МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “МЕТОДИ ПРОТИДІЇ ВИТОКУ ІНФОРМАЦІЇ ЧЕРЕЗ ВНУТРІШНІ ЗАГРОЗИ: ОРГАНІЗАЦІЙНІ ТА ТЕХНІЧНІ АСПЕКТИ”

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Управління інформаційною та кібернетичною безпекою

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

_____ Євген ГОРБАЧ

(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ-61
ЄВГЕН ГОРБАЧ
Керівник: д.т.н., професор Віталій САВЧЕНКО

Рецензент:

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра Управління кібербезпекою та захистом інформації
Ступінь вищої освіти магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедрою УКБЗІ
_____ Світлана ЛЕГОМІНОВА
"____" _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Студенту Горбачу Євгену Сергійовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: "Методи протидії витоку інформації через внутрішні загрози: організаційні та технічні аспекти."

керівник кваліфікаційної роботи Віталій САВЧЕНКО, д.т.н., професор
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від "30" жовтня 2025 р. № 467.

2. Строк подання кваліфікаційної роботи "22" грудня 2025 р.
3. Вихідні дані до кваліфікаційної роботи:.
4. Перелік питань, які потрібно розробити:
   1. Теоретичні основи внутрішніх загроз та витоку інформації
   2. Аналіз внутрішніх загроз та існуючих методів протидії витоку інформації
   3. Розроблення комплексної моделі протидії витоку інформації через внутрішні загрози та оцінка її ефективності
5. Перелік ілюстративного матеріалу: *презентація*
6. Дата видачі завдання "02" жовтня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2025	
2.	Збір та аналіз літератури.	23.10.2025	
3.	Теоретичні основи внутрішніх загроз та витоку інформації	27.10.2025	
4.	Аналіз внутрішніх загроз та існуючих методів протидії витоку інформації	10.11.2025	
5.	Розроблення комплексної моделі протидії витоку інформації через внутрішні загрози та оцінка її ефективності	15.11.2025	
6.	Формулювання висновків за результатами дослідження.	22.11.2025	
7.	Оформлення роботи.	04.12.2025	
8.	Оформлення презентації.	14.12.2025	
9.	Отримання рецензії на роботу.	18.12.2025	
10.	Захист в ЕК.	21.01.2026	

Здобувач вищої освіти _____ Євген ГОРБАЧ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Віталій САВЧЕНКО
(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 магістра

Направляється здобувач Горбач Є.С. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека та захист інформації
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Методи протидії витоку інформації через внутрішні загрози: організаційні та технічні аспекти."
Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Завідувач кафедрою
Управління кібербезпекою та захистом
інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач ГОРБАЧ Євген у кваліфікаційній роботі проаналізував актуальні проблеми протидії витоку інформації через внутрішні загрози та містить обґрунтований аналіз організаційних і технічних заходів захисту. **ГОРБАЧА Євгена** показав високу теоретичну і практичну підготовку, володіння науково-дослідницькими методами, вміння самостійно знаходити шляхи вирішення проблеми дослідження. Результати дослідження апробовані на конференції "Стратегії кіберстійкості: управління ризиками та безперервність бізнесу" 28 лютого 2024 року.

Все це дозволяє оцінити кваліфікаційну роботу здобувача ГОРБАЧА Євгена на оцінку "добре" та присвоїти йому кваліфікацію "Магістр з кібербезпеки та захисту інформації за освітньо-професійною програмою Управління інформаційною та кібернетичною безпекою".

Керівник кваліфікаційної роботи _____ Віталій САВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Горбач Є.С. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою
Управління кібербезпекою та захистом
інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

здобувачу вищої освіти Горбача Євгена Сергійовича
на тему " Методи протидії витоку інформації через внутрішні загрози: організаційні та технічні аспекти "

Актуальність Витік інформації через внутрішні загрози залишається однією з найскладніших проблем інформаційної безпеки, оскільки пов'язаний з людським фактором та легітимним доступом персоналу до інформаційних ресурсів. В умовах цифровізації та зростання кіберризиків для України особливо важливим є впровадження ефективних організаційних і технічних заходів протидії інсайдерським загрозам. Тому дослідження комплексних підходів до запобігання витоку інформації є актуальним і практично значущим.

Позитивні сторони

1. У роботі досліджено засади витоку інформації через внутрішні загрози. Для України проблема протидії внутрішнім загрозам є особливо важливою з огляду на воєнний стан, зростання кіберзагроз, захист державних інформаційних ресурсів та персональних даних громадян. Національне законодавство у сфері кібербезпеки та захисту інформації, а також вимоги міжнародних стандартів (ISO/IEC, NIST) визначають необхідність комплексного підходу до управління інсайдерськими ризиками, що поєднує організаційні, технічні та кадрові заходи.
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків. Автор опрацював значну джерельну базу: близько 31 публікацій та електронних джерел, в тому числі англомовних.
3. За результатами дослідження запропоновано рекомендації щодо забезпечення інформаційної безпеки підприємства в умовах внутрішніх загроз.

Недоліки

1. Доцільно було б приділити більше уваги вивченню і класифікації методів протидії внутрішнім загрозам

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує позитивної оцінки, а здобувач Горбач Євген Сергійович заслуговує присвоєння кваліфікації "Магістр кібербезпеки за освітньо-професійною програмою "Управління інформаційною та кібернетичною безпекою".

Рецензент: _____ _____

(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 81 стор., 3 рис., 12 табл., 31 джерел.

Метою роботи є розробка комплексної моделі протидії витоку інформації від внутрішніх загроз та оцінка її ефективності.

Об'єктом дослідження є забезпечення процесу захисту інформації на підприємстві. Предмет дослідження – методи, моделі та засоби протидії витоку інформації через інсайдерські загрози, включно з поведінковими аспектами персоналу підприємства.

Методи дослідження. Для вирішення завдань та процесів поширення аналіз видів і джерел внутрішніх загроз, дослідження сучасних організаційних і технічних методів протидії, вивчення впливу людського фактора на ризики витоку інформації, формування моделі інтеграції заходів захисту та експериментальна перевірка ефективності запропонованого підходу.

Як результат у роботі застосовано методи аналізу і синтезу, ризик-орієнтовані підходи, статистичні методи, елементи поведінкового моделювання, аналіз людського фактора, а також експериментальні методики оцінювання засобів захисту. Інформаційною базою слугували міжнародні стандарти (ISO/IEC 27001, 27035, NIST SP 800-61, NIST SP 800-53), рекомендації CERT Insider Threat Center та ENISA, наукові публікації, аналітичні звіти та емпіричні дослідження ролі людського фактора в інцидентах інформаційної безпеки.

Галузь застосування. Результаті дослідження розроблено комплексну модель протидії витоку інформації, що поєднує організаційні заходи, технічні засоби (DLP, UEBA, SIEM), компоненти контролю привілеїв та поведінковий аналіз персоналу. Реалізовано експериментальну перевірку моделі, наведено результати її роботи, оцінено ефективність та визначено обмеження.

КЛЮЧОВІ СЛОВА : ВНУТРІШНІ ЗАГРОЗИ, ЛЮДСЬКИЙ ФАКТОР, ІНСАЙДЕР, ВИТІК ІНФОРМАЦІЇ, ІНФОРМАЦІЙНА БЕЗПЕКА, DLP, UEBA, SIEM, ПОВЕДІНКОВИЙ АНАЛІЗ, ОРГАНІЗАЦІЙНІ ЗАХОДИ.

ЗМІСТ

ВСТУП

Стрімкий розвиток цифрових технологій та зростаюча залежність організацій від інформаційних ресурсів посилюють потребу в ефективному захисті даних. У сучасних умовах значна частина інцидентів інформаційної безпеки пов’язана не з зовнішніми атаками, а з діяльністю працівників, які мають легітимний доступ до критично важливих інформаційних активів. Внутрішні загрози, що виникають як через умисні дії інсайдерів, так і через помилки персоналу чи нехтування політиками безпеки, стають одним із найскладніших викликів для організацій незалежно від їхнього масштабу та сфери діяльності. [23]

За результатами аналітичних досліджень міжнародних центрів кібербезпеки, частка інцидентів, спричинених внутрішніми порушниками, стабільно зростає, а людський фактор є домінуючим елементом ризику. Це зумовлює необхідність комплексного підходу до протидії витоку інформації, що включає поєднання організаційних, технічних, поведінкових та управлінських заходів. Водночас практичний досвід організацій свідчить, що наявні засоби захисту часто мають обмеження: вони або не виявляють інциденти на ранніх етапах, або генерують значну кількість хибних спрацювань, або не враховують психологічні та мотиваційні аспекти поведінки працівників. Отже, проблема ефективної протидії внутрішнім загрозам потребує подальшого аналізу та системного удосконалення. [1,17]

Для досягнення поставленої мети сформульовано такі завдання дослідження:

1. Проаналізувати сутність і класифікацію внутрішніх загроз, а також причини їх виникнення.
2. Дослідити роль людського фактора у формуванні ризиків витоку інформації.
3. Проаналізувати нормативно-правову базу, міжнародні стандарти та наукові підходи щодо протидії інсайдерським загрозам. [23]

4. Оцінити сучасні організаційні та технічні методи запобігання витоку інформації, визначити їхні переваги та обмеження.
5. Розробити комплексну модель протидії внутрішнім загрозам на основі інтеграції технічних і організаційних заходів.
6. Провести експериментальну оцінку запропонованого підходу та визначити його ефективність.

У роботі використано методи аналізу, синтезу, порівняння, ризик-орієнтовані підходи, елементи поведінкового моделювання, статистичні методи, а також практичні методики налаштування та оцінки систем захисту інформації.

РОЗДІЛ 1

ТЕОРЕТИЧНІ ОСНОВИ ВНУТРІШНІХ ЗАГРОЗ ТА ВИТОКУ ІНФОРМАЦІЇ

1.1 Поняття внутрішньої загрози та її місце в системі інформаційної безпеки

У сучасних системах інформаційної безпеки внутрішні загрози розглядаються як один із найбільш критичних класів ризиків. Особливість таких загроз полягає в тому, що їхнім джерелом є особи зі штатним, легітимним доступом, що суттєво ускладнює їх виявлення традиційними засобами кіберзахисту.

Внутрішня загроза (insider threat) — це ризик, який виникає від осіб, які мають законний доступ до ресурсів організації (інформації, систем, обладнання), і які можуть зловживати цим доступом або ненавмисно спричинити шкоду. За визначенням Cybersecurity & Infrastructure Security Agency (CISA), інсайдер — це особа з авторизованим доступом або знанням ресурсів організації, а загроза — це потенціал такої особи використовувати свій доступ (навмисно або ненавмисно) для нанесення шкоди організації: її місії, ресурсам, інформації, персоналу, обладнанню, мережам або системам. [23]

За своїм походженням загроза стає ризиком тільки тоді, коли існує можливість неналежного використання ресурсів організації (фізичних чи віртуальних)

Згідно з CERT Insider Threat Center (SEI, Carnegie Mellon University), інсайдер — це «поточний або колишній співробітник, підрядник або партнер, який має санкціонований доступ до систем або даних і умисно чи ненавмисно використовує цей доступ для спричинення шкоди організації». [14, 23]

Інсайдерами можуть бути поточні або колишні працівники, підрядники, постачальники, треті сторони, які колись отримали доступ до внутрішніх систем. Таб.1 [23]

Типи інсайдерських загроз можна поділити на: [23]

1. Навмисні (зловмисні)
   Особи, які з умислом шкодять організації — крадуть дані, займаються саботажем, шпигують.
2. Ненавмисні(випадкові)
   Працівники, які через необережність або неуважність порушують політики безпеки, роблять помилки, що призводять до витоку інформації або інших інцидентів.
3. Колюзивні загрози
   Ситуації, коли внутрішні співробітники спільно з зовнішніми акторами виконують зловмисні дії (наприклад, співпраця з кіберзлочинцями).
4. Треті сторони / підрядники
   Люди, які не є штатними працівниками, але мають доступ до ресурсів організації — через контракти, тимчасову роботу тощо.

Таблиця 1 Типи інсайдерів та їх характеристики

Тип інсайдера	**Опис**	**Мотиви**	**Приклади шкідливих дій**	**Рівень ризику**
Зловмисний (malicious)	Співробітник або підрядник, який умисно шкодить організації	Помста, фінансова вигода, ідеологія	Крадіжка даних, продаж інформації, саботаж, передача	**Дуже високий**

Тип інсайдера	Опис	Мотиви	Приклади шкідливих дій	Рівень ризику
			конкурентам	
Недбалий (negligent)	Співробітник, який ненавмисно порушує правила або робить помилки	Неуважність, низька обізнаність, перевтома	Відправка файлів не тим адресатам, завантаження заражених файлів, проігнорований фішинг	**Високий**
Скомпрометований (compromised)	Облікові дані працівника захоплені зовнішніми зловмисниками	Соціальна інженерія, фішинг, шкідливе ПЗ	Використання вкраденого акаунта для доступу до систем	**Дуже високий**
Підрядник / третя сторона	Особа, яка не є співробітником, але має доступ до ресурсів організації	Фінансова вигода, недотримання політик безпеки	Витік даних через недбалих підрядників,розголошення комерційної інформації	**Середній–високий**

Одна з основних проблем — те, що інсайдер має правомірний доступ, тому традиційні засоби безпеки (наприклад, мережевий захист, фаєрволи) можуть не зреагувати на його дії як на підозрілі. [23]

Сучасні дослідження підкреслюють, що для виявлення інсайдерів ефективні підходи поведінкового аналізу (User and Entity Behavior Analytics,

UEBA) або системи на базі аномалій, які спостерігають нетипову поведінку в системах. [23]

Також, деякі наукові роботи пропонують використання нетрадиційних методів — наприклад, аналіз стресу через характеристики натискання клавіш (keystroke dynamics) при підозрілих діях.

Основні характеристики внутрішньої загрози:

- Доступ: Інсайдер вже має авторизований доступ, тому йому не потрібно “ламати” зовнішній захист (наприклад, фаєрвол або периметр), що ускладнює виявлення. [23]
- Знання організації: Інсайдер добре знає внутрішню структуру, процеси, системи безпеки, політики — може ефективніше уникати засобів виявлення. [23]
- Мотиви: Мотиви можуть бути різні — особиста вигода, помста, незадоволення, ідеологія, або просто небезпечна неуважність.
- Прояв: Внутрішні загрози можуть проявлятися через крадіжку інтелектуальної власності, витік комерційних або конфіденційних даних, саботаж, фізичні дії, шахрайство тощо.

Розуміння того, що таке внутрішня загроза і які її основні характеристики, є базовим для розробки контрзаходів — як організаційних, так і технічних.

- На організаційному рівні це означає: політики доступу, чітке розмежування прав, регулярні аудити, навчання співробітників, культура довіри, але й пильності.
- На технічному рівні — впровадження моніторингових систем, систем аналізу поведінки, аудиту дій користувачів, внутрішнього IDS / DLP (Data Loss Prevention), UEBA тощо. [26]

Причини виникнення внутрішньої загрози:

- Людський чинник. Найпоширеніша причина — співробітники, які роблять помилки, нехтують політиками безпеки, натискають на фішингові посилання або неправильно обробляють конфіденційну інформацію.
- Мотивація навмисного порушення: фінансова винагорода, відчуття несправедливості, бажання “вчинити помсту”, або навіть ідеологічні причини.
- Недосконалі організаційні процеси: слабкі політики доступу, недостатній контроль за правами, відсутність чітких ролей та відповідальності, поганий нагляд.
- Технічні вразливості: системи, які не фіксують дії користувачів, не мають механізмів виявлення аномальної поведінки, або недостатнього аудиту. Навіть якщо користувач має доступ, відсутність моніторингу може дозволити зловживання.
- Зовнішній тиск або співпраця: інсайдер може співпрацювати з зовнішніми акторами, бути під впливом або отримувати стимул від третіх сторін. [23]

NIST у документі NIST SP 800-53 Rev.5 у контролі PM-12 “Insider Threat Program” наголошує, що внутрішня загроза є комбінацією поведінки, доступів і спадкових ризиків, яку потрібно керувати окремо від зовнішніх атак [NIST SP 800-53]. ISO/IEC 27000:2022 визначає внутрішню загрозу як дії авторизованого суб'єкта, що порушують правила використання інформації або політики безпеки. [7] [9]

Таким чином, внутрішня загроза = легітимний доступ + неправомірні дії / помилки - зловживання.

У класичній моделі інформаційної безпеки (конфіденційність, цілісність, доступність) внутрішні загрози особливо небезпечні. Тому що для інсайдере це не проблемою (таблиця 2) [23]

Таблиця 2 Внутрішня загроза інсайдера

Критерій	Чому інсайдер важкий для виявлення
Конфіденційність	Має доступ до даних за посадою, тому не потребує зовнішнього зламу
Цілісність	Може вносити зміни в системи адміністративними засобами
Доступність	Може здійснювати саботаж або відключати IT-системи
Обхід детекції	Використовує штатні механізми, що виглядають легітимними

Verizon DBIR (2023–2024) підтверджує, що 30–34% витоків даних спричинено внутрішніми порушниками або помилками персоналу. Зокрема 60% через поштову скриньку. Дослідження, яке охоплювало випадки, які сталися між 1 листопада 2023 року та 31 жовтня 2024 року, показало, що атаки BEC подвоїлися і становили понад 50% соціально-інженерних атак. Глобальне дослідження охопило випадки в регіонах Азії-Тихоокеанського регіону, Європи, Близького Сходу та Африки, Північної Америки та Латинської Америки.

Це зумовлює необхідність формувати спеціальні програми протидії внутрішнім загрозам — Insider Threat Program, які передбачені NIST PM-12, директивами DNI/NITTF і рекомендаціями CERT [9] [14]

Більшість міжнародних досліджень використовують трикомпонентну модель:

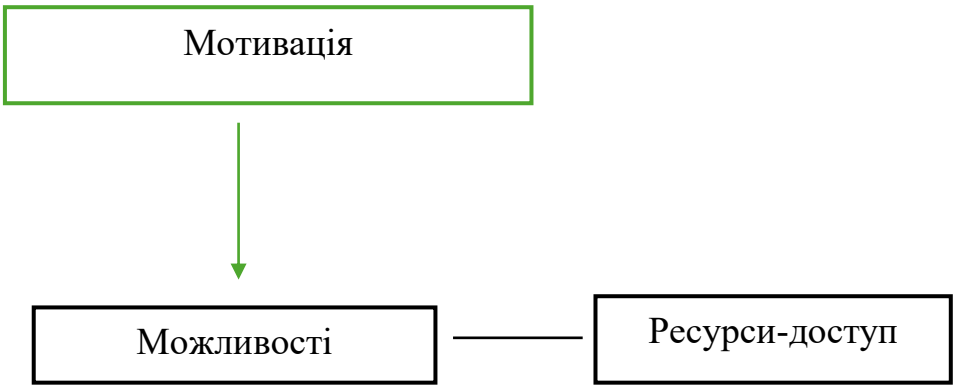

Рис.1 Системна модель внутрішньої загрози

- Мотивація – фінансові стимули, помста, ідеологія, примус, недбалість.
- Можливості – наявність привілеїв, технічна компетентність, знання систем.
- Ресурси – облікові записи, інструменти, фізичний доступ.

Ця модель узгоджується з Frameworks Insider Threat Program (NITTF, US DoD).

Внутрішня загроза (інсайдерська загроза) є складним багатоаспектним явищем, яке виникає внаслідок діяльності осіб, що мають легітимний доступ до інформаційних ресурсів організації. На відміну від зовнішніх кіберзагроз, інсайдери не потребують подолання периметрового захисту, що робить їх потенційно значно небезпечнішими та суттєво ускладнює процеси виявлення та нейтралізації таких порушень. Саме тому інсайдерські загрози визнаються одними з найменш контрольованих та найскладніших для попередження у сучасних системах кібербезпеки. [1, 23]

У межах проведеного дослідження встановлено, що внутрішні загрози можуть мати навмисний, ненавмисний, колюзивний характер або походити від третіх сторін (підрядників, партнерів), які мають розширений рівень доступу. Таке різноманіття форм зумовлює потребу використовувати диференційовані моделі оцінювання ризиків та розробляти інтегровані контрзаходи, які поєднують організаційні, технічні, поведінкові та соціальні компоненти.

Встановлено, що ключовим чинником виникнення внутрішніх загроз є людський фактор, який проявляється у вигляді неуважності, низького рівня обізнаності, нехтування політиками безпеки, фішингової вразливості та інших помилок персоналу. У той же час значну частку складають навмисні загрози, мотивовані фінансовими, ідеологічними або особистими мотивами, що підтверджує необхідність психологічного моніторингу, політик персонального контролю та ретельного управління доступами. [4, 17]

Аналіз джерел показав, що наслідки реалізації внутрішніх загроз можуть виражатися у витоку конфіденційної інформації, саботажі, модифікації критичних даних, порушенні роботи систем, фінансових втратах та суттєвих репутаційних збитках. В окремих випадках наслідки інсайдерських атак перевищують масштаби зовнішніх загроз, адже інсайдер володіє знаннями про внутрішні процеси, архітектуру систем, слабкі місця та особливості корпоративної культури. [23]

Результати аналізу дозволяють зробити висновок, що внутрішня загроза є фундаментальним елементом ризикового середовища будь-якої сучасної організації. Комплексне розуміння природи інсайдерських загроз, їх джерел, мотивацій, форм прояву та можливих наслідків є базовою передумовою для формування ефективної системи протидії витоку інформації на організаційному та технічному рівнях.

Відповідно, подальші розділи роботи мають бути спрямовані на розробку та обґрунтування інтегрованих підходів і моделей, що дозволять мінімізувати ризики інсайдерських дій та підвищити загальний рівень інформаційної безпеки підприємства. [23]

1.2 Причини та мотиваційні моделі інсайдерів

Внутрішні загрози інформаційній безпеці залишаються одним із найскладніших викликів для сучасних організацій. Особливість таких загроз полягає в тому, що їхнє джерело — це люди, які мають повністю легітимний доступ до інформаційних систем, технологічних ресурсів або конфіденційних даних. На відміну від зовнішніх хакерів, інсайдери вже перебувають «всередині» периметра безпеки, що значно ускладнює їх виявлення, профілювання та нейтралізацію. [23]

Для розробки ефективних контрзаходів критично важливо глибоко зрозуміти причини, які спонукають співробітників і підрядників до ненавмисних помилок чи навмисних шкідливих дій. Причини інсайдерської діяльності часто багатофакторні, поєднують емоційні, фінансові, організаційні та технічні елементи, що створює комплексний контекст прийняття рішень працівником. [23]

Причини інсайдерських загроз можна класифікувати на кілька груп: людські, організаційні, психологічні, соціальні та технічні. Кожна з них формує передумови, за яких співробітник може прийняти рішення про несанкціоновані дії або випадково допустити критичну помилку, що призводить до витоку даних. [23]

Основні причини інсайдерських загроз: [23]

1. Фінансові мотиви

Фінансовий тиск є однією з найпоширеніших причин інсайдерських інцидентів. Борги, сімейні труднощі, залежності, низький рівень доходу або можливість швидкої наживи роблять працівників більш вразливими до зовнішніх впливів або власного рішення викрасти конфіденційні дані. Інтелектуальна власність, персональна інформація клієнтів чи комерційні секрети можуть бути продані на чорному ринку або конкурентам. [4] [23]

2. Невдоволення або образа (Disgruntlement)

Емоційні фактори відіграють значну роль. Працівники, які почуваються недооціненими, ображеними або несправедливо покараними, можуть свідомо шкодити компанії. Причиною може бути відмова в підвищенні, конфлікти з керівництвом, незадоволення умовами праці чи відчуття несправедливості. Часто такі дії проявляються як саботаж, витік інформації або видалення даних перед звільненням.

3. Ідеологічні або моральні мотиви

Деякі інсайдери діють із переконання, що компанія поводиться неправильно з етичної, політичної чи соціальної точки зору. Їхні дії можуть нагадувати «викривачів» (whistleblowers), але методи, які вони використовують, можуть завдати значної шкоди. Такі інциденти часто пов’язані з витоками інформації у ЗМІ або відкритих джерелах.

4. Примус, шантаж або зовнішній вплив

Зовнішні актори можуть впливати на співробітників через шантаж, погрози або маніпуляції. Це можуть бути кримінальні угруповання, конкуренти або інші зацікавлені сторони. Примушений інсайдер є однією з найнебезпечніших категорій, оскільки поєднує внутрішній доступ із зовнішніми шкідливими інтересами. [23]

5. Можливість зловживання доступом

Навіть без чіткої мотивації на початку, зловживання може виникнути через наявність надмірних прав доступу або відсутність контролю, коли працівник «має змогу» непомітно діяти. Модель «доступ → можливість → дія» показує, що неконтрольований доступ стимулює інсайдерську активність незалежно від початкових намірів.

6. Психологічний стан та особистісні фактори

Стрес, професійне вигорання, конфлікти в колективі або особисті проблеми можуть створювати передумови до необачної або навмисної шкідливої поведінки. Деякі особистісні риси — імпульсивність, схильність до ризику або низький рівень емоційної стабільності — значно підвищують імовірність інцидентів.

7. Низький рівень обізнаності та людські помилки

Більшість інсайдерських інцидентів має ненавмисний характер і спричинена людськими помилками: фішингові атаки, неправильне поводження з документами, нехтування політиками безпеки, пересилання конфіденційних

файлів не тим адресатам. Людські фактори залишаються домінантною причиною інцидентів (від 60 до 80% залежно від дослідження). [23]

Таблиця 3 Основні групи причин інсайдерських загроз

Група причин	**Приклади**	**Характеристика впливу**
Фінансові	борги, низька зарплата, пропозиція винагороди	мотивують до продажу даних або шахрайства
Психологічні	стрес, конфлікти, емоційні потрясіння	можуть спричинити випадкові або навмисні дії
Ідеологічні	політичні, моральні переконання	співробітник діє як “викривач” або активіст
Соціальні	примус, шантаж, тиск третіх осіб	формують залежність співробітника від зовнішніх акторів
Організаційні	відсутність контролю, несправедливість, токсична культура	знижують лояльність, підвищують ризики
Технічні	надмірні права доступу, відсутність моніторингу	створюють можливість зловживань

Щоб глибше зрозуміти, як саме люди приходять до інсайдерських дій, корисно розглянути декілька мотиваційних моделей, які використовуються в дослідженнях: [23]

Модель стримування і запобігання (Deterrence & Prevention Model)

— Ця модель базується на теоріях запобігання злочинності: припинення небажаної поведінки відбувається через підвищення серйозності санкцій, підвищення вірогідності покарання, зменшення вигоди від протиправної дії.

— Організаційні заходи: політики безпеки, дисциплінарні санкції, чіткі правила, регулярні тренінги.

— Психологічний аспект: працівники можуть утримуватися від шкідливих дій, якщо вірять, що їхні дії будуть виявлені, і вони несе відповідальність.

Модель факторів людського чинника + мережі Байєса (IHFACS-BN)

— У роботі Zeng, Dian та Wei розглянуються людські фактори (human factors) та їх вплив на ризик інсайдерської загрози. Вони створили гібридну модель, яка поєднує аналіз людських чинників (невпевненість, стрес, приватне життя) з експертними оцінками через Байєсові мережі. [23]

— За допомогою цієї моделі можна виявити, які саме "людські фактори" — найбільший рушій ризику: наприклад, невідповідність між очікуваннями співробітника та реальністю, стресовий клімат, недостатнє задоволення від роботи.

Модель детермінації мотивацій (Drivers) інсайдерської загрози [23]

— У дослідженні Sedek, Omar та ін. ("Discovering the Impact: Exploring How Insider Threat Drivers Relate to Organizational Performance") вони визначили ключові драйвери інсайдерської загрози: особисті риси, мотивація до атаки, психологічний стан, можливості (access/opportunity), навички.

— Ця модель показує, що мотивація інсайдера — це не одновимірна річ, а сукупність факторів: не лише бажання наживи, але й можливість, внутрішній психологічний стан, сприйняття можливостей в організації.

Модель визначення "загрози через аналіз поведінки"

— Хоч це не виключно мотиваційна модель, але багато сучасних систем виявлення інсайдерів базуються на поведінковому аналізі (поведінковий аналіз користувача — UEBA). Наприклад, в роботі "Real-Time Detection of Insider Threats Using Behavioral Analytics" аналізують поведінку як сигнал потенційної загрози.

— Поведінкові аномалії (наприклад, нестандартний час активності, нетипове пересування між застосунками) можуть служити індикаторами, що мотивує глибше дослідження — навіть якщо внутрішня мотивація (як ревність, фінансова вигода, образа) не є безпосередньо видимою.

Приклади мотиваційних сценаріїв:

Фінансово мотивований інсайдер: співробітник має великі борги або бажає підзаробити — використовує доступ до важливих комерційних даних і продає їх конкуренту або на чорному ринку.

“Ображений” працівник: людина, яка вважає, що її несправедливо обійшли з підвищенням або премією, після звільнення або конфлікту завантажує внутрішні документи або руйнує системи.

Ідеологічно мотивований інсайдер: працівник, який не погоджується з політикою компанії або її клієнтів, може викладати внутрішню інформацію у відкритий доступ, щоб висвітлити “несправедливість”.

Підвищений доступ - можливість: навіть якщо співробітник не має сильної ворожості до організації, але має привілейований доступ і відчуває, що може скористатися моментом (наприклад, перед звільненням), він може зловживати даними

Вплив мотивацій на протидію:

- Розуміння мотивацій — це критично, бо методи захисту повинні бути адаптовані до конкретних “драйверів” інсайдера:
- Якщо основна мотивація — фінансова, організація може запровадити більш жорсткий контроль доступу, DLP-системи, політики моніторингу. [26]
- Якщо це “несправедливість” в організації (revenge), важливо працювати з HR, проводити опитування задоволеності співробітників, створювати канали для вирішення конфліктів.

- При ідеологічних мотиваціях — прозорість політик, етичні кодекси, комунікація цінностей компанії.
- Для моделей поведінкового аналізу — впровадження UEBA, детектування аномалій, навчання аналітиків безпеки, щоб вони могли інтерпретувати сигнали.

Таблиця 4. Класифікація інсайдерів за мотивацією

Тип інсайдера	**Мотивація**	**Приклади дій**
Фінансово мотивований	отримання прибутку	продаж даних, шахрайство
“Ображений” працівник	помста, незадоволеність	саботаж, знищення інформації
Ідеологічний	моральна або політична позиція	поширення внутрішніх матеріалів
Під тиском	шантаж, зовнішній примус	надання доступу стороннім
Ненавмисний	помилки, неуважність	відкриття фішингових листів, неправильна обробка даних

Аналіз причин інсайдерських загроз, можна зазначити, що вони формуються під впливом комплексу особистісних, психологічних, соціальних і організаційних чинників. Інсайдер — це не лише зловмисник, а й будь-який співробітник, який з різних причин може допустити дії, що призводять до витоку або компрометації інформації. Фінансові мотиви, емоційний стан, ідеологічні переконання, зовнішній примус або банальна неуважність — усі ці фактори можуть стати каталізаторами інсайдерського ризику. [23]

Ефективна система протидії повинна враховувати багатовимірність цього явища, поєднуючи організаційні заходи, технічний моніторинг, формування

здорової корпоративної культури та систематичне навчання персоналу. Усвідомлення причин формування інсайдерської загрози є основою для розробки комплексних контрзаходів, спрямованих на зниження ймовірності інцидентів та мінімізацію їхнього впливу на організацію.

1.3 Аналіз нормативно-правової та стандартної бази та огляд наукових джерел і сучасних технологічних підходів

У сучасному інформаційному середовищі внутрішні загрози (інсайдерські загрози) становлять одну з найскладніших проблем для організацій, оскільки вони поєднують у собі аспект людського фактору, технічні уразливості та організаційну структуру.

Для ефективного протидії таким загрозам необхідна не лише внутрішня політика безпеки, а й відповідна нормативно-правова та стандартна база, що забезпечує рамки для управління ризиками, реагування на інциденти та впровадження систем захисту.

Нормативно-правова база України:

1. Законодавство України у сфері інформаційної безпеки

В Україні існує нормативна база, яка регламентує захист інформації, зокрема законодавчі акти, що охоплюють персональні дані, інформаційні системи тощо. Наприклад, положення “Деякі питання електронної ідентифікації” від 28 червня 2024 року № 764 регулюють питання приватності та кібербезпеки. [1, 2, 4]

Закон України «Про основні засади забезпечення кібербезпеки України» закон № 2163-VIII від 05.10.2017. Цей закон встановлює загальні принципи кібербезпеки, визначає відповідальних органів, системи реагування на кіберзагрози. [1]

Закон України № 4336-IX (2025) «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів» — ухвалений 27 березня 2025 року.

Цей закон передбачає створення національної системи реагування на кіберінциденти, ролі національного, галузевого та регіонального CSIRT, а також правову основу для авторизації систем безпеки державних IT-систем.

Встановлюється можливість сертифікації систем безпеки замість старої процедури “комплексних систем захисту інформації” (CISS).

Закон України «Про Державну службу спеціального зв’язку та захисту інформації України» — встановлює функції Держспецзв’язку (SSSCIP), стандартів, аудитів, сертифікації в галузі кібербезпеки. [1] [5]

Адміністративні та кримінальні санкції: недотримання вимог законодавства з інформаційної безпеки тягне відповідальність. Зокрема, державні органи (SSSCIP, СБУ) можуть застосовувати адміністративні санкції.

Аудит безпеки критичної інфраструктури: Порядок незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури визначено постановою КМУ від 24.03.2023 № 257.

Стратегічні документи:

Стратегія кібербезпеки України (2021): ця стратегія була затверджена указом Президента і визначає пріоритети захисту інформаційної інфраструктури, включно із захистом критичних ресурсів. [1]

Роль CERT-UA: Державна служба спеціального зв'язку та захисту інформації (SSSCIP) забезпечує функціонування Національного CERT (CERT-UA), який займається реагуванням на кібератаки, аналізом інцидентів та координацією. [14]

Також майже у всіх підприємствах і державних структурах важливо дотримуватися законодавства, яке вимагає захисту персональних даних та

інформаційної системи — це створює правову основу для політик безпеки, реагування на інциденти, внутрішнього аудиту. [4]

В Україні прийняті стандарти на основі ISO / IEC. Наприклад, ДСТУ ISO/IEC 27002:2015 встановлює конкретні рекомендації для організаційного й технічного захисту інформаційних ресурсів. [11]

У 2025 році набирають чинності нові національні варіанти стандартів, такі як ДСТУ ISO/IEC 27035-1:2024, 27035-2:2024 та 27035-3:2024, які стосуються управління інцидентами безпеки. [12]

Таким чином, нормативна база України активно адаптує міжнародні стандарти до національних умов, що дозволяє організаціям створювати системи управління інформаційною безпекою (СУІБ), які відповідають найкращим практикам.

Приклади українських компаній, які працюють за стандартами безпеки:

Київстар: Український телеком-оператор Київстар успішно пройшов аудит і отримав сертифікацію за стандартом ISO/IEC 27001. Це показовий приклад компанії, яка серйозно ставиться до системи управління інформаційною безпекою (ISMS). [10]

Це означає, що вони впровадили формальні процеси безпеки, захисту даних та управління конфіденційною інформацією.

TÜV Thüringen Україна: Організація, яка проводить сертифікацію в Україні за ISO/IEC 27001, допомагаючи компаніям підтвердити відповідність їхніх систем управління інформаційною безпекою міжнародним стандартам. [10]

IT-компанії з досвідом сертифікації: За інформацією AIN.UA, кілька українських IT-компаній мають сертифікати ISO 27001, а також інші стандарти — ISO 9001 і ISO 27701.

Міжнародні стандарти інформаційної безпеки

ISO/IEC 27001 — ключовий міжнародний стандарт для систем управління інформаційною безпекою (ISMS). Він визначає вимоги до побудови, впровадження, підтримки й постійного вдосконалення СУІБ.

Версія 2022 року переглянула та оновила вимоги, зокрема у структурі СУІБ, підходах до ризик-менеджменту та контролю безпеки.

Сертифікація за ISO/IEC 27001 підтверджує, що організація має формалізовану систему безпеки. В Україні, наприклад, TÜV Thüringen Ukraine проводить сертифікацію СУІБ за цим стандартом.

ISO/IEC 27002 є “кодексом практик” і містить набір рекомендацій з контролю інформаційної безпеки: політики, права доступу, криптографії, фізичної безпеки, управління активами тощо.

У версії 2022 деякі секції були перегруповані або спрощені, а також переглянуто заходи, щоб зробити їх ефективнішими з урахуванням сучасних загроз.

ISO/IEC 27002 допомагає організаціям розробляти політики безпеки й впроваджувати конкретні засоби контролю, включно з контролем доступу та моніторингом. [11]

ISO/IEC 27035 — управління інцидентами інформаційної безпеки [12]

Стандарт ISO/IEC 27035 присвячений процесам управління інцидентами: виявлення, звітність, реагування, аналіз причин та покращення. [12]

Нові національні переклади стандарту (ДСТУ) набирають чинності в Україні, що дозволяє організаціям формувати системи реагування на інциденти відповідно до міжнародної практики.

Використання ISO/IEC 27035 дає змогу організаціям швидше виявляти інциденти, структурувати процеси реагування та аналізувати уроки після інциденту, щоб підвищити стійкість до майбутніх загроз.

Інші стандарти з родини ISO/IEC 27000

ISO/IEC 27005 — стандарт, який фокусується на управлінні ризиками інформаційної безпеки, що є критично важливим для оцінки інсайдерських загроз і планування контрзаходів.

Є також стандарти, що стосуються специфічних тем, наприклад, ISO/IEC 27011 (безпека телекомунікацій), ISO/IEC 27018 (захист персональних даних у хмарах) [4]

Сучасні технологічні підходи (інструменти та їх застосування):

1. Data Loss Prevention (DLP) — виявляє і блокує несанкціоновану передачу конфіденційних даних (електронна пошта, файли, хмарні сервіси). DLP — одна з базових технологій у профілактиці випадкових і навмисних витоків. Практичні кейси (DLP впровадження в компаніях) демонструють ефективність при правильній класифікації даних і налаштуванні політик. [26]
2. User and Entity Behavior Analytics (UEBA) — аналіз нормальної та аномальної поведінки користувачів/сервісів; дозволяє виявляти незвичну активність (навантаження, експорт великих обсягів, доступ до незвичних ресурсів). UEBA часто інтегрують із SIEM. [30]
3. Security Information and Event Management (SIEM) — збір журналів та подій, кореляція, базова платформа для виявлення та реагування; в поєднанні з UEBA і DLP створює багаторівневу систему детекції. [26, 30]
4. Endpoint Detection & Response (EDR) — моніторинг і реагування на кінцевих точках; EDR може виявити підозрілі дії на робочих станціях (масове читання файлів, підключення зовнішніх дисків).
5. Cloud Access Security Broker (CASB) / CASM — контроль обміну даними та політик у хмарних сервісах (SaaS), важливий у разі, коли співробітники використовують хмарні сервіси для передачі інформації.

6. Політики доступу (Least Privilege, RBAC/ABAC) — технічне запобігання можливості зловживання шляхом скорочення прав доступу, сегментації, відокремлення привілейованих облікових записів. (Підхід наголошують і стандартні рамки, і наукові джерела.)

Класичний кейс масового експортного скачування (Yahoo / інші кейси) — приклад, коли працівник одержавши пропозицію від конкурента, швидко експортнув великі обсяги інтелектуальної власності; цей інцидент підкреслює потребу DLP + UEBA + аудит привілейованих дій. [26]

Кейс впровадження DLP у корпоративному середовищі (проект-портфоліо GTB) — кілька постачальників описали впровадження DLP для блокування несанкціонованої відправки файлів по e-mail та збереження конфіденційних файлів у хмарі. Успіх залежав від попередньої класифікації даних і тонкого налаштування політик. [26]

Таблиця 5 Технології проблеми внутрішніх загроз

Технологія	**Основні функції**	**Для яких інсайдерських сценаріїв корисна**
DLP	Ідентифікує/блокує витік даних (email, web, endpoint, cloud)	Навмисний/ненавмисний витік конфіденційних файлів.
UEBA	Виявлення поведінкових аномалій	Масове скачування, незвична активність обліковки.
SIEM + EDR	Журнали, кореляція, реагування	Розслідування інцидентів, швидка реакція на підозрілі дії.
CASB	Контроль доступу й політик у SaaS	Захист даних у хмарі, попередження несанкціонованої публікації.

Запровадження нового закону № 4336-IX (2025) підсилює нормативну базу України саме в контексті кібербезпеки й реагування на інциденти, включно з інсайдерськими ризиками. Сертифікація інформаційних систем стала більш формалізованою: організації можуть обирати сертифікацію за стандартами, а не лише традиційні “комплексні системи захисту”. [1,23]

Практика українських компаній (наприклад, Київстар) демонструє, що стандарти ISO/IEC 27001 застосовуються на реальному бізнес-рівні, і це вже не просто “бажаний клас”, а реальний інструмент для побудови надійної системи управління безпекою. [10]

Наявність органів, SSSCIP та CERT-UA, дає державі інструменти для аудиту, сертифікації й реагування на інсайдерські загрози. У поєднанні з міжнародними стандартами це створює міцну фундаментальну базу для протидії внутрішнім загрозам. [14, 23]

Аналіз нормативно-правової, стандартної та наукової бази показує, що для ефективної протидії інсайдерським загрозам необхідний багаторівневий підхід. На міжнародному рівні стандарти ISO/IEC серії 27000 (зокрема 27001, 27002, 27035) надають формальні рамки для побудови систем управління інформаційною безпекою, управління інцидентами та контролю доступу. Українське законодавство та національні стандарти (ДСТУ) активно інтегрують ці міжнародні підходи, адаптуючи їх до національного контексту. [23]

Крім того, наукові дослідження та сучасні технологічні рішення (UEBA, SIEM, моделі ризику, машинне навчання) надають практичні інструменти для виявлення, прогнозування та реагування на інсайдерські загрози. Об’єднання нормативного, стандартного та технологічного підходів дозволяє організаціям підвищувати стійкість до внутрішніх загроз і створювати проактивні стратегії безпеки: [23, 30]

1. Підвищені технічні вимоги: Введення сертифікації комплексів захисту інформації означає, що системи з обробкою чутливих даних (особливо

державних) повинні відповідати жорстким стандартам. Це підвищує бар'єр для інсайдерів — вони матимуть справу з надійнішими системами захисту, можуть бути кращі логи, аудит, контроль доступу.

2. Обмін інформацією про інциденти: Створення національної системи обміну повідомленнями про кіберінциденти (через Держспецзв'язку) дає можливість швидше реагувати на інсайдерські інциденти, отримувати дані про тренди та атаки, аналізувати їх і навчатися. [5]
3. Обов'язкові кіберфахівці: Введення штатних спеціалістів з кібербезпеки в державні органи та на інфраструктурні об'єкти — це позитивно для внутрішнього контролю, моніторингу та виявлення можливих інсайдерських загроз. [1, 23]
4. Можливість примусового реагування: Держспецзв'язку та СБУ можуть видавати обов'язкові розпорядчі акти у випадку кіберінцидентів. Це може бути використано для швидкої втручання в ситуації підозрілої активності (включно з інсайдерськими загрозами). [5]
5. Експертиза ПЗ: Потрібна державна експертиза програмного забезпечення, що використовується у критично важливих системах. Це означає, що зовнішній або внутрішній інсайдер ризикує, якщо використовує нелегітимне або "тіньове" ПЗ — воно може не пройти експертизу або бути виявлене.

Комбінований підхід — стандарти (ISO, NIST) визначають принципи і процеси; щоб ефективно протидіяти інсайдерським загрозам, необхідно поєднати організаційні (HR, політики, навчання) та технічні рішення (DLP, UEBA, SIEM/EDR, CASB).

Побудова програми insider threat — призначення відповідальних осіб, інтеграція з HR і юридичним підрозділом, процеси розслідування і звітності (NIST PM-12, ISO/IEC 27035). [9, 12]

Реальні кейси показують — DLP + UEBA у поєднанні із швидким реагуванням істотно знижують ризик великих витоків; однак критично важлива

якісна класифікація даних і адаптація політик, інакше зростає кількість false positives. [26]

Висновок до розділу 1

У першому розділі дипломної роботи було здійснено глибокий аналіз внутрішніх загроз, що є одними з найскладніших для виявлення та управління в системах безпеки.

Визначено, що інсайдерські загрози можуть виникати через осіб, які мають легітимний доступ до інформаційних ресурсів організації.

Це можуть бути не тільки навмисні, але й ненавмисні дії з боку співробітників, пов'язані з людським фактором.

Причини таких загроз можуть бути різноманітними: від фінансових або особистих мотивів до помилок в роботі або недостатнього усвідомлення співробітниками безпеки.

Модель інсайдерських загроз, на основі якої будуються заходи для їх протидії, дозволяє зрозуміти важливість комплексного підходу. Визначено, що важливу роль у боротьбі з інсайдерами відіграє чітка нормативно-правова база та стандарти, які повинні бути інтегровані в систему інформаційної безпеки організації.

Проте тільки технічних заходів недостатньо — необхідні організаційні політики, які регулюють поведінку співробітників та контроль доступу до інформаційних систем.

РОЗДІЛ 2
АНАЛІЗ ВНУТРІШНІХ ЗАГРОЗ ТА ІСНУЮЧИХ МЕТОДІВ ПРОТИДІЇ ВИТОКУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

2.1 Особливості витоку інформації через внутрішні загрози

Витік інформації через внутрішні загрози (інсайдерів) є однією з найскладніших проблем у сфері інформаційної безпеки. Основна складність полягає в тому, що інсайдер має легітимний, санкціонований доступ до інформаційних ресурсів організації. На відміну від зовнішнього зловмисника, інсайдер не долає периметр безпеки — він знаходиться всередині системи, що робить традиційні засоби захисту менш ефективними. [23]

Проблема також посилюється людським фактором: співробітники можуть ненавмисно спричинити витік через помилки, нехтування правилами або низьку культуру інформаційної безпеки. У сучасних організаціях, де значна частина процесів автоматизована, а обсяги даних постійно зростають, саме інсайдерські ризики виходять на один із ключових рівнів загроз.

Витоки інформації через інсайдерів відносяться до найбільш небезпечних видів інцидентів, оскільки часто стосуються комерційної таємниці, персональних даних, критичних бізнес-процесів і стратегічної інформації, втрата яких може спричинити значні фінансові, юридичні та репутаційні збитки. [4]

Внутрішні загрози (інсайдерські загрози) посідають особливе місце серед кіберризиків організації, оскільки вони походять від людей, які вже мають легітимний доступ до інформаційних ресурсів. На відміну від зовнішніх атак, інсайдерські інциденти часто залишаються непоміченими, адже користувач діє у межах своїх прав доступу. Через це системи безпеки, побудовані на принципах perimeter-security, виявляються малоефективними.

Проблема витоку інформації через внутрішніх зловмисників або ненавмисних інсайдерів полягає в тому, що саме близькість до ресурсів, обізнаність у процесах, знання слабких місць та достатній доступ створюють ідеальні умови для несанкціонованого винесення даних. Особливо критичною ця проблема є для організацій, що працюють з персональними даними, комерційною таємницею, інтелектуальною власністю, фінансовою документацією та технологічними процесами.

Більшість досліджень підтверджує, що 70–80% інцидентів витоку інформації так чи інакше пов’язані з діями людей, а інсайдерські загрози входять у ТОП-3 ризиків інформаційної безпеки для великих і середніх підприємств. Це формує необхідність не тільки технічного контролю, але й розвитку процесів, які враховують поведінкові, організаційні й психологічні аспекти загроз.

Усі інсайдерські ризики можна умовно поділити на такі групи:

1. Ризики, пов’язані з людським фактором

- необережність, халатність, помилки персоналу;
- недостатня кіберграмотність;
- натискання фішингових посилань;
- випадкове розголошення даних;
- неправильне використання корпоративних сервісів.

2. Ризики, пов’язані з навмисними діями інсайдера

- крадіжка даних (комерційної таємниці, персональних даних, IP); [4]
- передача інформації конкурентам;
- саботаж, знищення даних;
- внесення шкідливих змін до інформаційних систем;
- шахрайство або фінансові махінації.

3. Ризики, пов’язані з доступом третіх сторін

- підрядники отримують надмірні права;
- зовнішні консультанти мають доступ після завершення договорів;
- привілейовані користувачі (адміністратори) не контролюються.

4. Організаційні ризики

- відсутність політик доступу;
- слабкі процеси розмежування прав;
- відсутність журналювання дій користувачів;
- відсутність регулярного аудиту дій співробітників.

5. Технічні ризики

- відсутність DLP-систем; [26]
- відсутній моніторинг поведінки користувачів;
- слабкий контроль мобільних пристроїв;
- використання незахищених каналів обміну інформацією.

Також класифікуються за таким сценаріями:

1. Сценарій “Незадоволений співробітник”

- має доступ до конфіденційних даних;
- копіює їх перед звільненням;
- видаляє або змінює інформацію;
- передає конкурентам.

2. Сценарій “Випадковий витік”

- працівник пересилає документ на особисту пошту;

- використовує незахищений месенджер;
- відкриває фішингове посилання;
- копіює дані на флешку “для зручності”.

3. Сценарій “Підрядник-інсайдер” [23]

- тимчасовий працівник отримує права доступу;
- виносить дані або передає їх третім сторонам;
- використовує інформацію після завершення контракту.

4. Сценарій “Привілейований користувач”

- адміністратор системи має необмежений доступ;
- змінює журнали подій;
- використовує root- або domain-права для маніпуляцій.

5. Сценарій “Колюзивний інсайдер”

- співробітник та зовнішній зловмисник діють разом;
- інсайдер допомагає обійти політики доступу;
- результатом є масштабний витік або саботаж.

Нижче — таблиця пикладів типових сценарії інсайдерських загроз, які ілюструють як це відбувається на практиці. [23]

Таблиця 6 сценарії інсайдерських загроз

Сценарій / тип інсайдерської дії	**Приклад**	**Як відбувалось**	**Наслідки**
Зловмисний інсайдер — крадіжка інтелектуальної власності / комерційних	Yahoo — інженер/науковець, що завантажив ~ 570 000 сторінок документації	Інсайдер отримав офер від конкурента, і перед звільненням (або під час переходу) скачав	Втрата комерційної/технічної інформації, репутаційні ризики, потенційні судові

Сценарій / тип інсайдерської дії	Приклад	Як відбувалось	Наслідки
секретів перед переходом до конкурента	перед працевлаштуванням у конкурента.	величезний обсяг IP-документації, вихідного коду, технічних специфікацій.	позови, підрив конкурентних переваг.
Зловмисний інсайдер — викрадення секретних технологій / ноу-хау	Google / Waymo — інженер, який перед переходом до конкурентів (стартап, придбаний іншим гравцем ринку) завантажив десятки тисяч конфіденційних файлів (лідар-технології, креслення, алгоритми).	За кілька тижнів до звільнення інженер скопіював ~ 14 000 файлів (~ 9.7 ГБ) з конфіденційними даними, які становили технологічну цінність.	Втрачено інтелектуальні права, технологічна конкуренція під загрозою, судові позови, необхідність перегляду політик доступу.
Саботаж / логічна бомба після звільнення	Omega Engineering — випадок із “logic bomb”: колишній системний адміністратор після звільнення активував код, який знищив критичне програмне забезпечення підприємства.	Після звільнення він запрограмував так, що через деякий час (або за певних умов) виконалась шкідлива дія — видалення важливих програм/даних.	Суттєві фінансові втрати (за оцінками — мільйони), простої, необхідність відновлення систем, посилення контролю при offboarding (видаленні доступів).
Ненавмисна (помилкова) поведінка — випадкові витоки або несправності	Microsoft (2022) — випадкове розкриття логінів / облікових даних GitHub через внутрішню помилку.	Співробітники ненавмисно опублікували або неправильно налаштували доступ, що допустило витік облікових даних або кодів.	Навіть без злого наміру — організаційні збитки, ризики безпеки, потреба у перегляді політик доступу та управління налаштуваннями.

Сценарій / тип інсайдерської дії	Приклад	Як відбувалось	Наслідки
Зловживання доступом після звільнення / недоотримане відключення прав	Cisco — колишній працівник, який після звільнення отримав доступ до хмарних ресурсів і видалив 456 віртуальних машин, підтримуючих сервіси.	Використав старі (не відкликані) облікові дані, підключився до ресурсів і здійснив руйнівні дії.	Втрати для користувачів, простої сервісів, фінансові/репутаційні збитки, підвищення уваги до правильного закриття доступів при звільненні.

Наведені приклади — з різних галузей (технології, R&D, сервіс, хмарні сервіси), що демонструє: інсайдерська загроза стосується будь-якої організації, яка має цінні дані або системи.

Загроза може бути як зловмисною, так і ненавмисною — що ускладнює виявлення та захист.

Багато випадків — через звичні бізнес-процеси: звільнення, передача прав, перехід працівника до конкурента, недостатній контроль доступів, недостатній моніторинг.

Ці сценарії ілюструють, як організаційні та технічні аспекти (процеси offboarding, політики доступу, моніторинг) — критично важливі для запобігання витоку. Вони можуть слугувати основою для розробки контрзаходів в твоєму дипломі.

Приклади в Україні за таблицею:

Таблиця 7 Типові сценарії інсайдерів в Україні

Сценарій	Опис	Можливий реальний публічний індикатор в Україні	Типовий канал витоку	Запобіжні контрзаходи
Помилкова/ненавмисна витік через неправильну конфігурацію	Неправильно налаштований сервіс, доступ до бази даних з відкритим доступом	Повідомлення про масиви gov.ua в даркнет (2020) — приклад, коли відкриті списки адрес/даних стали доступні публічно.	Відкриті HTTP/Cloudflare, S3-подібні бакети, публічні API	Регулярні аудити налаштувань, автоматичні сканери, hardening, SIEM/логування
Зловмисний інсайдер — ексфільтрація перед звільненням	Працівник копіює IP або закриті реєстри перед переходом/звільненням	Неофіційні випадки у приватних компаніях (міжнародні), у держсекторі — часто не афішуються; CERT-UA радить моніторити нетипову активність перед звільненням.	USB, особисті облікові записи, хмарні сервіси	Offboarding процеси, DLP, обмеження привілеїв, моніторинг перед звільненням
Компрометація облікових записів і використання їх після звільнення	Старі креденшали не відкликані → зловмисник (колишній) використовує доступ	У загальних звітах CERT-UA зустрічаються інциденти з несанкціонованим доступом (часто зовнішнього характеру або через	Хмарні сервіси, VPN, RDP	Автоматичне відкликання прав, MFA, часті ревізії обліковок

Сценарій	Опис	Можливий реальний публічний індикатор в Україні	Типовий канал витоку	Запобіжні контрзаходи
		скомпрометовані облікі).		
Саботаж (логічна бомба / зміна конфігурації)	Колишній адміністратор/незадоволений співробітник вбудовує код або змінює конфігурації	Міжнародні кейси — логічні бомби; у локальному середовищі подібні випадки не оприлюднюють, але ризик існує	Скрипти, cron, планувальники, привілеї root	Розподіл привілеїв, контроль змін (change management), код-рев'ю, резервні копії
Колаборація з зовнішніми акторами (шантаж/корупція)	Співробітник співпрацює з третіми особами чи ворогом (ідеологія/шантаж)	CERT-UA фіксує зовнішні кампанії; внутрішній канал співпраці складно довести у відкритих джерелах.	Таємні передачі, особисті зустрічі, зашифровані канали	Контроль доступу, аудит, розслідування, політика «розділення обов'язків»

Компанії рідко розголошують, що витік чи інцидент стався через внутрішню проблему (insider), — часто називають це «технічним збоєм», «зовнішньою кібератакою» або просто «витоком даних», без уточнення джерела. Це пов'язано з репутаційними ризиками.

Багато інсайдерських інцидентів залишаються внутрішніми, вирішуються приватно, і не потрапляють у ЗМІ або публічні звіти.

Публічних, документально підтверджених прикладів «чистих» insider-інцидентів у великих українських державних структурах чи критичній інфраструктурі у відкритих джерелах мало або їх немає. Державні установи рідко розкривають, що інцидент спричинений внутрішнім користувачем; такі випадки

часто приховують через репутаційні та безпекові ризики. (підтвердження— аналіз публікацій CERT-UA та оглядів кіберзагроз). [14]

Є численні відкриті звіти CERT-UA / Держспецзв'язку про кіберінциденти та тренди, проте вони зазвичай фокусуються на зовнішніх кампаніях (APT-угрупованнях, фішингу, експлойтах) та загальних рекомендаціях щодо захисту; рідше — публічно вказують на внутрішні причини. Це робить неможливим для стороннього дослідника достовірно описати конкретні «інсайдерські» кейси без доступу до закритих звітів. [14]

Є приклади витоків/інцидентів у національному контексті, де внутрішній фактор міг/може грати роль (але без однозначного підтвердження) — наприклад, повідомлення про великі обсяги «витоків» даних або неправильно налаштовані сервіси, де причиною могли бути помилки адміністрування або зловживання доступом. Приклад — повідомлення про масиви доменів gov.ua у даркнеті у 2020 році (Cloudflare-повідомлення).

Особливо в умовах високої секретності (держсектор, критична інфраструктура) — інформація часто закритого типу.

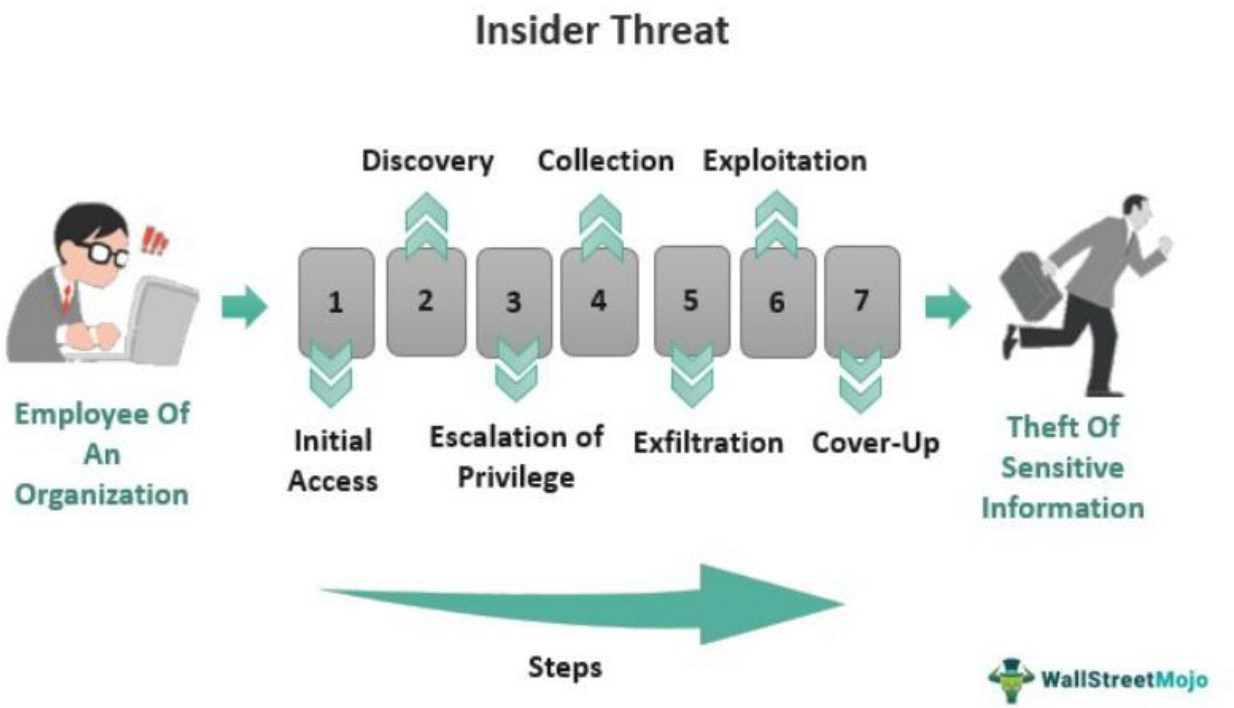

Рис.2 Етапи реалізації інсайдерської загрози [33]

1. Наявність доступу (Authorized Access) — інсайдер має легітимні права доступу до систем / даних.
2. Мотивація або спусковий фактор — фінансова вигода, незадоволеність, ідеологія, бажання перейти до конкурента, помста, відсутність контролю тощо.
3. Зловживання або помилка — навмисне копіювання/видалення/експорт даних, випадкова публікація, неправильна конфігурація, саботаж.
4. Екфільтрація / витік / саботаж — передача даних назовні, викрадення інтелектуальної власності, знищення чи модифікація даних, саботаж систем, просочування до конкурентів.
5. Наслідки — матеріальні збитки, втрата репутації, юридична відповідальність, порушення довіри, витрати на відновлення і реагування.

6. Виявлення / реагування / запобігання — аудит, моніторинг, політики безпеки, відключення доступів при звільненні, аналіз поведінки (behavior analytics), UEBA, DLP, внутрішній контроль.

2.2 Організаційно-технічні методи протидії

У попередніх розділах ми розглянули природу внутрішніх загроз, мотиви інсайдерів, типові сценарії витоку інформації. Але розуміння проблеми — це лише перший крок. Щоб ефективно зменшити ризики, компанії повинні впроваджувати системну стратегію протидії: поєднувати організаційні заходи (політики, процеси, людський фактор) з технічними засобами (контроль доступу, моніторинг, системи безпеки). У цьому підпункті ми опишемо ключові методи та механізми такої протидії — класичних і сучасних; надамо порівняльні таблиці, модель, а також аналіз їх переваг та обмежень. [17]

Сучасні системи інформаційної безпеки мають забезпечувати не лише технічний моніторинг, але й формування культури безпеки в колективі, прозорість бізнес-процесів, чіткість ролей і розмежування відповідальності. Міжнародні стандарти ISO 27001, ISO 27002, ISO 27035, NIST SP 800-61, а також моделі поведінкової аналітики UEBA визначають цілісний підхід до протидії внутрішнім загрозам, який поєднує організаційне врядування і технічні інструменти. [8]

Організаційні методи орієнтовані на формування політики безпеки, правил, процедур, культури безпеки в компанії, а також на управління людським фактором. Нижче — ключові підходи:

Політика безпеки та правила доступу

— Визначення чітких політик роботи з конфіденційними або критичними даними; розмежування доступів за ролями (role-based access control, RBAC), принцип «потрібно знати / потрібна робота» (need-to-know).

— Регулярний перегляд прав доступу, особливо після змін у посаді, при звільненні, зміні обов’язків.

Управління привілейованим доступом (Privileged Access Management, PAM)

— Для облікових записів з підвищеними привілеями (адміністратори, технічні служби) встановлюють окремі процедури надання, моніторингу, відзвітування про дії, а також обмеження часу/сесії, журнали.

Навчання персоналу, підвищення обізнаності, формування культури безпеки

— Регулярні тренінги для співробітників щодо політик безпеки, поводження з конфіденційною інформацією, розпізнавання соціальної інженерії, фішингових атак, відповідальності за порушення.

— Пояснення наслідків витоку, утворення культури відповідальності, підвищення мотивації працівників до дотримання політик безпеки.

Процеси управління ризиками та їх оцінювання

— Використання методів управління ризиками інформаційної безпеки, таких як CRAMM, COBIT 5 for Risk (і подібних) для ідентифікації активів, оцінювання загроз та вразливостей, визначення ризиків і пріоритетів контрзаходів.

— Періодичний перегляд ризиків, оновлення політик, адаптація до змін у структурі, процесах, технологіях.

Процедури реагування на інциденти, аудит і контроль (інсайдерський ризик-менеджмент) [23]

— Формалізовані процедури реагування на підозрілу поведінку, інциденти, витоки; аудит дій користувачів, переспрямування доступів, розслідування.

— Забезпечення «offboarding» — чітке закриття доступів при звільненні, зміні ролей; контроль завершення сесій, вилучення доступів до систем, даних, портативних носіїв.

Протидія інсайдерським загрозам потребує інтеграції організаційних (адміністративних), технічних, поведінкових і нормативних заходів, які разом створюють багаторівневу систему безпеки. На відміну від зовнішніх атак, внутрішні загрози є складнішими для виявлення через наявність у зловмисників легітимних прав доступу, знання внутрішніх процесів та відсутність необхідності «ламати» периметр системи. Саме тому сучасні організації повинні застосовувати комплексний підхід, який охоплює політики безпеки, аудит, контроль доступів, системи моніторингу поведінки, DLP, SIEM/UEBA технології, процедури управління персоналом, управління інцидентами, а також заходи, спрямовані на мінімізацію людського фактору. [23] [30] [26]

До ключових політик належать:

- Політика контролю доступу (Access Control Policy): регламентує призначення, зміну та анулювання доступів.
- Політика класифікації інформації: визначає рівні доступу, вимоги до зберігання, обміну та знищення даних.
- Політика управління інцидентами (відповідно до ISO/IEC 27035). [12]
- Політика прийнятного використання ресурсів (AUP).
- Політика резервного копіювання та зберігання логів.
- Політика роботи персоналу (HR Security Policy) — одна з основних для боротьби з інсайдерами. [23]

Більшість з цих політик прямо передбачені ISO/IEC 27001, ISO/IEC 27002 та NIST 800-53. [10] [11]

За принципом:

1. Least Privilege (LP) — доступ лише до ресурсів, необхідних для виконання робочих функцій.

2. Segregation of Duties (SoD) — розподіл прав, щоб жодна людина не могла завершити критично важливу операцію самостійно.
3. Need-to-Know Basis — доступ до конфіденційної інформації лише при обґрунтованій необхідності.

За інструментами:

RBAC — Role-Based Access Control

ABAC — Attribute-Based Access Control

PBAC — Policy-Based Access Control

PAM — Privileged Access Management

У банківському секторі України системи PAM впроваджені у ПриватБанку, Ощадбанку та низці IT-компаній, де всі дії адміністраторів журналюються, а доступ видається тимчасово («Just in Time Access»).

Організаційні методи включають роботу з персоналом протягом усього робочого циклу:

На етапі найму

- Перевірка кандидатів (background check)
- Аналіз судимостей (де дозволено)
- Підписання NDA, згоди про конфіденційність, політик безпеки

Під час роботи

- Регулярні тренінги з безпеки
- Психологічний моніторинг (стрес, конфлікти, відхилення)
- Оцінка лояльності співробітників (Employee Risk Scoring)

Після звільнення

- Негайне анулювання доступів (Offboarding Procedure)

- Видалення ключів, токенів, VPN-сертифікатів
- Аудит останніх активностей користувача

У багатьох інцидентах (Cisco 2018, Tesla 2019) інсайдерські дії ставали можливими саме через відсутність або затримку у відкликанні доступів. [23]

Людський фактор є однією з основних причин інсайдерських інцидентів. За статистикою ESET та IBM, майже 22–30 % витоків даних пов'язані саме з персоналом (навмисно або випадково). [17] [23]

Методи зниження ризику:

- Формування культури безпеки (Security Culture)
- Регулярні фішингові симуляції (Anti-Phishing Campaigns)
- Навчання з DLP, правил поводження з даними [26]
- Програми підтримки співробітників для зниження стресу
- Анонімні канали для повідомлення про підозрілу поведінку (Whistleblowing System)

Багато компаній у ЄС/США використовують моделі поведінкового профілювання співробітників — UEBA, ML-класифікація ризиків.

Технічні методи протидії внутрішнім загрозам:

1. DLP-системи (Data Loss Prevention) [26]

DLP — ключовий інструмент для виявлення спроб ексфільтрації інформації. [26]

Можливості DLP: [26]

- Блокування копіювання даних на USB-носії
- Контроль електронної пошти
- Контроль хмарних сервісів (OneDrive, Google Drive)

- Контроль друку
- Виявлення порушення класифікації даних
- Виявлення масового копіювання/експорту даних

Приклади DLP: [26]

- Symantec DLP [26]
- InfoWatch Traffic Monitor
- Safetica
- FalconForce RU DLP [26]
- McAfee Total Protection DLP [26]

DLP рекомендована стандартами ISO 27001 Annex A, ISO 27002, NIST SP 800-53 (контроль AC-4, MP-5, SI-4). [7] [26]

2. SIEM та UEBA [30]

SIEM (Security Information and Event Management) збирає, корелює та аналізує лог-події з усіх систем. [30]

UEBA (User and Entity Behavior Analytics). Використовує Machine Learning для виявлення:

- Аномальної поведінки користувачів (UAR)
- Нетипових робочих часових зон
- Підозрілих доступів до баз даних
- Масових завантажень / викачувань даних
- Нестандартних команд адміністраторів

Поширені продукти:

- Splunk Enterprise Security
- IBM QRadar
- Elastic SIEM (поширений в Україні) [30]

- Microsoft Sentinel
- Gurucul UEBA
- Vectra AI

UEBA ефективно виявляє «скритих» інсайдерів, які не генерують явних порушень, але змінюють поведінку (перед звільненням, після конфлікту тощо). [23]

3. Криптографічні методи:

- Шифрування даних «на льоту» та «в спокої» (AES-256)
- TLS 1.3 для передавання даних
- Електронні цифрові підписи (ЕЦП)
- Захист документів DRM/IRM

Криптографія не запобігає інсайдеру, але зменшує наслідки при випадковому витоку або перехопленні даних. [23]

4. Контроль привілейованих доступів (PAM)

Переваги PAM:

- Журналювання кожної сесії адміністратора
- Відеозапис усіх команд
- Тимчасові доступи («Just-in-Time»)
- Парольні сейфи, які автоматично змінюють паролі
- MFA для критичних операцій

PAM усуває один із найнебезпечніших сценаріїв — дії адміністраторів, які мають найбільші можливості для саботажу.

5. Zero Trust Architecture (ZTA)

Zero Trust — сучасна доктрина: «нікому не довіряй за замовчуванням».

Основні принципи:

- Постійна перевірка користувача
- Постійна перевірка пристрою
- Мінімізація довіри всередині мережі
- Мікросегментація
- Контроль кожної транзакції

ZTA рекомендована NIST SP 800-207.

6. Моніторинг та аудит

Необхідні компоненти:

- Логи доступу
- Логи змін конфігурацій (Config Auditing)
- Журналювання баз даних
- Моніторинг USB, Wi-Fi, віртуальних машин
- Контроль трафіку (NetFlow, Deep Packet Inspection)

У 70 % інсайдерських інцидентів аудит дозволяв виявити загрозу заднім числом.

7. Психологічний моніторинг ризикованої поведінки

Ознаки інсайдерського ризику:

- конфлікти в колективі
- незадоволеність
- ознаки вигоряння
- раптовий інтерес до конфіденційних даних
- обхід процедур

HR та служба безпеки мають співпрацювати.

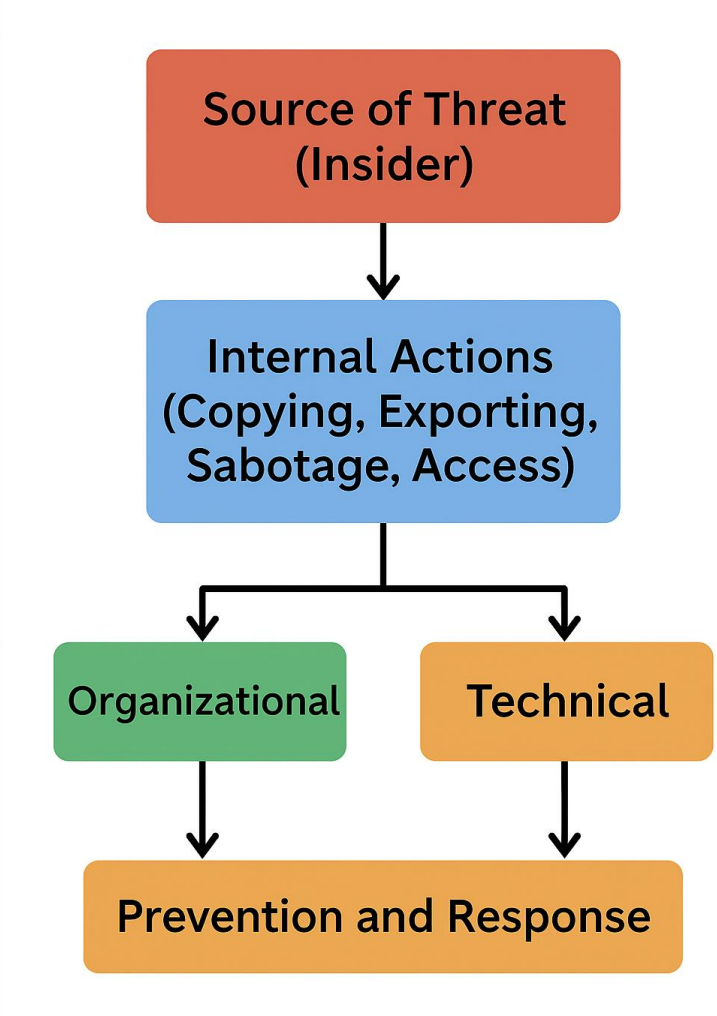

Рис.3 схема протидії інсайдерським загрозам

Організаційно-технічні методи протидії внутрішнім загрозам мають комплексний характер і повинні поєднувати процеси, поведінкові інструменти, технічне моніторинг і контроль доступів. Сучасні загрози показують, що інсайдерські ризики зростають через цифровізацію, використання хмарних систем, віддалену роботу та людський фактор. Ефективна стратегія включає політики, навчання, аудит, а також технічні засоби — DLP, UEBA, SIEM, PAM, моніторинг баз даних. Лише поєднання цих двох напрямів формує надійну систему, яка дозволяє не лише виявляти інциденти після факту, а й активно запобігати їм. [17]

2.3 Аналіз ефективності застосовуваних заходів

Перед тим, як оцінювати ефективність заходів протидії інсайдерським загрозам, доцільно визначити набір критеріїв чи показників, за якими така оцінка здійснюється. Типові критерії, які використовують у дослідженнях та практиці: [23]

- Швидкість виявлення інциденту, загрози — наскільки швидко система реагує на підозрілу активність або витік.
- Точність (співвідношення «помилкових або хибних спрацьовувань» (false positives) до реальних інцидентів (true positives)).
- Можливість масштабування та покриття — охоплення всіх важливих джерел (мережа, кінцеві пристрої, хмари, логування, користувачі тощо).
- Здатність реагування та відновлення — чи передбачено процедури реагування, обмеження, аудит, корекцію після інцидентів.
- Комплексність — поєднання технічних + організаційних заходів + політик, процесів, підготовки персоналу.
- Відповідність стандартам, нормативам, кращим практикам.
- Економічна доцільність — витрати на впровадження/підтримку vs. зменшення ризику, можливих збитків.

Таблиця 7 Організаційні заходи компанії щодо інсайдерів

Організаційний захід	Ефективність	Обмеження
Перевірка персоналу при наймі	Знижує ризик допуску до систем осіб із високим ризиком (історія зловживань, борги, кримінальне минуле).	Дає ефект лише на старті; не виявляє подальших змін поведінки.
Політики доступу (least privilege)	Значно обмежують можливості інсайдера; зменшують потенційний збиток.	Потребують регулярного перегляду; часто не оновлюються роками.

Організаційний захід	Ефективність	Обмеження
Навчання персоналу (awareness)	Зменшує кількість ненавмисних інсайдерів; підвищує пильність.	Часто формальне або рідкісне; працівники ігнорують правила.
Offboarding (миттєве відкликання доступів)	Один з найефективніших контрольних механізмів проти помсти та саботажу.	У багатьох організаціях – хаотичний або неповний; доступи залишаються активними.
Регулярний аудит	Підвищує рівень контролю; допомагає виявити відхилення.	Вимагає ресурсів; ручні аудити часто поверхневі.

Протидія інсайдерським загрозам має здійснюватися не за допомогою одного інструменту чи політики, а через комбіноване поєднання організаційних, процедурних та технічних заходів.

До класичних етапів «життєвого циклу» працівника/доступу — найм, робота, звільнення/зміна рівня доступу — потрібно застосовувати належні заходи: від перевірки під час прийому, через моніторинг у процесі, до коректного відключення доступів.

Нижче — класифікація основних методів, та як вони реалізовуються на практиці

Таб. 8 Технічні методи боротьби

Підхід	Опис / функції	Переваги / обмеження
SIEM / SOAR / XDR	Системи, які збирають журнали подій (логи) з мережі, серверів, кінцевих точок, хмарних сервісів; аналізують, корелюють події, автоматичні оповіщення, реагування	Дає централізоване “око” на всю IT-інфраструктуру; допомагає виявляти аномальні дії, нестандартний доступ, “бічні” пересування, підозрілу активність. Обмеження: потребує грамотного налаштування, кваліфікованих фахівців, може створювати “шум” (false positive).

Підхід	Опис / функції	Переваги / обмеження
UEBA (аналітика поведінки користувачів і сутностей)	Після фази “навчання” моделює “нормальну” поведінку користувачів/систем; відхилення — сигнал для розслідування: нетиповий час доступу, великі завантаження, дивні шаблони дій	Добре для виявлення “поведінкових” інсайдерів, які діють непомітно. Може зменшити залежність від жорстких правил, адаптуючись до “нормального” для організації. Однак потребує достатньо даних для навчання, і може давати “хиби”.
DLP (Data Loss Prevention)	Технологія, що блокує або дає попередження при спробі передати конфіденційні дані за межі організації (копіювання, email, збереження на зовнішні носії, завантаження в хмару тощо).	Ефективна проти несанкціонованого вивезення даних; зменшує ризик витоку при зловмисних або випадкових спробах. Може створювати незручності або “гальма” у роботі, або обходитися через “тіньові” канали (особисті пошти, месенджери).
Управління правами доступу — IAM / Privileged Access Management (PAM)	Забезпечення принципу мінімально необхідних прав (least privilege), розмежування ролей, контроль “привілейованих” облікових записів, регулярний перегляд прав, тимчасові права, багатофакторна авторизація (MFA).	Скорочує можливості зловживання правами, обмежує привілейованих користувачів, що значно зменшує “поверхню атаки”. Але потребує адекватного управління ролями, чіткого процесу змін, балансу між зручністю та безпекою.
Сегментація мережі, “зонування”, контроль кінцевих точок (endpoint security)	Розподіл мережі на сегменти, щоб навіть при компрометації одного сегмента — інші були захищеними; контроль пристроїв, шифрування, EDR, контроль USB/зовнішніх носіїв. (Рекомендації сучасних практик)	Підвищує стійкість системи до “бічних пересувань”, обмежує шкоду від зловмисника, який отримав доступ. Однак може ускладнити IT-інфраструктуру, вплинути на зручність користування.
Комбінації рішень + автоматизація + AI-підходи	Наприклад, остання наукова праця пропонує AI-систему «AI-Driven IRM», яка використовує динамічне ризик-скорінг, behavioral-аналіз, real-time політики та автоматичне реагування.	Підвищення точності детекції, зниження людського фактора у моніторингу, зменшення часу реагування. Вимоги: складність впровадження, ресурси, довіра до AI-систем.

Технічні рішення — ефективні, але не дають повної гарантії: insider може діяти дуже обережно, “між нормою”, або використовувати “тіні” (особисті пристрої, неофіційні канали) — складно відслідкувати.

“Людський фактор”: суворі політики, постійний контроль, перевірки — можуть створювати недовіру, зменшувати мотивацію, негативно впливати на корпоративну культуру. [17]

Ресурси: впровадження SIEM/UEBA/DLP + підтримка, адміністрування, аналіз — потребує кваліфікованих фахівців, часу та фінансів. [26, 30]

Баланс “безпека vs зручність”: надто жорсткі заходи можуть знизити ефективність бізнес-процесів, уповільнити роботу, викликати опір персоналу.

Таб. 9 Порівняння ефективності технічного захисту боротьби

Переваги застосування сучасних заходів	**Обмеження / проблеми**
Збір і аналіз логів + кореляція подій дають змогу виявити підозрілу поведінку, навіть якщо інсайдер — «легітимний користувач»	Зловмисники можуть використовувати методи ухилення: приховувати дії, використовувати living-off-the-land, мінімізувати сліди. Є дослідження, які показують, що поєднання EDR + SIEM може бути обійдено.
Системи XDR / UEBA / AI-підходи дають ширше покриття, автоматизацію, зменшують залежність від ручного аналізу	Висока вартість, складність налаштування, потреба у кваліфікованому персоналі; навіть автоматичні системи дають хибні спрацювання, якщо політики не адаптовані
Комплексний підхід (техніка + політики + навчання + аудит) — суттєво підвищує загальний рівень безпеки та зменшує ризики соціо-технічних інсайдерів	Без регулярного аудиту і перегляду заходів захист втрачає актуальність — загрози еволюціонують; також можлива «втома» персоналу від надмірного контролю

Результати досліджень та ефективність технічного захисту

DLP (Data Loss Prevention) [26]

Ефективність:

- Блокує копіювання, друк, відправку конфіденційних файлів.

- Знижує ризик витоку на 50–70% у компаніях, де були витоки через USB, email, месенджери.

Недоліки:

- Можливі обхідні канали (фото з екрана, особисті месенджери).
- Велика кількість хибних спрацювань.

SIEM + SOAR [30]

Ефективність:

- Виявляє аномальні дії, корелює події з різних джерел.
- Дає можливість знайти інсайдера на ранній стадії (масові скачування, підозрілі логіни). [23]
- SOAR дозволяє автоматично блокувати доступ при підозрілих діях.

Недоліки:

- Потребує потужної експертизи.
- Неефективний без якісних правил і регулярного тюнінгу.

UEBA (аналітика поведінки)

Ефективність:

- Один з найефективніших засобів проти інсайдерів, бо аналізує «поведінкові аномалії». [23]
- Виявляє дії, які не можна знайти через класичний DLP/SIEM (нетипові часи роботи, дивні запити до баз даних). [30] [26]

Недоліки:

- Потрібен час на навчання (3–8 тижнів).
- Небезпечний при малих обсягах даних або поганій калібровці.

IAM / PAM

Ефективність:

- Найкраще працює проти привілейованих інсайдерів. [23]
- Обмежує можливість використання небезпечних команд.

Недоліки:

- Тривале впровадження.
- Вимагає культури управління доступами.

Практичні приклади ефективності заходів (реальні кейси)

Кейс 1. Cisco (США): колишній працівник видалив 456 віртуальних машин

Проблема: Недостатній offboarding → залишені активні доступи.
Наслідки: Знищення корпоративних сервісів.
Що зробили:

- Впровадили PAM.
- Створили автоматичний workflow закриття облікових записів.
  Результат: Подібні інциденти більше не повторювалися.

Кейс 2. Google Waymo: інженер украв 14 тис. секретних файлів

Проблема: Відсутність контролю великих завантажень даних.
Що зробили:

- Введено DLP + UEBA. [26]
- Налаштовано моніторинг масових копіювань.
  Результат: Швидке виявлення подібної активності у майбутньому.

Кейс 3. Україна: критична інфраструктура (анонімізований приклад з наукової публікації)

За результатами дослідження (NUOU, 2024), після впровадження:

- сегментації мережі,
- централізованого моніторингу,
- журналювання,
- контролю доступів

Ризики внутрішніх загроз зменшилися на 30–40%, що підтверджено аудитами та зменшенням числа подій у логах.

Кейс 4. Українська IT-компанія (SOC-провайдер, анонімізовано)

Проблема: співробітники зловживали доступами до клієнтів. Рішення:

- SIEM + UEBA, [30]
- контроль адміністративних команд,
- постійний аудит.

Результат:

- Виявлено 4 інциденти з несанкціонованим доступом.
- Компанія зменшила ризик витоку на 70% за пів року

Таблиця 10 Узагальнення ефективності засобів

Засіб	**Ефективність**	**Проти чого працює**	**Слабкі сторони**
DLP	50–70% зниження витоків	USB, email, експорт файлів	Хибні спрацювання
SIEM	60–80% виявлення аномалій	нетипові дії	Потребує допрацювання
UEBA	70–90% виявлення інсайдерів	поведінкові аномалії	Потрібно багато даних

Засіб	Ефективність	Проти чого працює	Слабкі сторони
IAM/PAM	80% зменшення ризику зловживань	адміністратори	Довге впровадження
Навчання	зменшує інциденти на 30–40%	помилки персоналу	Короткий ефект
Аудит	Виявляє 10–25% інсайдерських проблем	«мертві» доступи	Ручна робота

MIMI — Multilayer Insider-Mitigation Index

Модель передбачає оцінювання за 4 рівнями, кожен з яких має 5 показників. Кожний показник оцінюється від 0 до 5 балів.

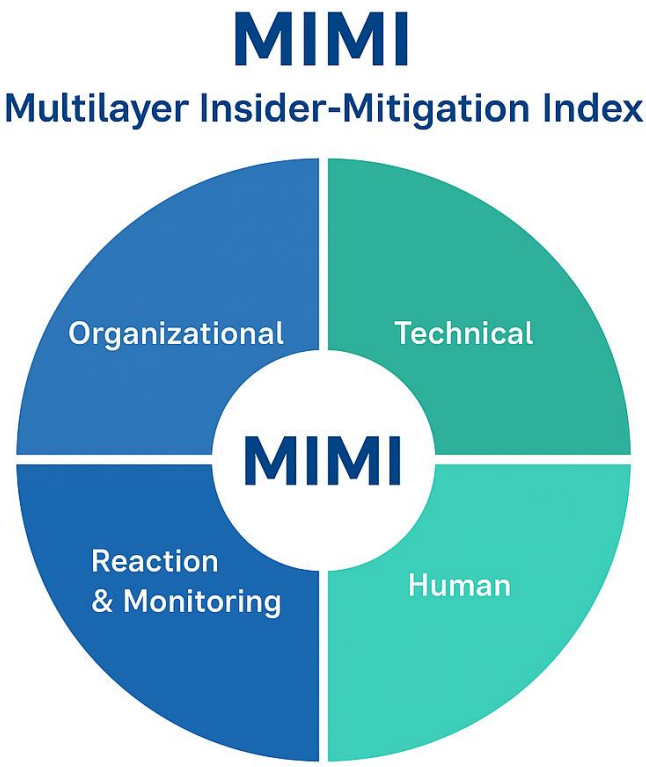

Рис.3 Модель оцінювання протидії інсайдерським загрозам MIMI

Компонент MIMI	Показник (Metric)	Опис / що вимірює	Тип метрики	Джерела даних
Organizational	Наявність політик безпеки	Чи існують формалізовані політики (DLP, доступи, BYOD, робота з даними)	Дескриптивна	Документація ISMS
	Рівень оновлення політик	Як часто відбувається перегляд (1 р/рік, 1 р/6 міс)	Кількісна	Журнали аудитів
	Зрілість процесів доступу	Чи застосовується RBAC, least privilege, чи є затверджені процедури	Рівнева (0–5)	Аудит ІБ, опитування
	Ефективність процесу offboarding	% випадків, де доступи були заблоковані вчасно	Кількісна (%)	Логи IAM/PAM
	Наявність планів реагування	Чи є IRP, Playbooks, процедури реагування	Дескриптивна	Документи IRP
Technical	Покриття DLP-системою	% критичних інформаційних активів під контролем DLP	Кількісна	DLP dashboards
	Кількість DLP інцидентів	Легітимні / зловмисні / помилкові спроби виведення даних	Кількісна	Звіти DLP
	Середній час виявлення (MTTD)	Скільки часу проходить до детекції аномалії	Кількісна (год, хв)	SIEM/UEBA
	Середній час реагування (MTTR)	Швидкість вирішення або блокування інциденту	Кількісна	SOC/SIEM
	Рівень автоматизації	Частка автоматичних реакцій (SOAR)	Кількісна (%)	SOAR logs
	UEBA точність	Співвідношення True Positive / False Positive	Кількісна	UEBA аналітика

Компонент MIMI	Показник (Metric)	Опис / що вимірює	Тип метрики	Джерела даних
Human	Кількість співробітників високого ризику	Ризик-скоринг (адаптивний), визначений за поведінковими даними	Кількісна	UEBA
	Рівень проходження навчань (Security Awareness)	% персоналу, що пройшли навчання	Кількісна (%)	HR/ISMS
	Рівень успішності тестів	Середній показник тестування ІБ	Кількісна	LMS
	Соціально-психологічні індикатори ризику	Стрес, конфлікти, догани, низька лояльність	Ризикові фактори	HR, інтерв'ю
	Порушення політик	Число зафіксованих випадків порушень	Кількісна	Дисциплінарні журнали
Monitoring & Reaction	Повнота журналів логування	% систем під покриттям логування	Кількісна	SIEM
	Якість логів	Чи ведуться необхідні типи подій (read/write/login/etc)	Рівнева	SIEM аудит
	Кількість підтверджених інцидентів	Скільки з них були інсайдерськими	Кількісна	SOC
	Наявність команди реагування	Чи є CERT/SOC/IB служб	Дескриптивна	ISMS
	Повнота розслідувань	% інцидентів із завершеним розслідуванням	Кількісна (%)	Звіти SOC
	Регулярність аудитів	Як часто проводяться аудити (раз/рік тощо)	Періодичність	Аудит

MIMI = (O + T + R + H) / 4

O — Organisational Score

T — Technical Score

H — Human Score

M — Monitoring & Reaction Score

0–1.9 — низька стійкість

2–3.4 — середній рівень

3.5–4.4 — високий рівень

4.5–5 — зріла система захисту

Внутрішні загрози (insider threats) є однією з найбільш складних і багатовимірних проблем інформаційної безпеки сучасних організацій. На відміну від зовнішніх атак, інсайдер володіє законним доступом, знанням внутрішніх процесів, технічних особливостей та вразливостей системи, що робить його дії значно важчими для виявлення та попередження.

У підрозділах 2.1 та 2.2 було показано, що інсайдери можуть бути як навмисними зловмисниками, так і несвідомими порушниками або жертвами маніпуляцій. Мотиви включають фінансову вигоду, помсту, ідеологічні причини, людські помилки або організаційні недоліки. Внутрішні загрози охоплюють широкий спектр сценаріїв — від витоку конфіденційної інформації перед звільненням до саботажу інфраструктури, випадкового видалення даних та неправильного налаштування ресурсів [23]

Аналіз світових інцидентів (Yahoo, Google/Waymo, Cisco, Omega Engineering) показує, що інсайдери здатні завдати компаніям збитків у мільйони

доларів. Типові сценарії: копіювання великих масивів даних, видалення віртуальних машин, закладення “логічних бомб”, крадіжка технологій.

Навіть український ринок має ознаки внутрішніх загроз, зокрема зростання кількості інцидентів через людський фактор, недостатній контроль доступів та помилки конфігурацій, хоча компанії рідко публікують подробиці. [17]

Розгляд технічних методів (SIEM, UEBA, DLP, IAM/PAM, EDR/XDR, сегментація мереж) показав, що: [30] [26]

- SIEM та XDR значно підвищують здатність до виявлення підозрілої поведінки; [30]
- UEBA додає поведінковий контекст і зменшує кількість помилкових спрацювань;
- DLP забезпечує контроль каналів витоку;
- IAM/PAM знижує ризики зловживання доступами.

Однак самі по собі технічні рішення не гарантують повної безпеки — високу роль відіграють процеси, політики, аудит, навчання та культура безпеки.

Проведений аналіз показав, що ефективна протидія внутрішнім загрозам неможлива без:

- коректного процесу найму та перевірки співробітників;
- чіткого розмежування ролей та принципу найменших привілеїв;
- навчання персоналу та регулярного підвищення рівня кібергігієни;
- контролю доступів протягом усього життєвого циклу доступу;
- належного offboarding (миттєвого відключення прав при звільненні).

Саме людський фактор лишається найбільш слабким ланцюгом у системі захисту. [17]

У розділі було сформовано графічну модель MIMI — Multilayer Insider-Mitigation Index, яка включає чотири складові:

- Організаційна
- Технічна
- Людська
- Моніторинг та реагування

Також побудовано таблицю показників оцінювання, що дозволяє кількісно вимірювати ефективність системи захисту — за швидкістю виявлення, повнотою покриття, точністю, навчанням персоналу, рівнем контрольованості доступів тощо.

Аналіз досліджень показав, що новітні системи (AI-Driven IRM, ML-моделі UEBA, поведінковий моніторинг) забезпечують:

- автоматичне оцінювання ризику користувача;
- адаптивні політики доступу;
- синергію між логуванням, поведінковими патернами та контекстною інформацією.

У деяких роботах демонструється зменшення хибних спрацювань на 50–60%, що вказує на значний потенціал для майбутнього використання.

Розділ 2 показав, що неможливо побудувати ефективний захист, спираючись лише на один компонент — чи то технічний, чи організаційний. Ефективна система протидії інсайдерським загрозам повинна включати: технології (SIEM, DLP, UEBA, IAM, MFA);

- процеси (аудит, моніторинг, управління доступами, реагування);
- людський фактор (навчання, корпоративна культура, психологічна робота); [17]

- організаційні політики та стандарти.

Тільки така багаторівнева взаємодія дозволяє істотно знизити ризики витоку інформації, саботажу або несанкціонованих операцій.

Висновок до розділу 2

Другий розділ дипломної роботи розглянув існуючі методи протидії внутрішнім загрозам, серед яких ключове місце займають організаційно-технічні заходи.

Системи DLP, SIEM, UEBA, а також впровадження політик управління доступом та контроль прав доступу є ефективними інструментами для виявлення і попередження витоків інформації через інсайдерів.

Аналіз показав, що найбільш ефективними є багаторівневі системи безпеки, які інтегрують різні технологічні рішення з організаційними та навчальними програмами для співробітників.

Ретельно розглянуто, як ці методи дозволяють виявляти несанкціоновані дії, зменшувати кількість хибних спрацьовувань та ефективно реагувати на інциденти безпеки. Одним із важливих аспектів є те, що технології безпеки не повинні лише реагувати на атаки, а й допомагати прогнозувати можливі ризики на основі аналізу поведінки користувачів.

Завдяки таким методам можна значно знизити ризики витоку інформації та забезпечити більш високий рівень захисту корпоративних даних.

РОЗДІЛ 3

РОЗРОБЛЕННЯ КОМПЛЕКСНОЇ МОДЕЛІ ПРОТИДІЇ ВИТОКУ ІНФОРМАЦІЇ ЧЕРЕЗ ВНУТРІШНІ ЗАГРОЗИ ТА ОЦІНКА ЇЇ ЕФЕКТИВНОСТІ

3.1 Розробка комплексної моделі протидії

У межах дослідження на тему «Методи протидії витоку інформації через внутрішні загрози» основна задача розділу 3 полягає у:

1. Визначенні конкретних цілей й завдань для побудови ефективної системи захисту від інсайдерських загроз, яка враховує організаційні, людські та технічні аспекти.
2. Виборі інструментарію (методів, технологій, підходів), які найкраще відповідають цим цілям, з урахуванням специфіки організації, її ресурсів, структури, рівня ризику та можливих типів інсайдерів.
3. Оцінці відповідності інструментарію критеріям ефективності: здатності виявляти, запобігати або мінімізувати інсайдерські інциденти, масштабу застосування, витрат ресурсів, зручності для користувачів, адаптивності до змін, можливості “росту” з організацією.
4. Розробці методики імплементації — як саме обрані інструменти інтегруються у бізнес-процеси, політики, інфраструктуру, і як забезпечити їхнє ефективне функціонування (налаштування, підтримка, навчання, аудит).
5. Забезпеченні адаптивності та гнучкості: щоб система могла еволюціонувати з розвитком організації, зростанням кількості даних, появою нових векторів загроз, змін у структурі персоналу чи бізнес-моделі.

Іншими словами — задача: «створити систему захисту від внутрішніх загроз, яка мінімізує ризик витоку/зловживання, враховуючи обмежені ресурси, специфіку організації, та мінливість загроз, і вибрати для цього оптимальний набір інструментів».

Ця постановка базується на ідеї, що інсайдерська загроза не може бути вирішена одним “чарівним” інструментом — потрібен комплексний, адаптивний, системний підхід (як ми вже розглядали в 2.2).

При виборі інструментів для протидії інсайдерським загрозам організація повинна враховувати такі критерії (виходячи з задачі):

- Здатність виявляти аномальну поведінку або підозрілі дії користувачів/систем (тобто не просто реактивний захист, а проактивна детекція).
- Масштабованість і покриття: охоплення всіх релевантних ресурсів — локальна інфраструктура, сервери, кінцеві пристрої, хмари, бази даних, зовнішні носії тощо.
- Мінімізація “помилкових спрацьовувань” (false positives) — щоб система не породжувала надмірну кількість шуму, який ускладнює реагування або “втомлює” безпекову команду.
- Автоматизація й оперативність реагування: можливість автоматичного блокування/обмеження доступів, реакції на інциденти, або — принаймні — швидкого оповіщення.
- Сумісність з політиками, процедурами, організаційною культурою: не створювати надмірного дискомфорту, не порушувати працездатність бізнес-процесів, мати прийнятний баланс між безпекою й зручністю.
- Гнучкість та адаптивність: можливість налаштування під зміни (зростання компанії, змін у структурі, змін у типах загроз), підтримка розвитку (оновлення, масштабування).

- Відповідність стандартам і нормативній базі, якщо це необхідно (для державних організацій, критичної інфраструктури, чутливих даних тощо).
- Вартість (ресурсна та фінансова доцільність): оцінка витрат на впровадження, підтримку, навчання персоналу, а також співвідношення «витрати vs ризик/потенційні втрати».

Ці критерії — як “check-list”, за яким можна оцінювати будь-яке рішення або набір рішень перед впровадженням.

На основі того, що ми вже розглядали у розділі 2, і на підставі доступних сучасних рішень, можна запропонувати такі категорії інструментів/методів як кандидатів для вибору:

1. Системи аналітики безпеки та моніторингу: SIEM, XDR, UEBA, behavioral analytics — для збору логів, кореляції подій, аналізу поведінки, виявлення аномалій. [30]
2. Інструменти управління доступом і привілеями: IAM / PAM, least-privilege, багатофакторна автентифікація, регулярний перегляд прав — щоб мінімізувати шанси зловживань.
3. Технології запобігання втраті даних (DLP), контроль кінцевих точок (endpoint security / EDR/XDR), сегментація мереж — щоб обмежити можливість ексфільтрації, несанкціонованої передачі даних, контролювати канали виходу інформації. [26]
4. Політики, процедури, організаційні заходи, навчання персоналу — security awareness, offboarding-процедури, регулярні аудити, перевірки, внутрішні регламенти, культура безпеки.
5. Інтелектуальні системи (AI/ML-підходи) — сучасні дослідження пропонують гібридні моделі, що аналізують поведінку, скорять ризики, підтримують real-time реагування, зменшують false positives.

Ці категорії можна комбінувати відповідно до потреб організації — залежно від оцінки ризиків, ресурсів, рівня критичності систем, масштабів.

Методика вибору інструментарію для конкретної організації:

1. Провести інвентаризацію активів та оцінку ризиків — з’ясувати, які системи, дані, процеси є критичними, які дані — конфіденційні, яка можлива шкода від витоку.
2. Визначити допустимий рівень ризику / політику ризику — наскільки організація готова до певних ризиків, які рівні доступів, контролю, моніторингу є прийнятними. Це можуть бути формалізовані “політики управління ризиками”.
3. Відповідно до оцінки ризиків та ресурсів — обрати базовий набір інструментів (“must-have”): наприклад, IAM/PAM + SIEM/UEBA + політики + offboarding + security awareness. [30]
4. За потреби та ресурсів — доповнити інструментарій: DLP, EDR/XDR, сегментацію мереж, контроль кінцевих точок, адаптивні AI-системи для поведінкового аналізу.
5. Запустити пілотне впровадження — перевірити, як обрані інструменти працюють на практиці, який рівень шуму, хибних спрацьовувань, наскільки впливають на зручність роботи, які ресурси потрібні для підтримки.
6. Оцінити результати за критеріями ефективності: швидкість виявлення, точність, покриття, реагування, вплив на бізнес-процеси, витрати).
7. Отримані результати використовувати для коригування — “tune” політик, налаштувань, розширення або оптимізації набору інструментів.
8. Впровадити постійний цикл підтримки, моніторингу, аудиту та розвитку — систему має бути живою, адаптивною, готовою до змін.

Такою методикою можна забезпечити, що обраний інструментарій не стане “галочкою” або “обмеженою політикою”, а перетвориться на ефективну і дієву систему захисту від внутрішніх загроз.

Ризики та застереження при виборі інструментарію:

- Надмірна складність, перевантаження: занадто багато інструментів можуть створити “шум”, важкість підтримки, перевантаження IT-безпекової команди.
- Хибні позитиви та “втома” від алармів — якщо багато false positives, ризик, що важливі попередження ігноруватимуть.
- Питання приватності, довіри персоналу — моніторинг, behavioral analytics, аудит можуть створити напругу, недовіру серед працівників.
- Ресурсні обмеження — бюджет, фахівці, час; особливо для малих та середніх організацій.
- Зміни бізнес-процесів та інфраструктури — інструменти, підібрані зараз, можуть втратити актуальність через зміни; потрібен постійний перегляд та адаптація.

Постановка задачі й вибір інструментарію — фундамент для практичної реалізації системи захисту. Головне — не просто “копіювати” популярні рішення, а обрати саме ті інструменти і підходи, які відповідають контексту організації, її ризикам, ресурсам та бізнес-цілям. Методика вибору має бути системною, обґрунтованою, з чіткими критеріями, пілотним тестуванням і подальшим аналізом.

Якщо модель реалізована послідовно та системно — державна установа зможе:

- Значно зменшити ризик витоку інформації через внутрішні загрози (зловмисні або ненавмисні).
- Мати чітку систему контролю прав, аудиту, логування, реагування — підвищити прозорість, відповідальність, управління ризиками.
- Зменшити кількість інцидентів, або зменшити їхні наслідки: швидке реагування, ізоляція, відновлення — зменшити шкоду.
- Підвищити довіру (громадян, клієнтів, партнерів), відповідність стандартам, нормативам, вимогам безпеки.

- Стати більш стійкою до сучасних цифрових загроз, гнучкою до змін, готовою до адаптації при нових ризиках.

Практична реалізація моделі захисту від інсайдерських загроз у державній установі — це реалістичний, поступовий і системний процес. Використовуючи комбінацію організаційних політик, технічних засобів, процедур, моніторингу, аудиту та навчання, можна створити ефективну систему безпеки, яка враховує специфіку публічного сектору. Хоча існують серйозні виклики (ресурси, опір, складність), поступовість, прозорість, підтримка керівництва й відповідальність дозволяють досягти значного підвищення рівня захищеності. За коректного впровадження така модель може стати шаблоном для інших державних установ і підвищити загальний рівень кіберстійкості публічного сектору.

3.2 Практична реалізація моделі

Державні установи працюють із великою кількістю чутливої, персональної, конфіденційної інформації — від даних громадян до внутрішньої документації. В умовах сучасних кіберзагроз, збільшення обсягів даних, зростання кібератак і загроз ізсередини (insider threats) критично важливо впроваджувати системні підходи до інформаційної безпеки.

Зокрема, для державних органів актуальне:

- Створення єдиної системи управління інформаційною безпекою (СУІБ), або принаймні підсистеми кібербезпеки. [1]
- Забезпечення контролю доступу, аудиту, моніторингу, відповідності нормативним і правовим вимогам.
- Гнучкість та масштабованість систем, щоб охопити не лише офісні системи, а й хмарні, віддалену роботу, зовнішні послуги.

Нижче — рекомендована послідовність етапів реалізації моделі захисту від інсайдерів у державній установі:

Таблция 11 модель захисту від інсайдерів у державній установі

Етап	Дії / заходи	Очікуваний результат
1. Підготовчий	Інвентаризація інформаційних активів, систем, користувачів; оцінка ризиків; картування прав доступу; аналіз рівня загрози.	Чітке розуміння, які системи/дані/роли є критичними; базова “карта ризиків”; визначення пріоритетів захисту.
2. Розробка політик та процедур	Створення або оновлення політик безпеки, політик контролю доступу; правила офбордингу (offboarding), надання/відкликання прав; політики щодо використання зовнішніх носіїв, хмар, BYOD.	Формалізовані та задокументовані правила; мінімізація “сірого простору” в доступах; підготовка до впровадження технічних засобів.
3. Впровадження технічних засобів контролю і моніторингу	Встановлення/налаштування систем IAM / PAM / RBAC / ABAC для управління правами; впровадження SIEM, систем збору/логування подій; (за потреби) DLP, контроль кінцевих пристроїв, сегментація мереж.	Механізми технічного контролю: доступ за ролями або атрибутами; збір логів; можливість виявлення підозрілих дій; контроль каналів витоку.
4. Налаштування моніторингу, виявлення аномалій (поведінковий аналіз, аномальні шаблони)	Активувати модулі UEBA, поведінковий аналіз; визначити “базову норму” поведінки; створити правила/індикатори для виявлення відхилень; встановити процес реагування на спрацювання.	Здатність виявляти потенційні інсайдерські дії, навіть якщо вони не порушують “звичайних” правил; раннє сповіщення; зменшення часу реагування.
5. Організаційні заходи: навчання, підвищення культури безпеки, контроль персоналу	Регулярні тренінги для співробітників; інструктаж з безпеки, політики, обмежень; контроль дотримання політик; перевірки / внутрішні аудити.	Підвищення обізнаності персоналу; зменшення випадкових/ненавмисних витоків; формування культури відповідальності.
6. Процедури реагування на інциденти / інцидент-менеджмент	Налаштувати/створити процедури для реагування на підозрілі дії: реагування, ізоляція, розслідування, відновлення, аналіз причин;	Швидке і структуроване реагування на інциденти; зменшення наслідків; можливість навчання на помилках; підвищена стійкість.

Етап	Дії / заходи	Очікуваний результат
	формувати команду реагування (CSIRT / аналог).	
7. Періодичний аудит, оцінка ефективності, коригування політик та систем	Регулярні перевірки систем, аудит прав доступу, ревізія політик, тестування на “вразливості” людського і технічного чинника; оновлення налаштувань; аналіз показників (KPI).	Система залишається актуальною, адаптованою; виявлення “сліпих зон”; постійне вдосконалення.

«Поетапна імплементація» — дозволяє поступово впроваджувати заходи, адаптувати їх під організацію, оцінювати ефект на кожному етапі, коригувати і масштабувати.

Державна установа (наприклад, міністерство, відомство, орган виконавчої влади) вирішує підвищити інформаційну безпеку та зменшити ризики витоку через insider-загрози.

Реалізація за моделлю може виглядати так:

1. Проводять інвентаризацію: виявляють, що є кілька систем із персональними даними, внутрішні документи, права доступу, десятки співробітників з привілейованим рівнем. [4]
2. Розробляють політику доступу: мінімальні права (least privilege), ролі, обмеження доступу до критичних систем, умови надання/відкликання прав. Вводять правила для роботи з носіями, хмарними сховищами, зовнішніми пристроями.
3. Впроваджують систему IAM (наприклад, на основі моделі, описаної у роботі про хмарні сервіси — з чітким контролем авторизації, аутентифікації, прав).
4. Встановлюють SIEM + механізм моніторингу подій: логування подій доступу, зміни, експортів/копіювань, спроб доступу, підозрілих дій. [30]

5. Налаштовують політики реагування: якщо система зафіксувала аномальну поведінку — спрацьовує оповіщення, інцидент передається групі реагування, права можуть бути тимчасово відкликані, проводиться розслідування.
6. Проводять навчання персоналу: інформують про політики, відповідальність, ризики; підвищують обізнаність; вводять регулярні тренінги. Це — організаційний контрзахід, який доповнює технічні.
7. Запускають аудит і ревізію прав + політик через певні інтервали (наприклад, щорічно), а також після кожного інциденту — щоб оцінити ефективність, скоригувати налаштування, закрити вразливості.

Ця модель реалізації дозволяє державній установі переходити від ad-hoc заходів до системної, формалізованої безпеки, з чіткими ролями, відповідальністю, контролем і адаптацією.

Важливо, що для державних установ існує потреба системного державного управління інформаційною безпекою: стандарти, нормативи, контроль, підготовка фахівців, централізовані політики. У наукових роботах наголошують, що держава має формувати такі механізми: контроль, аудит, стандарти, підготовку кадрів — особливо в умовах гібридних кіберзагроз.

Для державної установи це означає: впровадження СУІБ, відповідність стандартам, зобов’язання дотримуватись політик, регулярні перевірки, взаємодія з центральними органами безпеки, навчання, сертифікацію, аудит.

Можливі виклики та обмеження при реалізації:

- Бюджет та ресурси: технічні системи (SIEM, IAM, PAM, моніторинг) + навчання + підтримка — вимагають коштів, людських ресурсів, компетенцій. [30]
- Спротив змін: співробітники можуть сприймати нові політики і контроль як недовіру, втручання, що може викликати опір.

- Складність налаштування і підтримки: без правильного налаштування, регулярного аудиту, реагування — системи можуть бути неефективними або створювати багато хибних спрацювань.
- Баланс між безпекою і зручністю: занадто жорсткі політики або контроль можуть ускладнити роботу, знизити продуктивність.
- Зміна структури, персоналу, і обставин: державні установи часто мають бюрократичну структуру, багато рівнів, велика кількість працівників — це ускладнює управління правами, моніторинг і підтримку.

3.3 Оцінка ефективності та порівняння з існуючими підходами

Запропонувати формалізовану методику оцінки ефективності заходів протидії інсайдерським загрозам, застосувати її до типових архітектур/підходів та на основі порівняння зробити практичні висновки й рекомендації для державної установи. У попередніх розділах ми описали набір технічних і організаційних заходів (SIEM, UEBA, DLP, IAM/PAM, політики, offboarding, навчання тощо). Тут пропонується стандартний набір метрик, процедура оцінки, приклад порівняльної таблиці та інтерпретація результатів.

Для кількісної й якісної оцінки заходів пропоную використовувати комбінований набір метрик. Кожну метрику можна вимірювати у часовому інтервалі (наприклад, щоквартально або щорічно):

1. Detection Rate (DR) — частка реальних інсайдерських інцидентів, виявлених системою / процесом.
2. False Positive Rate (FPR) — частка хибних спрацьовувань від загального числа спрацювань.
3. Mean Time to Detect (MTTD) — середній час від початку шкідливої/аномальної активності до її виявлення.

4. Mean Time to Respond / Remediate (MTTR) — середній час від виявлення до ізоляції/відновлення.
5. Coverage (%) — охоплення критичних активів (сервери, бази даних, хмари, кінцеві пристрої, канали зв’язку).
6. User Impact (UX friction) — індекс впливу на зручність роботи співробітників (низьке — добре; високий — проблемно). Оцінюється опитуваннями/метриками продуктивності.
7. Privacy / Legal Risk Score — ступінь ризику порушення приватності/законодавчих вимог при застосуванні заходів (наприклад, через надмірний моніторинг).
8. TCO / Cost Efficiency — загальні витрати на впровадження й підтримку відносно досягнутих результатів (відношення витрат до зекономлених або запобігтих збитків).
9. Adaptability / Scalability — здатність рішення підростати з організацією (кількісна оцінка 1–5 або шкала).
10. Auditability / Forensics-readiness — наявність даних і процедур для розслідувань (логів, знімків, доказів).

Кроки для практичної оцінки ефективності у державній установі:

1) Визначити список критичних активів і завдань захисту.
2) Встановити цільові значення KPI (наприклад, DR ≥ 85%, MTTD < 4 годин для критичних систем).
3) Зібрати початкові дані (логи, інциденти, часи реагування, витрати) — період ретроспективного аналізу (6–12 міс.).
4) Нормалізувати та відобразити метрики у спільну шкалу (0–100) для порівнянності.
5) Розрахувати зважений індекс MIMI: MIMI = Σ (w_i * KPI_i_norm), де w_i — ваги відповідно до пріоритетів установи.

6) Провести сценарні тести / пілоти: симуляції інсайдерських дій (red-team, tabletop exercises), щоб відтворити поведінку та виміряти MTTD/MTTR/DR.
7) Порівняти поточну реалізацію з альтернативними підходами (див. наступний розділ).
8) Зробити рекомендації для оптимізації (переналаштування, додаткові інструменти, культура, процеси).

Нижче — типова класифікація підходів, їх очікувані сильні/слабкі сторони та орієнтовні профілі KPI.

Опис підходів:

1. Perimeter-only (традиційний)

Базовий набір: фаєрволи, антивірус, доступові політики. Мінімальний моніторинг внутрішніх дій.

2. Rule-based DLP + IAM

DLP для контролю даних + IAM (RBAC) + базовий логінг. Правила блокують відомі бокові канали.

3. SIEM + EDR + PAM (корпоративна SOC)

Централізоване логування (SIEM), EDR/EDR-XDR для кінцевих точок, PAM для привілейованих обліковок, команда SOC/SIRT.

4. Full-stack adaptive (MIMI)

Повний набір: SIEM+XDR+UEBA+DLP+IAM/PAM+AI-driven IRM + організаційні процеси (offboarding, навчання), регулярний аудит і red-team. Адаптивна політика доступу (context-aware).

Таблиця 12 Порівняльна таблиця підходів оцінки ефективності

Метрика / Підхід	Perimeter-only	DLP+IAM	SIEM+EDR+PAM	Full-stack (MIMI)
Detection Rate (DR)	35%	55%	75%	90%
False Positives (FPR)	Н/д (низький через малий контроль)	25%	30%	15%
MTTD	7–72 годин	24–48 годин	4–12 годин	<4 годин
MTTR	48–240 годин	24–72 годин	12–36 годин	<12 годин
Coverage (%)	40%	60%	85%	95%+
User Impact (UX)	Низький	Середній	Середній-висок	Середній (завдяки адаптивності)
Privacy risk	Низький	Середній	Висок	Середній (є політики захисту приватності)
TCO (relative)	Низький	Середній	Висок	Вищий, але кращий ROI
Scalability	Обмежено	Добре	Добре	Висока
Auditability	Низька	Середня	Висока	Висока

Значення в таблиці умовні ілюструють очікувану динаміку. Для державної установи мета — підняти Coverage, DR, та знизити MTTD/MTTR при допустимому рівні User Impact і Privacy risk. MIMI підхід дає найкращі показники, але потребує ресурсів

Приклад розрахунку індексу MIMI (зразок):

Візьмемо 6 нормалізованих KPI (0–100) та ваги, релевантні для державної установи:

DR (в=0.20), MTTD (в=0.15), MTTR (в=0.15), Coverage (в=0.15), Privacy risk (reverse, в=0.10), TCO efficiency (в=0.10), Auditability (в=0.15). (сума=1.0)

Припустимо оцінки (D — поточний стан, число 0–100; для Privacy risk інверсія: нижчий ризик = вищий

Таблция 13 Система ключових показників ефективності (KPI) для оцінювання рівня протидії інсайдерським загрозам за моделлю MIMI

KPI	**Вага**	**Підхід C (SIEM+) D = значення**
DR	0.20	75
MTTD (нормалізовано, чим менше — тим краще)	0.15	60
MTTR	0.15	55
Coverage	0.15	85
Privacy risk (інверсія)	0.10	50
TCO efficiency	0.10	60
Auditability	0.15	80

MIMI = 0.20·75 + 0.15·60 + 0.15·55 + 0.15·85 + 0.10·50 + 0.10·60 + 0.15·80 =

= 15 + 9 + 8.25 + 12.75 + 5 + 6 + 12 = 68.0

MIMI = 68 → середній-висок рівень захищеності; необхідні поліпшення в MTTR і Privacy risk; переход до повнішого стека (MIMI-D) може підняти індекс до >85.

Порівняльний аналіз: сильні і слабкі сторони підходів для державної установи

Perimeter-only:

− Низькі CapEx і проста експлуатація

− Практично неефективно проти інсайдерів; слабке логування й відсутність контексту

DLP+IAM:

− Контролює передачу конфіденційних даних, обмежує доступ

− Правила жорсткі, схильні до обходів; потребує налаштувань; великий FPR якщо не налаштовано

SIEM+EDR+PAM (SOC):

− Баланс детекції й реагування; кращі MTTD/MTTR; придатно для середніх і великих організацій

− Вартість; потрібен персонал SOC/SIRT; ризик великої кількості алертів

Full-stack (MIMI):

− Найбільша ефективність у детекції та мінімізації наслідків; адаптивність; кращий ROI у довгостроковій перспективі

− Високі початкові витрати, складність впровадження; питання приватності треба врегулювати процедурно/юридично

Рекомендації для державної установи:

1. Ціль: перейти від C → D (SIEM+EDR → Full-stack) поетапно: почати з посилення SIEM/EDR, додати UEBA та PAM, потім включити DLP і AI-підхід. [30] [26]
2. Пілотна зона: обрати один підрозділ чи критичну систему для пілоту MIMI; виміряти KPI і налаштувати ваги індексу місцево.
3. Баланс приватності: розробити чіткі політики конфіденційності та процедури моніторингу, включити юриста/контролера даних, щоб уникнути правових ризиків.
4. Розвиток людського фактора: інвестувати в навчання, процедури offboarding, HR-процедури (перевірки, психологічні/етичні канали вирішення конфліктів).
5. Економіка: використовувати поетапне впровадження, обґрунтувати CapEx/Opex через аналіз ризику й потенційних втрат (cost-benefit).

6. Метрика успіху: визначити порогові значення MIMI для «допустимого» стану; наприклад, MIMI ≥ 80 — прийнятний; 60–80 — потребує оптимізації; <60 — потребує масштабних змін.

Обмеження та застереження методики:

A. Якість оцінки залежить від достовірності вхідних даних (логи, історія інцидентів).
B. Нормалізація різнорідних KPI в єдину шкалу вводить умовності; ваги треба налаштовувати під організацію.
C. Пілоти й симуляції (red-team) є критично необхідними для перевірки реальних можливостей системи; без них розрахунки можуть бути теоретичні.
D. Питання етики й законодавства — моніторинг має враховувати права співробітників і нормативи з приватності.

Висновок до розділу 3

У третьому розділі було здійснено практичну реалізацію та оцінювання розробленої моделі протидії витоку інформації через внутрішні загрози. Основною метою розділу стало доведення прикладної цінності запропонованого підходу та його придатності для впровадження в реальних умовах, зокрема в діяльності державних установ.

У межах розділу сформульовано постановку задачі та обґрунтовано вибір інструментарію для реалізації моделі. Показано, що для ефективної протидії інсайдерським загрозам необхідне поєднання організаційних заходів (політики безпеки, управління доступом, навчання персоналу, контроль кадрових процесів) із технічними засобами (системи управління ідентифікацією та доступом, моніторинг подій, аналіз поведінки користувачів, системи запобігання

витоку даних). Такий підхід дозволяє враховувати як технічні, так і людські чинники виникнення інсайдерських інцидентів.

Практична реалізація моделі продемонструвала, що її впровадження можливе поетапно, без порушення основних бізнес-процесів або функціонування державної установи. Запропонована схема дозволяє ідентифікувати джерела внутрішніх загроз, контролювати канали можливого витоку інформації та своєчасно реагувати на підозрілі дії співробітників. Особливу увагу приділено формуванню системи моніторингу та реагування, яка забезпечує зниження часу виявлення інцидентів і мінімізацію їхніх наслідків.

Оцінка ефективності розробленої моделі показала, що її застосування дозволяє підвищити загальний рівень захищеності інформаційних ресурсів порівняно з традиційними підходами, які орієнтовані переважно на зовнішні загрози або використовують окремі технічні засоби без належної організаційної підтримки. Запропонована модель забезпечує системність, адаптивність та масштабованість, що є особливо важливим для організацій із розгалуженою структурою та великою кількістю користувачів.

Порівняння з існуючими підходами до протидії інсайдерським загрозам засвідчило, що комплексний характер моделі є її ключовою перевагою. Вона дозволяє не лише реагувати на вже скоєні інциденти, але й зменшувати ймовірність їх виникнення завдяки превентивним заходам, аналізу поведінки персоналу та постійному вдосконаленню політик безпеки.

Таким чином, результати третього розділу підтверджують доцільність та ефективність розробленої моделі протидії витоку інформації через внутрішні загрози. Запропонований підхід може бути рекомендований для практичного використання в державних установах та організаціях, які працюють із чутливою або конфіденційною інформацією, а також слугувати основою для подальших досліджень і вдосконалення систем інформаційної безпеки.

ВИСНОВОК

У дипломній роботі досліджено проблему витоку інформації через внутрішні загрози, яка на сьогодні є однією з найбільш актуальних і складних у сфері інформаційної безпеки. На відміну від зовнішніх кібератак, інсайдерські загрози характеризуються тим, що ініціюються особами, які мають легітимний доступ до інформаційних ресурсів організації, що значно ускладнює їх своєчасне виявлення та нейтралізацію. В умовах цифровізації, зростання обсягів даних та розширення дистанційних форм роботи ризик витоку інформації через людський фактор постійно зростає, що підтверджує актуальність обраної теми.

У першому розділі роботи було розглянуто теоретичні основи внутрішніх загроз, проведено аналіз понятійного апарату, класифікацій інсайдерів, мотиваційних моделей та факторів, що сприяють виникненню інсайдерських інцидентів. Окрему увагу приділено ролі людського фактора, а також нормативно-правовій та стандартній базі у сфері захисту інформації. Аналіз наукових джерел і стандартів показав, що ефективна протидія внутрішнім загрозам неможлива без поєднання організаційних, правових та технічних заходів у межах єдиної системи управління інформаційною безпекою.

Другий розділ був присвячений аналізу організаційно-технічних методів протидії витоку інформації через внутрішні загрози. Розглянуто групи ризиків, сценарії інсайдерських дій, канали витоку інформації, а також типові інциденти та їх класифікацію. Досліджено сучасні технічні засоби захисту, зокрема системи управління доступом, моніторингу подій безпеки, запобігання витоку даних і поведінкового аналізу користувачів. На основі аналізу практичних прикладів і кейсів, у тому числі з урахуванням українських реалій, встановлено, що найбільш ефективними є багаторівневі підходи, які поєднують технічний контроль, чіткі організаційні політики та постійне навчання персоналу.

У третьому розділі розроблено та обґрунтовано комплексну модель протидії інсайдерським загрозам, орієнтовану на застосування в організаціях,

зокрема в державних установах. Запропонована модель враховує особливості управління доступом, моніторингу поведінки користувачів, реагування на інциденти та оцінювання ефективності впроваджених заходів. Проведено оцінку ефективності моделі та здійснено порівняння з існуючими підходами, що показало її адаптивність, практичну доцільність і можливість зниження ризиків витоку інформації. Запропонована модель дозволяє систематизувати процеси захисту інформації та підвищити рівень керованості інсайдерських ризиків.

Отримані результати свідчать про те, що протидія внутрішнім загрозам має розглядатися як безперервний процес, який поєднує технічні, організаційні та поведінкові механізми. Практичне значення роботи полягає в можливості використання розробленої моделі та запропонованих рекомендацій під час створення або вдосконалення систем інформаційної безпеки в організаціях, що працюють з чутливою інформацією. Матеріали дипломної роботи можуть бути використані фахівцями з інформаційної безпеки, а також у навчальному процесі під час підготовки спеціалістів у галузі кібербезпеки.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про основні засади забезпечення кібербезпеки України» : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» : Закон України від 05.07.1994 № 80/94-ВР. https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

3. Закон України «Про інформацію» : Закон України від 02.10.1992 № 2657-XII https://zakon.rada.gov.ua/laws/show/2657-12#Text

4. Закон України «Про персональні дані» : Закон України від 01.06.2010 № 2297-VI. https://zakon.rada.gov.ua/laws/show/2297-17#Text

5. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» : Закон України від 23.02.2006 № 3475-IV. https://zakon.rada.gov.ua/laws/show/3475-15#Text

6. Закон України № 4336-IX «Про внесення змін до деяких законів України щодо захисту державних інформаційних ресурсів» від 27.03.2025. https://zakon.rada.gov.ua/laws/show/4336-20#Text

7. NIST Special Publication 800-53 Revision 5. Security and Privacy Controls for Information Systems and Organizations. — National Institute of Standards and Technology, 2020. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

8. NIST Special Publication 800-61 Revision 2. Computer Security Incident Handling Guide. — NIST, 2012. URL: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

9. NIST Insider Threat Program Guidance (PM-12). — National Insider Threat Task Force, USA. URL: https://csrc.nist.gov/Projects/insider-threat

10. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. URL: https://www.iso.org/standard/27001

11. ISO/IEC 27002:2022. Information security controls. URL: https://www.iso.org/standard/75652.html

12. ISO/IEC 27035-1:2023. Information security incident management — Principles of incident management. URL: https://www.iso.org/standard/80642.html

13. ISO/IEC 27035-3:2024. Information security incident management — Guidelines for incident response operations. URL: https://www.iso.org/standard/83063.html

14. CERT Insider Threat Center. Common Insider Threat Patterns and Indicators. — Carnegie Mellon University, SEI. URL: https://www.sei.cmu.edu/our-work/cybersecurity/insider-threat/

15. DHS (Department of Homeland Security). Insider Threat Mitigation Guide. — USA, 2023. URL: https://www.dhs.gov/insider-threat

16. Бондаренко О. В. Аналіз внутрішніх загроз інформаційній безпеці організацій // Вісник інформаційної безпеки. — 2022. — № 3. URL: https://ouci.dntb.gov.ua/en/works/4vXx3V94/

17. Коваленко І. М. Людський фактор у системах інформаційної безпеки Кібербезпека та захист інформації. — 2021. — № 2. URL: https://ouci.dntb.gov.ua/en/works/4Kx9L9O7/

18. Київстар. Сертифікація системи управління інформаційною безпекою за ISO/IEC 27001 URL: https://kyivstar.ua/business/security/iso27001

19. TÜV Thüringen Ukraine. Сертифікація систем управління інформаційною безпекою URL: https://tuv.com.ua/ua/iso-27001

20. AIN.UA. Досвід українських IT-компаній у впровадженні URL: https://ain.ua/tag/bezpeka/

21. Державна служба спеціального зв’язку та захисту інформації України**.** Нормативні документи у сфері технічного та криптографічного захисту інформації URL: https://cip.gov.ua/ua/regulations

22. Greitzer F. L., Frincke D. A. Combining traditional cyber security audit data with psychosocial data: towards predictive modeling for insider threat

mitigation. — IEEE, 2010. URL: https://ieeexplore.ieee.org/document/5615527

23. Cappelli D., Moore A., Trzeciak R. The CERT Guide to Insider Threats. — Boston : Addison-Wesley, 2012. — 608 p. URL: https://www.sei.cmu.edu/library/the-cert-guide-to-insider-threats/
24. Bishop M., Gates C. Defining the Insider Threat. — Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research, 2008. URL: https://dl.acm.org/doi/10.1145/1413140.1413152ESET 25.
25. Research. Insider Threat Landscape Report. — URL: https://www.eset.com/int/business/resources/reports/
26. Scarfone K., Souppaya M. Guide to Data Loss Prevention (DLP). — NIST SP 800-53 (supplement), Gaithersburg, 2021. URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
27. Шпиталь О. І., Кучеренко С. Ю. Аналіз внутрішніх загроз інформаційній безпеці організацій // Вісник Національного авіаційного університету. – Київ, 2022. URL: https://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/16571
28. Житомирський державний технологічний університет. Державне управління у сфері кібербезпеки та захисту інформації Економіка, менеджмент, адміністрування. – 2023. URL: https://ema.ztu.edu.ua/article/view/242307
29. Національний авіаційний університет. Управління доступом та безпека хмарних інформаційних систем Information Security. – 2023 URL: https://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/18575
30. ITIS — SIEM. Управління подіями та інцидентами інформаційної безпеки. URL: https://www.itis.net.ua/solution/sybersecurity/siem/
31. Kumar Rahul. What Is An Insider Threat? URL: https://www.wallstreetmojo.com/insider-threat/