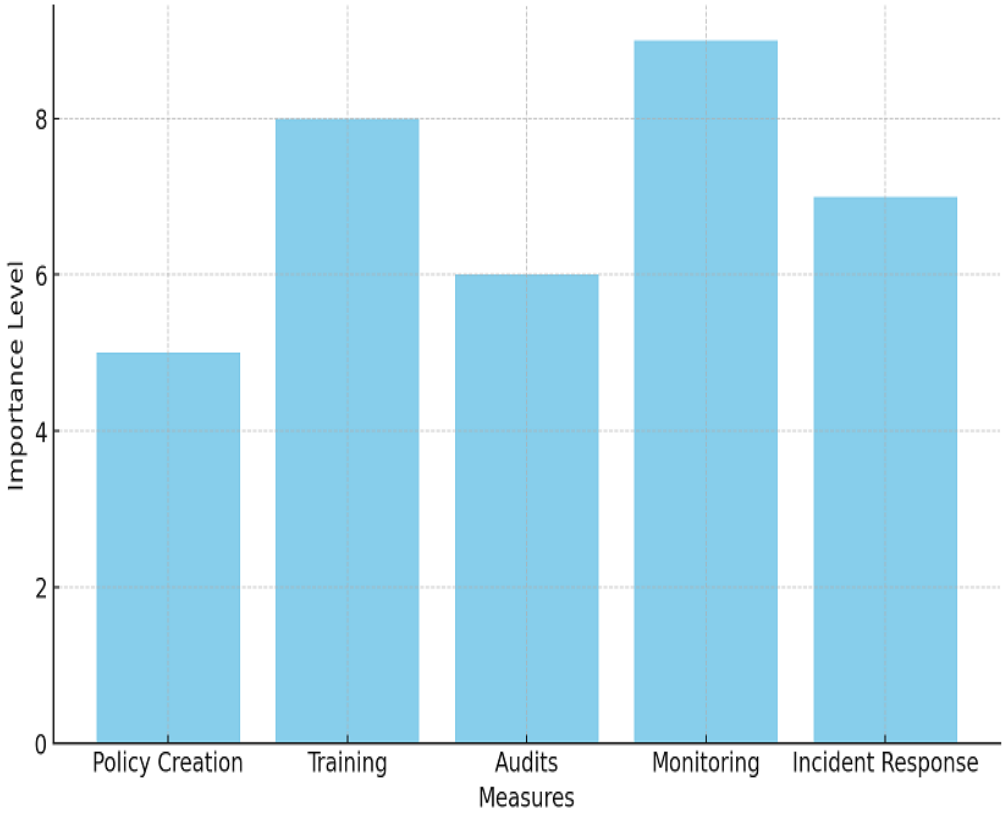

Рис2.2 Схема архітектури DLP-системи, що показує взаємодію між компонентами

Основні функції DLP-систем

- **Ідентифікація конфіденційних даних.**

  DLP-системи використовують різноманітні методи для виявлення захищеної інформації: пошук за ключовими словами, регулярними виразами (наприклад, номери кредитних карток, паспортів), шаблонами, аналіз контексту, машинне навчання.

- **Моніторинг і контроль передачі даних.**

Система відслідковує всі спроби копіювання, передачі, друку, завантаження файлів, а також роботу з електронною поштою, веб-браузерами, месенджерами, хмарними сервісами.

- **Блокування або попередження про порушення.**
  Залежно від налаштувань, DLP може блокувати операції, які порушують політику безпеки, або попереджати користувача і адміністратора для подальшого аналізу.
- **Аудит та звітність.**
  Документування всіх інцидентів, створення детальних логів, статистика спроб передачі конфіденційних даних, що дозволяє проводити розслідування та оцінку ефективності заходів.
- **Інтеграція з іншими системами безпеки.**
  DLP зазвичай інтегруються з SIEM, IAM, системами антивірусного захисту, шлюзами безпеки для створення єдиної екосистеми безпеки.

Особливості впровадження

Впровадження DLP-системи вимагає попереднього аудиту інформаційних потоків підприємства, класифікації інформації, визначення пріоритетних напрямів контролю. Крім того, важливо налагодити роботу з персоналом для адаптації політик і навчання користувачів.

Приклади рішень на ринку

На ринку представлено багато провідних DLP-рішень від компаній Symantec (Broadcom), McAfee, Forcepoint, Digital Guardian, Microsoft (Azure Information Protection). Кожне має свої особливості архітектури, підтримує різні типи агентів і пропонує унікальні функції аналітики.

Крім зазначених технологічних і організаційних аспектів, при побудові системи захисту від витоку даних важливо також враховувати аналіз ризиків і пріоритезацію захисних заходів. Підприємства повинні ідентифікувати найбільш критичні активи і визначити потенційні вектори атак, щоб сконцентрувати ресурси на захисті найціннішої інформації. Такий підхід дозволяє оптимізувати інвестиції в безпеку та підвищити загальну ефективність системи.

Сучасні організації все частіше впроваджують моделі Zero Trust, які передбачають, що ніхто всередині мережі не є автоматично довіреним, а кожен доступ до ресурсів має перевірятися незалежно від місцезнаходження користувача чи пристрою. Це суттєво знижує ризики внутрішніх витоків, пов’язаних із неправомірним використанням легітимних облікових записів.

Також актуальним є використання аналітики поведінки користувачів (User and Entity Behavior Analytics, UEBA), яка за допомогою алгоритмів машинного навчання і штучного інтелекту виявляє аномальні дії, що можуть бути індикаторами витоку або підготовки до нього. Наприклад, раптове масове копіювання файлів, незвичний час активності або спроби доступу до незвичних ресурсів.

Особливу увагу слід приділяти автоматизації процесів реагування. Впровадження систем автоматичного блокування підозрілих дій, повідомлення відповідальних осіб, ізоляції інфікованих пристроїв або сесій дозволяє значно скоротити час виявлення і локалізації інцидентів.

Не менш важливим є аспект постійного аудиту та удосконалення системи безпеки. Загрози постійно змінюються, з’являються нові вразливості та методи атак, тому система захисту повинна бути гнучкою і адаптивною. Регулярний аналіз інцидентів, перевірка відповідності політикам, оновлення програмних рішень та підвищення кваліфікації персоналу є обов’язковими складовими ефективного управління ризиками витоку даних.

У сучасному світі важливо також враховувати законодавчі та нормативні вимоги до захисту даних, які дедалі жорсткіше регулюють діяльність підприємств. Відповідність таким вимогам не лише знижує ризики санкцій, а й підвищує довіру клієнтів і партнерів.

Отже, побудова системи захисту від витоку даних — це не одноразовий проєкт, а безперервний процес, що потребує інтеграції технологій, організаційних заходів, навчання і постійного контролю, спрямований на збереження цілісності і конфіденційності інформації підприємства.

2.3 Організаційні заходи контролю

Організаційні заходи контролю є важливою складовою системи захисту від витоку даних на підприємстві. Вони створюють рамки, у межах яких технічні засоби безпеки можуть ефективно працювати, а також формують культуру безпеки, яка мінімізує ризики, пов’язані з людським фактором. Організаційний контроль включає розробку політик, норм і процедур, навчання персоналу, розмежування відповідальності, а також механізми аудиту і моніторингу.

Розробка політик безпеки інформації

Основою організаційних заходів є чітко сформульовані і документовані політики безпеки, які визначають правила поводження з інформацією на підприємстві. Вони повинні охоплювати:

- Класифікацію інформації — визначення рівнів конфіденційності (наприклад, публічна, внутрішня, конфіденційна, секретна) з відповідними вимогами до зберігання, передачі та обробки.
- Правила доступу — порядок надання, зміни і відкликання доступу до інформаційних ресурсів, принцип найменших привілеїв.
- Використання IT-ресурсів — обмеження на використання носіїв інформації, встановлення програмного забезпечення, доступ до мережі, робота з хмарними сервісами.
- Обробка інцидентів — визначення процедур виявлення, документування, розслідування та реагування на інциденти безпеки.
- Відповідальність і санкції — чітке визначення відповідальності співробітників за порушення політик і заходи дисциплінарного впливу.

Політики повинні регулярно переглядатися та оновлюватися відповідно до змін технологій, загроз і нормативних вимог.

Розмежування повноважень і контроль доступу

Важливим заходом є чітке розмежування обов’язків і прав доступу серед співробітників, що мінімізує ризик несанкціонованого доступу або витоку інформації. Наприклад, особи, відповідальні за адміністрування систем, не повинні мати необмежений доступ до конфіденційних бізнес-даних без контролю.

Крім того, впровадження систем контролю доступу, таких як RBAC (Role-Based Access Control) або ABAC (Attribute-Based Access Control), дозволяє гнучко керувати правами на основі ролей або атрибутів користувачів.

Навчання і підвищення обізнаності персоналу

Оскільки більшість витоків даних пов’язані з людським фактором — необережністю або недостатньою обізнаністю — регулярне навчання є критично важливим. Програми навчання повинні включати:

- Ознайомлення зі стандартами і політиками безпеки підприємства.
- Тренінги з розпізнавання фішингових і соціально-інженерних атак.
- Інструктажі щодо безпечного поводження з конфіденційною інформацією.
- Проведення тестувань на проникнення, симуляцій фішингу і оцінка поведінки співробітників.

Такі заходи допомагають формувати відповідальне ставлення до безпеки і знижують ризики помилок.

Внутрішній аудит і моніторинг дотримання політик

Регулярний внутрішній аудит дозволяє оцінити ефективність впроваджених заходів, виявити порушення та слабкі місця. Аудит включає:

- Перевірку відповідності політикам безпеки.
- Аналіз логів і звітів DLP, SIEM, UEBA.
- Оцінку роботи систем реагування на інциденти.
- Інтерв’ю з персоналом і оцінку знань.

Результати аудиту використовуються для коригування політик і вдосконалення системи захисту.

Планування та тестування реагування на інциденти

Організаційні заходи повинні передбачати наявність чітких планів реагування на інциденти, які включають:

- Швидке виявлення і локалізацію витоку.
- Повідомлення відповідальних осіб і керівництва.
- Проведення розслідування та усунення причин.
- Відновлення інформаційної системи.

- Інформування зовнішніх регуляторів, якщо це передбачено законодавством.

Регулярне тестування планів за допомогою тренувань і симуляцій підвищує готовність підприємства до реальних інцидентів.

Формування культури безпеки

Організаційні заходи мають бути спрямовані не лише на технічні аспекти, а й на формування корпоративної культури безпеки. Це включає мотивацію співробітників до дотримання політик, відкритий діалог про кіберзагрози, підтримку ініціатив з безпеки, а також створення безпечного середовища для повідомлення про підозрілі події без страху покарання.

Таким чином, організаційні заходи контролю є фундаментом, на якому базується ефективність технічних рішень і загальна система захисту підприємства від витоку даних. Без чітких політик, навчання, аудиту і культури безпеки технічні засоби не зможуть повною мірою забезпечити надійний захист інформації.

Важливо також впроваджувати системи внутрішнього контролю та звітності, які дозволяють виявляти відхилення від політик безпеки в режимі реального часу. Це можуть бути регулярні перевірки використання корпоративних ресурсів, моніторинг аномалій у поведінці користувачів, а також оцінка ефективності заходів безпеки на основі ключових показників (KPI).

Значну увагу слід приділяти керуванню ланцюгом постачання і взаємодії з партнерами, адже часто витік даних відбувається через сторонні організації або підрядників. Впровадження вимог до безпеки у договорах, аудит постачальників та регулярний контроль дотримання безпекових стандартів допоможуть мінімізувати ці ризики.

Ще одним важливим аспектом є організація ефективної комунікації між підрозділами — інформаційною безпекою, IT, юридичним відділом, кадровою службою та менеджментом. Вчасний обмін інформацією про інциденти, зміни в політиках і нові загрози сприяє оперативному реагуванню і профілактиці витоків.

Не менш актуальним є впровадження процедур контролю змін (Change Management), які регламентують внесення будь-яких змін до інформаційних систем, конфігурацій та політик безпеки. Це знижує ймовірність випадкових

помилок, що можуть призвести до витоку інформації.

Для підвищення мотивації співробітників варто розробляти програми винагород і визнання за дотримання стандартів безпеки, що допомагає створити позитивне ставлення до безпеки на всіх рівнях організації.

3. Розробка варіанту системи захисту від витоку даних на підприємстві

3.1. Формування політик безпеки

Політики безпеки інформації є фундаментальним елементом системи захисту підприємства від витоку даних. Вони встановлюють загальні правила, стандарти та норми поведінки, що регламентують використання, зберігання та передачу інформаційних ресурсів, а також визначають відповідальність за їх дотримання. Формування чітких і зрозумілих політик безпеки забезпечує єдине бачення безпеки в організації, сприяє координації дій різних підрозділів і створює основу для впровадження технічних і організаційних заходів контролю.

Основні цілі політик безпеки

Політики безпеки мають на меті:

- Захистити конфіденційну, цінну і критичну інформацію від несанкціонованого доступу, витоку, втрати або пошкодження.
- Визначити правила класифікації і обробки інформації відповідно до її важливості і рівня конфіденційності.
- Регламентувати порядок надання і контролю доступу до інформаційних систем і ресурсів.
- Сприяти формуванню культури безпеки серед співробітників через визначення їх ролей і відповідальності.
- Встановити стандарти для безпечної роботи з інформацією на всіх рівнях організації.
- Забезпечити відповідність нормативним та законодавчим вимогам.

Структура політик безпеки

Типова політика безпеки містить наступні розділи:

1. Вступ і область застосування

   Опис мети документа, сфер застосування політики, категорій інформації, на яку поширюються правила, а також визначення термінів і понять.

2. Обов’язки і відповідальність

   Визначення ролей і відповідальності різних груп користувачів — від

керівництва до звичайних співробітників, а також підрозділів IT та безпеки.

3. Класифікація інформації

   Правила і критерії поділу інформації на класи (наприклад, публічна, внутрішня, конфіденційна, секретна), що визначають рівень захисту і доступу.

4. Управління доступом

   Порядок надання, зміни і відкликання доступу до інформаційних ресурсів, використання аутентифікації і авторизації, принцип найменших привілеїв.

5. Правила поводження з інформацією

   Вимоги до збереження, передачі, копіювання, друку, архівування і знищення інформації.

6. Політика безпеки кінцевих точок і мережі

   Вказівки щодо безпечного використання робочих станцій, мобільних пристроїв, мережевого обладнання, використання VPN, антивірусного захисту.

7. Обробка інцидентів безпеки

   Процедури виявлення, повідомлення, розслідування і реагування на інциденти, включаючи план дій при витоку даних.

8. Навчання і підвищення обізнаності

   Визначення механізмів навчання співробітників і підтримки їх знань у сфері безпеки.

9. Відповідальність і санкції

   Наслідки порушення політик, дисциплінарні заходи, юридична відповідальність.

Процес розробки політик

Розробка політик безпеки є багатоступеневим процесом, який включає:

- Залучення ключових стейкхолдерів

  До розробки залучаються керівники різних рівнів, IT-фахівці, служба безпеки, юридичний відділ і представники бізнес-підрозділів. Це забезпечує врахування усіх бізнес-вимог і специфіки діяльності.

- Аналіз вимог і нормативної бази

  Вивчаються законодавчі акти, стандарти і галузеві регламенти, які застосовуються до підприємства, наприклад, GDPR, ISO/IEC 27001, PCI DSS.
- Визначення цілей і обсягу політик

  Формулюються конкретні цілі безпеки, які мають бути досягнуті, та охоплюються всі критичні області.
- Написання і узгодження тексту

  Документ створюється у зрозумілій формі, проходить обговорення і погодження між зацікавленими сторонами.
- Впровадження і комунікація

  Політики розповсюджуються серед співробітників, проводяться навчання і роз’яснювальні заходи.
- Моніторинг і оновлення

  Політики регулярно переглядаються і оновлюються з урахуванням змін у бізнесі, технологіях і законодавстві.

Важливість адаптації політик до специфіки підприємства

Політики безпеки мають бути адаптовані під конкретний бізнес-контекст, розмір підприємства, галузь діяльності, використовувані технології і рівень загроз. У малих компаніях вони можуть бути простішими, у великих — деталізованими та багаторівневими.

Вплив політик безпеки на інші компоненти системи захисту

Чітко сформовані політики безпеки створюють основу для:

- налаштування технологічних засобів контролю (DLP, IAM, SIEM);
- розробки процедур аудиту і контролю;
- планування навчання і підвищення обізнаності;
- формування культури безпеки в організації.

Таким чином, формування політик безпеки є одним із ключових кроків у створенні ефективної системи захисту від витоку даних. Вони задають правила гри, які повинні дотримуватися всі учасники інформаційних процесів, і забезпечують єдину рамку для технічних і організаційних заходів.

Важливо також зазначити, що процес формування політик безпеки має враховувати особливості корпоративної культури та рівень технічної грамотності персоналу. Політики повинні бути написані зрозумілою мовою, містити конкретні приклади дозволених і заборонених дій, щоб мінімізувати ризик їх неправильного тлумачення та дотримання.

Крім того, при розробці політик доцільно застосовувати підхід ризик-орієнтованого управління — тобто зосереджувати увагу на найбільш критичних для підприємства даних і процесах. Це дозволяє ефективніше використовувати ресурси і забезпечувати належний рівень захисту без перевантаження системи зайвими правилами.

Не менш важливим є механізм регулярного перегляду та оновлення політик. Світ інформаційних технологій та загроз постійно змінюється, тому політики мають адаптуватися до нових викликів, технологій і нормативних вимог. Впровадження процедури контролю версій документів і затвердження змін підвищує прозорість і відповідальність у цьому процесі.

Також слід забезпечити широку комунікацію та ознайомлення з політиками не лише всередині компанії, а й із зовнішніми партнерами, підрядниками і контрагентами, якщо їх діяльність передбачає обробку чи доступ до конфіденційної інформації підприємства.

Особливу увагу потрібно приділяти інтеграції політик безпеки з іншими корпоративними політиками та процедурами, такими як політика управління ризиками, політика інформаційної безпеки, політика управління інцидентами. Це забезпечує цілісність і взаємозв’язок усіх аспектів захисту інформації.

3.2 Модель реалізації контролю даних

Контроль даних є одним із ключових напрямків у системі захисту інформації на підприємстві, спрямованим на запобігання несанкціонованому доступу, витоку, втраті або пошкодженню критичних даних. Реалізація ефективного контролю даних потребує побудови цілісної моделі, яка враховує специфіку інформаційних потоків, організаційну структуру, а також сучасні технологічні можливості.

Основні принципи моделі контролю даних

Модель контролю даних базується на декількох фундаментальних принципах:

- Повний життєвий цикл даних. Контроль має охоплювати всі етапи роботи з даними: їх створення, обробку, зберігання, передачу і знищення. Цей підхід гарантує, що інформація захищена незалежно від способу і місця використання.
- Розмежування доступу і прав. Відповідно до принципу найменших привілеїв, користувачі і системи отримують доступ лише до тієї інформації, яка необхідна для виконання їхніх завдань. Це мінімізує ризики витоків через надмірні права.
- Ідентифікація і аутентифікація. Забезпечення надійного підтвердження особи користувача або системи перед наданням доступу до даних, з використанням багатофакторної аутентифікації, цифрових сертифікатів або біометричних методів.
- Моніторинг і аудит. Постійне відстеження доступу і операцій з даними, а також ведення журналів для подальшого аналізу інцидентів і забезпечення звітності.
- Автоматизація контролю. Використання спеціалізованих систем (DLP, SIEM, IAM), які автоматично виявляють і блокують потенційно небезпечні операції, знижуючи залежність від ручного контролю.

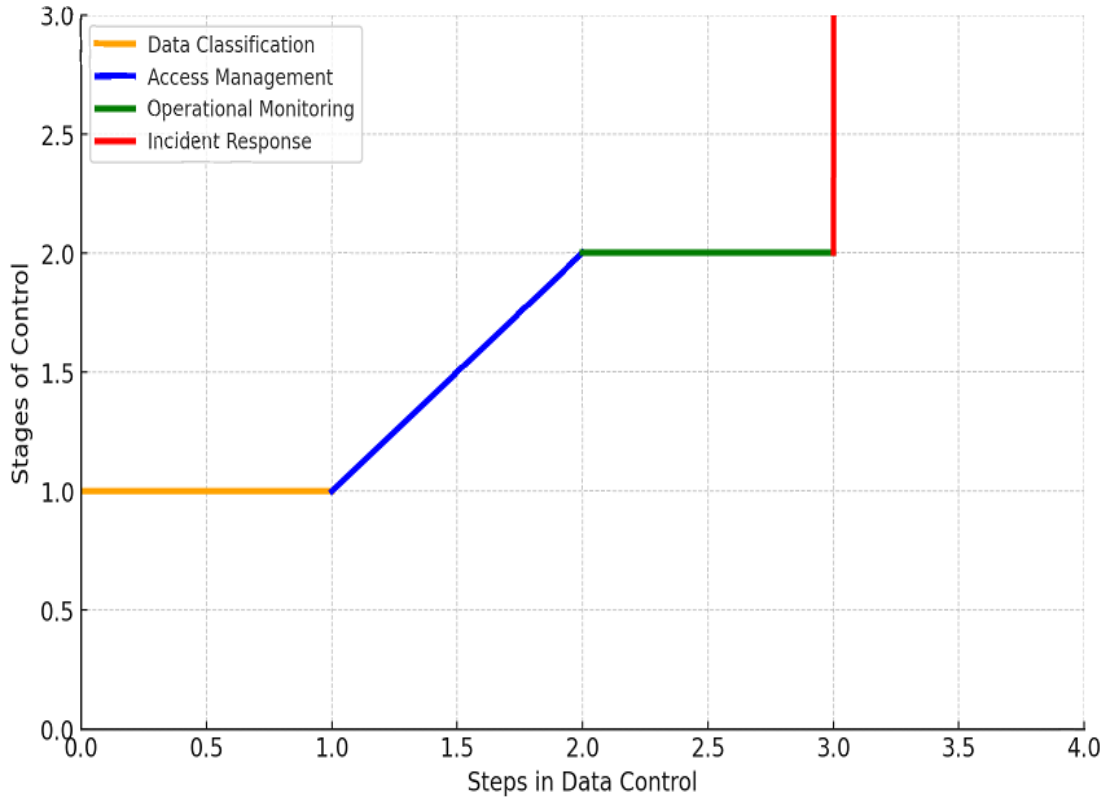

Рис3.2 Схема контролю даних, що включає класифікацію, управління доступом, моніторинг операцій, реагування на інциденти та аудит

Архітектурні компоненти моделі контролю даних

Реалізація контролю даних у підприємстві передбачає взаємодію кількох рівнів і компонентів:

1. Рівень класифікації інформації.

   На цьому рівні відбувається визначення категорій даних за рівнем конфіденційності і важливості. Класифікація є базою для встановлення відповідних політик доступу і контролю.

2. Рівень управління доступом.

   Сюди входить ідентифікація користувачів, аутентифікація, авторизація та призначення ролей. Використовуються механізми RBAC, ABAC або гібридні моделі.

3. Рівень контролю дій з даними.

   Включає моніторинг операцій користувачів з інформацією — копіювання, редагування, пересилання, друк. Для цього застосовуються агенти на кінцевих точках, мережеві сенсори, аналіз вмісту і поведінки.

4. Рівень реагування і протидії.

   Автоматичне блокування або попередження про потенційний витік, ініціація процесів реагування, інформування відповідальних осіб.

5. Рівень аудиту і звітності.

   Збереження логів і формування аналітичних звітів, що використовуються для аналізу інцидентів, аудиту і покращення політик.

Функціональні можливості моделі контролю

- Динамічний контроль доступу.

  Зміна прав доступу в залежності від контексту: місцезнаходження користувача, часу, пристрою, поточної загрози.

- Контроль потоків інформації.

  Відстеження руху даних між системами, користувачами, зовнішніми каналами (електронна пошта, хмарні сервіси) з метою виявлення несанкціонованих передач.

- Захист від витоку через фізичні носії.

  Обмеження можливості копіювання на USB, CD, зовнішні диски; шифрування даних на носіях.

- Інтеграція з системами управління інцидентами.

  Швидке реагування на інциденти витоку за допомогою автоматизованих механізмів і участі експертів.

Сценарії впровадження моделі

- Корпоративна мережа.

  Реалізація комплексного контролю за інформаційними потоками всередині організації і між віддаленими офісами.

- Віддалені користувачі і мобільні пристрої.

  Забезпечення захисту даних при роботі поза межами корпоративної мережі із застосуванням VPN, DLP-агентів і мобільного управління.

- Хмарні сервіси і SaaS.

  Контроль доступу та передачі даних у хмарі через CASB (Cloud Access Security Broker) і інтеграцію з DLP.

Вплив на безпеку підприємства

Правильно побудована модель реалізації контролю даних дозволяє значно знизити ризики втрати, крадіжки або компрометації інформації, забезпечити відповідність нормативам, підвищити довіру клієнтів і партнерів, а також захистити репутацію компанії.

3.3 Рекомендації з впровадження та аудиту системи захисту

Впровадження та подальший аудит системи захисту інформації — це складний та багатоетапний процес, що вимагає не лише технічної експертизи, а й стратегічного планування, міжвідомчої координації та постійного удосконалення. Правильно організовані заходи впровадження і регулярний аудит забезпечують не лише захист інформаційних активів підприємства, а й допомагають підтримувати їх у відповідності з нормативними та законодавчими вимогами.

Основні етапи впровадження системи захисту

1. Оцінка поточного стану інформаційної безпеки

   Перед початком впровадження необхідно здійснити детальний аудит існуючих процесів, систем, політик і технологій. Це дозволяє виявити слабкі місця, потенційні ризики і пріоритетні області для вдосконалення.

2. Визначення цілей і вимог до системи захисту

   Виходячи зі специфіки підприємства, сфери діяльності, типів оброблюваної інформації та законодавчих вимог, формуються чіткі цілі впровадження, які мають бути досягнуті системою безпеки.

3. Розробка або адаптація політик і процедур

   На основі аналізу і цілей створюються або оновлюються політики безпеки, що регламентують роботу з інформацією, права доступу, обробку інцидентів тощо.

4. Вибір і впровадження технологічних рішень

   Підбираються програмні і апаратні засоби відповідно до бізнес-вимог: DLP-системи, IAM, SIEM, системи шифрування, антивірусні засоби та інше. Важливо забезпечити їх інтеграцію в існуючу IT-інфраструктуру.

5. Навчання і підвищення обізнаності персоналу

Організовуються регулярні тренінги і навчальні сесії для співробітників, що допомагають формувати культуру безпеки і знижують ризики, пов’язані з людським фактором.

6. Моніторинг, аудит і оцінка ефективності

   Після впровадження системи здійснюється постійний моніторинг подій безпеки, аналіз інцидентів, а також проведення внутрішніх і зовнішніх аудитів для оцінки відповідності політикам і стандартам.

Рекомендації щодо проведення аудиту системи захисту

- Регулярність і системність.

  Аудити мають проводитися регулярно (щонайменше раз на рік) і охоплювати всі ключові компоненти системи безпеки — технічні засоби, політики, процедури, персонал.

- Комплексність підходу.

  Аудит має включати оцінку технічного стану (налаштування систем, оновлення), дотримання процедур, аналіз журналів подій, ефективність навчання і культуру безпеки.

- Залучення незалежних експертів.

  Для об’єктивної оцінки рекомендується залучати сторонніх фахівців, які мають досвід у проведенні подібних перевірок і можуть надати незалежний звіт.

- Оцінка ризиків і вразливостей.

  В рамках аудиту необхідно проводити пентести, аналіз вразливостей, тестування реагування на інциденти.

- Документування і звітність.

  Результати аудиту мають бути задокументовані, містити рекомендації щодо усунення виявлених недоліків і заходи для вдосконалення системи.

- Моніторинг виконання рекомендацій.

  Важливо контролювати впровадження запропонованих заходів і оцінювати їх ефективність.

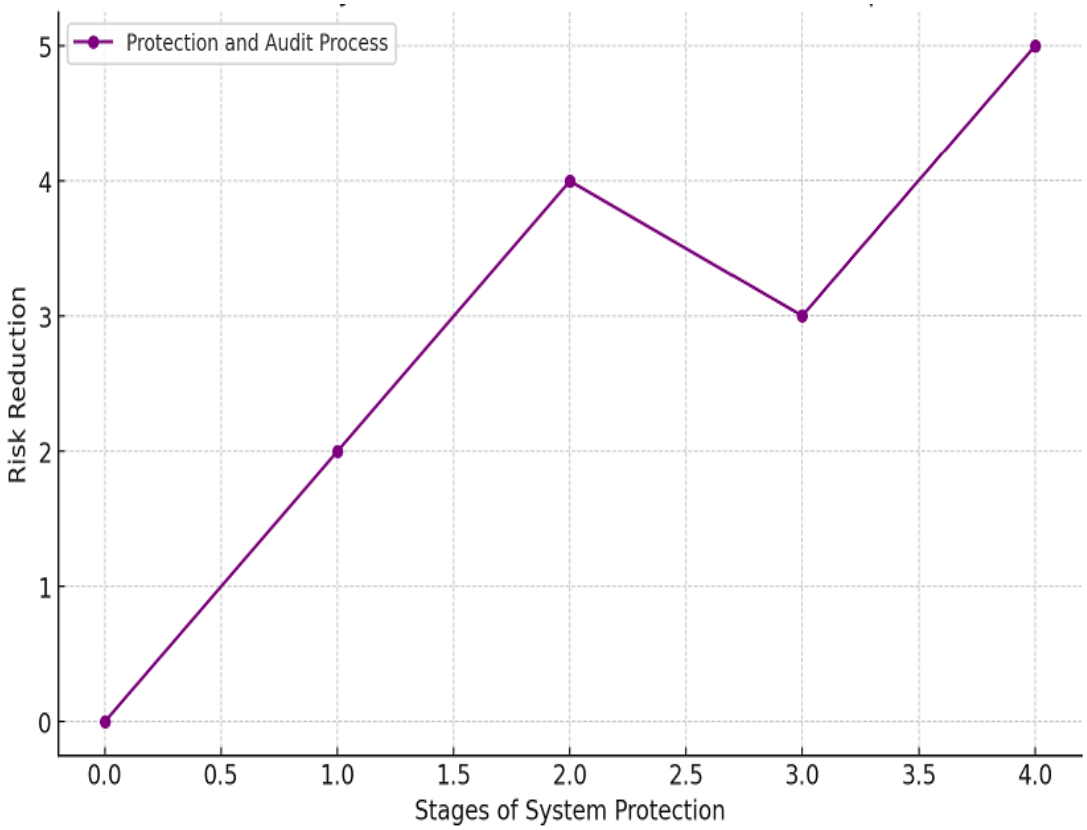

Рис3.3 Етапи впровадження системи захисту і аудитів від оцінки ризиків до навчання персоналу і моніторингу ефективності

Впровадження системи управління безпекою інформації (ISMS)

Однією з кращих практик є впровадження ISMS відповідно до стандарту ISO/IEC 27001. Така система дозволяє систематизувати процеси управління безпекою, забезпечити їх документованість, а також інтегрувати аудит та постійне удосконалення в корпоративні процеси.

Ключові фактори успішного впровадження і аудиту

- Підтримка керівництва — без активного залучення топ-менеджменту важко забезпечити необхідні ресурси і дотримання політик.
- Чітке планування — визначення етапів, ресурсів, відповідальних осіб.
- Залучення всіх підрозділів — безпека — це не лише задача IT, а й усієї організації.
- Гнучкість і адаптивність — система має відповідати змінам бізнесу, технологій і загроз.
- Комунікація і навчання — регулярне інформування і підвищення кваліфікації персоналу.

Таким чином, системний підхід до впровадження та аудиту системи захисту інформації дозволяє підвищити рівень безпеки, мінімізувати ризики витоку даних і забезпечити стійкість підприємства до кіберзагроз.

Додатково варто звернути увагу на впровадження системи безперервного контролю і вдосконалення (Continuous Monitoring and Improvement). Вона передбачає автоматизований збір і аналіз даних про безпекові події, швидке реагування на нові загрози та адаптацію політик і технологічних рішень відповідно до актуального стану кіберсередовища. Це дозволяє підприємству зберігати високий рівень захисту в умовах постійної еволюції методів атак.

Особливе значення має застосування методологій управління ризиками, які інтегрують впровадження і аудит системи захисту у загальну систему управління підприємством. Це забезпечує пріоритизацію заходів, раціональне розподілення ресурсів і максимальну ефективність з урахуванням бізнес-цілей.

Не менш важливим є впровадження механізмів внутрішнього звітування про інциденти та створення безпечних каналів комунікації для співробітників, які можуть повідомляти про підозрілі події без страху репресій. Такий підхід сприяє ранньому виявленню витоків і мінімізує можливі збитки.

Також рекомендується проводити періодичні навчальні тренінги та практичні вправи (tabletop exercises), що моделюють інциденти безпеки. Вони допомагають відпрацювати взаємодію між підрозділами, перевірити готовність і швидкість реагування, а також виявити можливі прогалини в процедурах.

Впровадження системи захисту і її аудит повинні базуватися на чітких метриках і показниках ефективності (KPIs), які дозволяють вимірювати успіхи і проблемні зони. До таких показників належать, наприклад, час виявлення інциденту, кількість виявлених спроб витоку, рівень відповідності політикам тощо.

Нарешті, слід звернути увагу на важливість інтеграції систем захисту з бізнес-процесами підприємства. Безпека має бути невід’ємною частиною повсякденної діяльності, а не окремою технічною задачею, що дозволить уникнути конфліктів інтересів і забезпечить гармонійну роботу організації.

Висновки

У роботі проведено комплексне дослідження проблеми захисту від витоку даних на підприємстві, визначено основні загрози, методи та засоби запобігання втраті конфіденційної інформації. Визначено ключову роль систем захисту у забезпеченні безперервності бізнес-процесів та збереженні репутації організації.

Проаналізовано сучасні технологічні рішення, зокрема системи Data Loss Prevention (DLP), моніторинг поведінки користувачів (UEBA), управління доступом (IAM) та системи збору і аналізу подій безпеки (SIEM). Окрему увагу приділено організаційним заходам контролю — розробці політик безпеки, навчанні персоналу, внутрішньому аудиту та формуванню культури інформаційної безпеки.

Визначено, що ефективний захист від витоку даних можливий лише за умови комплексного підходу, що поєднує технічні, організаційні і процесні заходи. Розроблено модель реалізації контролю даних, яка охоплює всі етапи їх життєвого циклу, забезпечує сегментацію доступу і автоматизований моніторинг дій.

Сформульовано рекомендації щодо впровадження систем захисту, які включають оцінку ризиків, розробку і затвердження політик, вибір і інтеграцію технічних засобів, а також організацію постійного аудиту і навчання співробітників. Наголошено на необхідності підтримки керівництва та формування довготривалої культури безпеки в організації.

Запропоновані заходи дозволяють суттєво підвищити рівень інформаційної безпеки, знизити ризики витоку, несанкціонованого доступу і втрати даних, а також відповідати вимогам сучасного законодавства та міжнародних стандартів. Впровадження системи захисту від витоку даних сприяє створенню надійного цифрового середовища, що підтримує довіру клієнтів, партнерів і співробітників.

Таким чином, правильно організована система захисту від витоку даних є необхідним стратегічним ресурсом для сучасних підприємств, особливо в умовах зростаючих кіберзагроз і активної цифрової трансформації бізнес-процесів.

ПЕРЕЛІК ПОСИЛАНЬ

1. ISO — International Organization for Standardization
https://www.iso.org/isoiec-27001-information-security.html

2. NIST — National Institute of Standards and Technology
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

3. European Union GDPR Portal
https://gdpr.eu/

4. PCI Security Standards Council
https://www.pcisecuritystandards.org/

5. IBM Security — Cost of a Data Breach Report
https://www.ibm.com/security/data-breach

6. Verizon Data Breach Investigations Report (DBIR)
https://www.verizon.com/business/resources/reports/dbir/

7. Symantec (Broadcom) Data Loss Prevention
https://www.broadcom.com/products/cyber-security/information-protection/data-loss-prevention

8. Microsoft Security Documentation
https://learn.microsoft.com/en-us/security/

9. Forcepoint DLP Solutions
https://www.forcepoint.com/product/data-loss-prevention-dlp

10. OWASP — Open Web Application Security Project
https://owasp.org/

11. ENISA — European Union Agency for Cybersecurity
https://www.enisa.europa.eu/publications

12. Cybersecurity Insiders — Endpoint Security Report 2022
https://20645266.fs1.hubspotusercontent-na1.net/hubfs/20645266/CSI-2022-Endpoint-Security-Report-Adaptiva-Final-03282022%20(1).pdf

13. BlackBerry — Endpoint Detection and Response (EDR)

https://www.blackberry.com/us/en/solutions/endpoint-security/endpoint-detection-and-response#how-it-works

14. Gartner — Endpoint Detection and Response Solutions https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions

15. Microsoft Defender for Endpoint series — What is Defender for Endpoint? https://www.microsoft.com/en-us/security/blog/2023/03/02/microsoft-is-named-a-leader-in-the-2022-gartner-magic-quadrant-for-endpoint-protection-platforms/

16. Microsoft Defender for Endpoint architecture requirements and key concepts https://learn.microsoft.com/en-us/microsoft-365/security/defender/eval-defender-endpoint-architecture?view=o365-worldwide

17. VMware Carbon Black — Endpoint Detection and Response (EDR) Datasheet https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmwcb-datasheet-edr.pdf

18. VMware Carbon Black Workload Architecture https://carbonblack.vmware.com/resource/carbon-black-workload-architecture#section1

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)