МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
(повна назва випускної кафедри)

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

на тему: СИСТЕМА УПРАВЛІННЯ РИЗИКАМИ В СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Виконав: студент групи 1КІ-23
Спеціальності 123 «Комп'ютерна інженерія
Мишко Іван Сергійович
Керівник роботи
к.т.н., доцент Захарова Марія В'ячеславівна
Кількість балів: _____

Оцінка: ECTS _____

Черкаси, 2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ БІЗНЕС-КОЛЕДЖ

Кафедра комп’ютерної інженерії та інформаційних технологій
(повна назва випускової кафедри)

Спеціальність 123 “Комп'ютерна інженерія ”
(шифр і назва спеціальності)

Освітня програма Комп'ютерна інженерія
(назва освітньої програми)

ЗАТВЕРДЖУЮ

Завідувач кафедри
комп’ютерної інженерії та інформаційних технологій
(назва кафедри)
_____ Хотунов В.І.
(підпис) (ПІБ)
«____»_____2025 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Мишку Івану Сергійовичу
(прізвище, ім’я, по батькові студента)

1. Тема кваліфікаційної роботи Система управління ризиками в сфері інформаційної безпеки

Науковий керівник роботи к.т.н., доцент Захарова Марія В'ячеславівна
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом закладу вищої освіти від «*7*» *жовтня* 2024 р. № *68У*

2. Строк подання студентом випускної роботи «__» _____ 202_р.

3. Вихідні дані до випускної роботи *відомості про загрози безпеки, класифікації ризиків інформаційної безпеки, методики оцінки ризиків, стандарти інформаційної безпеки.*

4. Зміст випускної роботи (перелік питань, які потрібно розробити) *включає постановку задачі управління ризиками в інформаційній безпеці, аналіз типових загроз, опис методів оцінки ризику, розробку структури системи управління ризиками, макет користувацького інтерфейсу з візуалізацією (карта ризиків, графіки), а також оцінку ефективності запропонованої моделі.*

5. Перелік графічного матеріалу (з точним зазначенням обов’язкових креслень) *включає блок-схему процесу управління ризиками, матрицю оцінки ризиків, графік динаміки залишкового ризику, макет інтерфейсу користувача та таблицю оцінених ризиків із розрахунками.*

6. Дата видачі завдання «__» _____ 202_ р.

КАЛЕНДАРНИЙ ПЛАН

№ пп	Назва етапів виконання пояснювальної записки кваліфікаційної роботи бакалавра	Терміни виконання етапів	Примітка про виконання
1	Вступ	20.01.2025р.	
2	Пошук та аналіз літературних джерел	12.02.2025р.	
3	Розділ 1 Загальні положення управління ризиками інформаційної безпеки	26.02.2025р.	
4	Розділ 2 Аналіз процесу управління ризиками інформаційної безпеки	18.03.2025р.	
5	Розділ 3 Практичні аспекти вдосконалення системи управління ризиками інформаційної безпеки	29.04.2025р.	
6	Висновки	05.05.2025р.	
8	Оформлення пояснювальної записки кваліфікаційної роботи бакалавра (чистовий варіант)	14.05.2025р.	
9	Здача пояснювальної записки кваліфікаційної роботи бакалавра на кафедру для рецензування (за 14 днів до захисту)	05.06.2025р.	
10	Перевірка пояснювальної записки кваліфікаційної роботи бакалавра на наявність ознак плагіату (за 10 днів до захисту)	09.06.2025р.	

Студент _____ Мишко Іван Сергійович
(підпис) (прізвище, ім'я по батькові студента)

Науковий керівник _____ к.т.н., Захарова Марія В'ячеславівна
(підпис) (науковий ступінь, вчене звання, прізвище, ім'я по батькові)

Анотація

У кваліфікаційній роботі бакалавра запропоновано модель удосконаленої системи управління ризиками в сфері інформаційної безпеки з акцентом на кількісне оцінювання ризиків та інтеграцію цифрових інструментів для візуалізації даних. Розглянуто сучасні методи аналізу ризиків, включно з побудовою матриці ризику, розрахунком залишкового ризику та побудовою інтерфейсу користувача для підтримки прийняття рішень.

В роботі проаналізовано основні загрози в інформаційній сфері, розроблено блок-схему системи та створено візуальний дашборд, що демонструє динаміку ризиків. Особливу увагу приділено побудові інтерактивної карти ризиків і застосуванню інструментів, сумісних з ISO/IEC 27005. Запропонована система дозволяє ефективно моніторити рівень ризику, оцінювати вплив загроз і приймати управлінські рішення для зменшення залишкового ризику.

Кваліфікаційна робота бакалавра містить __ аркуші пояснювальної записки, __ рисунків, __ таблиць і __ додатки.

Ключові слова: *інформаційна безпека, управління ризиками, матриця ризику, залишковий ризик, візуалізація, інтерфейс системи.*

Annotation

The bachelor's qualification thesis proposes a model for an improved risk management system in the field of information security, focusing on quantitative risk assessment and the integration of digital tools for data visualization. The work explores modern methods of risk analysis, including the construction of a risk matrix, calculation of residual risks, and the development of a user interface to support decision-making.

The study analyzes major threats in the information domain, designs a process flowchart for risk management, and develops a visual dashboard displaying risk dynamics. Special attention is given to the construction of an interactive risk map and the application of tools compliant with ISO/IEC 27005. The proposed system enables efficient monitoring of risk levels, assessment of threat impact, and informed decision-making to reduce residual risk.

The bachelor's thesis consists of __ pages of explanatory notes, __ figures, __ tables, and __ appendices.

Keywords: *information security, risk management, risk matrix, residual risk, visualization, system interface.*

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАЧЕНЬ

ІБ	Інформаційна безпека
ІС	Інформаційна система
РР	Залишковий ризик
КР	Категорія ризику
ІТ	Інформаційні технології
ISO/IEC	Міжнародна організація зі стандартизації / Міжнародна електротехнічна комісія
ISMS	Information Security Management System (Система управління інформаційною безпекою)
CIA	Confidentiality, Integrity, Availability (Конфіденційність, цілісність, доступність)
CVSS	Common Vulnerability Scoring System (Система оцінки вразливостей)
OWASP	Open Web Application Security Project (Проект з безпеки веб застосунків)
SQLi	SQL Injection (Ін’єкція SQL-запитів)
XSS	Cross-Site Scripting (Міжсайтове скриптування)
SOC	Security Operations Center (Центр операцій безпеки)
DLP	Data Loss Prevention (Запобігання витоку даних)
SIEM	Security Information and Event Management (Система керування подіями безпеки)

ВСТУП

У сучасному світі, що стрімко трансформується під впливом цифрових технологій, інформація стала ключовим ресурсом, від ефективного управління яким значною мірою залежить стабільність функціонування державних інституцій, підприємств, організацій та добробут громадян. З одного боку, розвиток інформаційно-комунікаційних технологій (ІКТ) відкриває широкі можливості для підвищення ефективності діяльності, а з іншого — призводить до виникнення нових загроз і вразливостей. Саме тому питання забезпечення інформаційної безпеки (ІБ) набуває особливої актуальності. Зростання обсягів кібератак, витоків даних, внутрішніх інцидентів безпеки вимагає системного підходу до управління ризиками в сфері ІБ.

Актуальність теми. На тлі глобалізації та цифрової трансформації, питання управління ризиками інформаційної безпеки набуває критичного значення. Актуальність цієї теми обумовлена необхідністю забезпечення надійного захисту конфіденційної, цілісної та доступної інформації у всіх сферах суспільного життя. Стрімке зростання кількості інцидентів інформаційної безпеки, ускладнення інформаційних систем, а також збільшення залежності організацій від цифрових сервісів робить проблематику управління ризиками надзвичайно важливою. Попри наявність міжнародних стандартів (ISO/IEC 27001, ISO 31000) та методичних рекомендацій, проблема адаптації системи управління ризиками до конкретних умов діяльності українських підприємств залишається відкритою.

Метою даної роботи є розроблення та обґрунтування підходів до вдосконалення системи управління ризиками в сфері інформаційної безпеки з урахуванням сучасних загроз, методологічних підходів та практичних інструментів.

Для досягнення мети роботи передбачається виконати такі основні **завдання**:

— визначити сутність інформаційної безпеки в сучасних умовах;

— проаналізувати ключові ризики та методи їх оцінювання;

— дослідити інструменти управління ризиками в інформаційній сфері;

— запропонувати та обґрунтувати модель вдосконалення системи управління ризиками.

Об’єктом дослідження є процес управління ризиками в сфері інформаційної безпеки організацій, що функціонують у цифровому середовищі.

Предметом дослідження виступає сукупність методів, підходів і інструментів управління ризиками в сфері ІБ, а також їх ефективність та практична реалізація в умовах реального функціонування інформаційних систем.

Для реалізації поставлених завдань у роботі використано такі основні **методи:**

— аналіз наукових джерел щодо підходів до управління ризиками в ІБ;

— моделювання процесу оцінки та обробки ризиків відповідно до стандартів ISO/IEC 27005 та NIST SP 800-30;

— використання кількісних методів (оцінка ризику за формулою $R = P \times I$);

— графічна візуалізація даних у вигляді діаграм, матриць та дашбордів;

— розробка макету користувацького інтерфейсу для демонстрації вдосконаленої системи.

Інформаційну базу дослідження склали: міжнародні та національні стандарти (ISO/IEC 27001, ISO/IEC 31000), чинне законодавство України у сфері ІБ, наукові праці вітчизняних та зарубіжних дослідників, статистичні дані, аналітичні звіти міжнародних компаній з кібербезпеки (Kaspersky, IBM Security, Cisco, Deloitte), а також матеріали професійних конференцій та семінарів.

Практичне значення. Результати дослідження можуть бути використані підприємствами, що працюють із критично важливою інформацією, для підвищення ефективності своєї політики безпеки. Запропонована модель управління ризиками може бути впроваджена в організаціях, що прагнуть відповідати вимогам міжнародних стандартів та покращити показники інформаційної безпеки.

Особистий внесок здобувача. Всі основні положення, запропоновані в роботі, є результатом самостійного дослідження автора. У разі використання ідей або моделей інших дослідників це обов’язково зазначено з відповідним посиланням.

Апробація результатів дослідження Результати роботи представлені на студентській конференції Черкаського державного фахового бізнес-коледжу, де були представлені основні положення та практичні результати розробленої моделі управління ризиками в сфері інформаційної безпеки.

Структура і обсяг роботи. Кваліфікаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел (62 найменувань). Загальний обсяг роботи становить 80 сторінок комп’ютерного тексту, без урахування додатків.

РОЗДІЛ 1 ЗАГАЛЬНІ ПОЛОЖЕННЯ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Сутність та значення інформаційної безпеки в сучасному суспільстві

У XXI столітті відбувається трансформація соціально-економічних процесів під впливом стрімкого розвитку інформаційно-комунікаційних технологій. Цей процес спричинив формування якісно нового типу суспільства — інформаційного або цифрового, у якому домінуючим ресурсом стає не матеріальний капітал, а інформація. Її обсяг, точність, доступність і захищеність визначають рівень конкурентоспроможності держав, ефективність функціонування бізнесу та якість життя окремої особи [4].

Інформація перетворилась на стратегічний нематеріальний актив, який здатний впливати на управлінські, економічні, політичні та соціальні процеси. У сучасному суспільстві вона виконує подвійну функцію: з одного боку, є засобом організації та регуляції діяльності, а з іншого — об'єктом, що підлягає захисту й управлінню.

Інформацію можна класифікувати за різними ознаками: за формою подання (текстова, графічна, числова тощо), за походженням (внутрішня, зовнішня), за функціональним призначенням (управлінська, технологічна, аналітична). У контексті цифрової економіки найбільш цінною є аналітична та управлінська інформація, яка забезпечує підтримку прийняття рішень, формування стратегій і прогнозів.

Науковці виокремлюють такі ключові властивості інформації як ресурсу:

— Репродуктивність — здатність багаторазово використовуватись без втрати якості;

— Інваріантність — незалежність від фізичного носія;

— Мультиплікативність — збільшення вартості інформації при її обробці й аналізі;

— Чутливість до контексту — зміна значущості залежно від ситуації;

— Суттєвість часового фактора — інформація швидко втрачає актуальність [8].

Інформація — це той чинник, що поєднує інтереси трьох ключових учасників цифрового середовища: держави, бізнесу та окремої особи [12]. Це трикутник взаємозалежності, у якому інформаційні потоки стають каналами впливу, контролю і зворотного зв'язку (див. рис. 1.1).

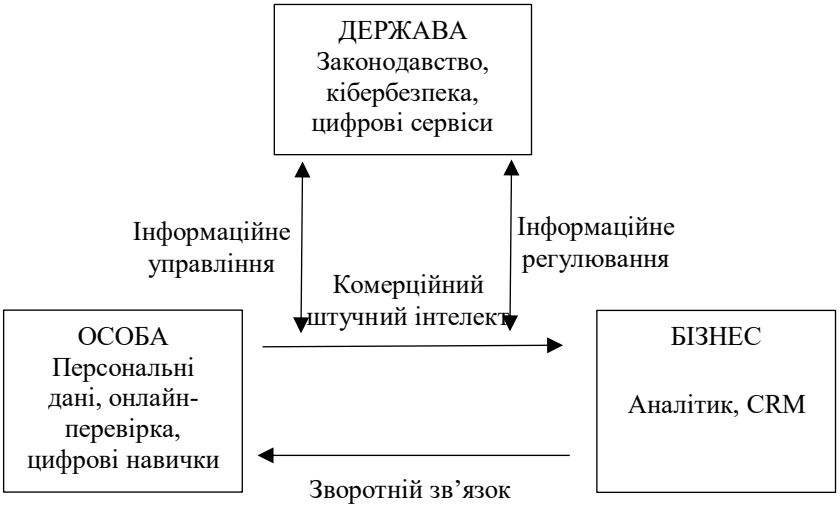

Рисунок 1.1 - Інформація як стратегічний ресурс у тріаді: держава – бізнес – особа

Як видно зі схеми, держава відповідає за нормативно-правове регулювання, розвиток цифрової інфраструктури, кіберзахист; бізнес — за використання інформації як джерела прибутку, підвищення ефективності, оптимізації логістики й маркетингу; особа — не лише споживач, але і виробник інформації, носій персональних даних, що є об'єктом захисту та управління [17].

Особливої уваги заслуговує питання приватності та захисту персональної інформації, що є критичним в умовах масового збору даних (Big Data), використання штучного інтелекту, а також розвитку концепції «розумного суспільства» (Smart Society), де дані про особу автоматично обробляються численними цифровими системами.

Ще одним критичним аспектом є інформаційна асиметрія — ситуація, коли одна сторона має доступ до значно більших обсягів інформації, ніж інша. Це створює нерівність між учасниками суспільних відносин: наприклад, корпорації

мають змогу аналізувати поведінку користувача в режимі реального часу, тоді як сам користувач не усвідомлює масштаби цього збору [2].

У свою чергу, цифровий розрив — це ще один прояв нерівності, що виражається в обмеженому доступі до інформаційних технологій у частини населення через технічні, економічні або освітні бар'єри. Це явище не лише знижує рівень цифрової інклюзії, а й ускладнює реалізацію концепцій електронного врядування, онлайн-освіти, телемедицини тощо.

Отже, інформація в сучасному суспільстві виступає не лише об'єктом використання, а й предметом управління і захисту. Вона є ресурсом, який забезпечує прийняття стратегічних рішень, стимулює інновації, формує конкурентні переваги та визначає якість життя громадян. У зв'язку з цим зростає потреба у формуванні ефективної системи управління інформаційною безпекою, де інформація розглядається як актив, що підлягає оцінюванню, контролю і захисту від ризиків [28].

Інформаційна безпека є системною категорією, що охоплює як технічні, так і організаційно-правові заходи, спрямовані на захист інформації та інформаційних систем від будь-яких загроз, які можуть вплинути на їх нормальне функціонування. Ключовими складовими інформаційної безпеки, які формують її базову концепцію, є конфіденційність, цілісність та доступність — так звана CIA-модель (Confidentiality, Integrity, Availability) [48].

Ці три аспекти визначають фундаментальні вимоги до захисту інформації незалежно від її форми, обсягу, способу зберігання або обробки. Кожен із них відображає окремий напрям ризиків, що має бути врахований під час проєктування, впровадження та експлуатації систем інформаційної безпеки.

Конфіденційність означає забезпечення недоступності інформації для сторонніх осіб, яким не надано відповідного рівня доступу. Її порушення призводить до витоку даних, що може спричинити як репутаційні, так і фінансові втрати для організації. В межах цифрового простору загроза конфіденційності реалізується через:

— несанкціонований доступ;

— прослуховування трафіку;

— розкриття логінів і паролів;

— атаки соціальної інженерії (phishing, baiting тощо).

Забезпечення конфіденційності реалізується шляхом застосування криптографічних алгоритмів, систем контролю доступу, політик розмежування прав, а також регулярного моніторингу подій доступу [60].

Цілісність означає забезпечення точності, повноти та незмінності інформації протягом усього її життєвого циклу. Порушення цілісності може бути спричинене як навмисним втручанням (наприклад, шкідливим ПЗ), так і помилками користувачів або програмних модулів.

Типовими прикладами порушення цілісності є:

— фальсифікація даних у фінансових звітах;

— підміна файлів під час передачі через мережу;

— модифікація баз даних хакерами.

— Механізми забезпечення цілісності включають контрольні суми (hash-функції), цифрові підписи, журнали змін (audit trails) та системи виявлення змін (file integrity monitoring).

Доступність означає, що інформація повинна бути доступною для авторизованих користувачів у потрібний час, без затримок або збоїв. Це критично важливо для забезпечення безперервності бізнес-процесів, особливо в сферах охорони здоров’я, фінансів, державного управління [4].

Типові загрози доступності:

— відмова апаратного забезпечення;

— атаки типу «відмова в обслуговуванні» (DDoS);

— помилки конфігурації систем;

— стихійні лиха, що виводять системи з ладу.

Для гарантування доступності застосовуються методи резервного копіювання (backup), кластеризації серверів, впровадження політик відновлення після інцидентів (Disaster Recovery Plans), а також системи високої доступності (High Availability, HA) (див. рис. 1.) [7].

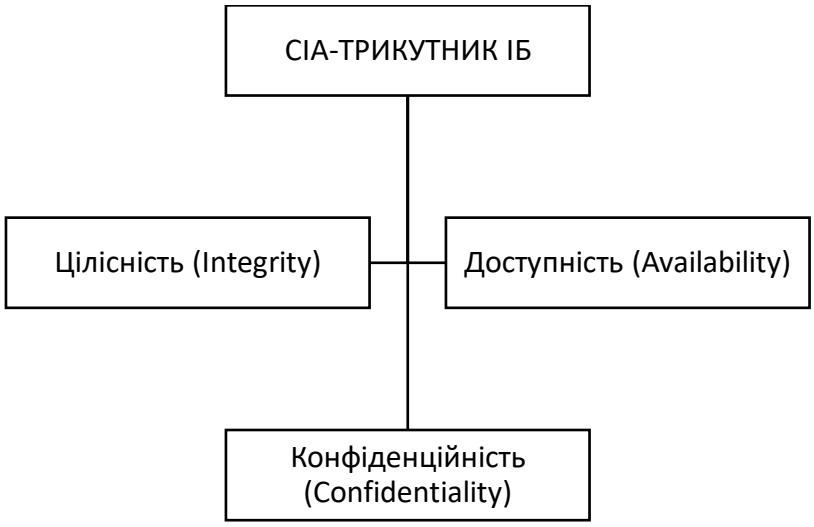

Рисунок 1.2 - Базова модель ІБ (CIA triangle)

Рисунок 1.2 демонструє трикутник CIA, що візуалізує рівноправність і взаємозалежність трьох основних вимірів інформаційної безпеки. Порушення будь-якого з них призводить до компрометації всієї системи, а надмірна увага до одного аспекту на шкоду іншим — до дисбалансу та зниження загального рівня захищеності [9].

Наприклад, система, яка забезпечує виняткову конфіденційність (наприклад, через складну багатофакторну автентифікацію), але недоступна для користувачів у потрібний момент, вважається неефективною з точки зору цілісного підходу до ІБ. Аналогічно, система, орієнтована на 100% доступність, але з вразливостями до фальсифікації або несанкціонованого доступу, створює критичні ризики.

Конфіденційність, цілісність і доступність — це основоположні принципи інформаційної безпеки, що утворюють єдину систему координат для оцінки стану та якості захисту інформаційних активів. Ефективне управління інформаційними ризиками можливе лише за умови комплексного забезпечення всіх трьох компонентів, з урахуванням специфіки об’єкта, актуальних загроз та технічних можливостей організації [12].

Формування ефективної системи інформаційної безпеки неможливе без наявності належного нормативно-правового регулювання. Законодавча база виступає фундаментом, який визначає принципи, вимоги, межі відповідальності та процедури взаємодії суб’єктів інформаційного простору, а також засади

захисту даних, обробки інформації та реагування на інциденти. У цьому контексті надзвичайно важливу роль відіграє як національне законодавство, так і міжнародні стандарти, що задають єдину методологічну рамку для усіх країн і компаній, які прагнуть до цифрової зрілості та захищеності.

На міжнародному рівні ключовим документом, що визначає вимоги до систем управління інформаційною безпекою, є стандарт ISO/IEC 27001. Він встановлює структуровані підходи до захисту інформації, зокрема передбачає впровадження політики інформаційної безпеки, управління ризиками, контроль доступу, захист комунікацій, а також процедури моніторингу, аудиту та безперервного покращення системи. У доповнення до нього діє стандарт ISO/IEC 27002, який надає практичні рекомендації щодо реалізації контролів безпеки. Для оцінювання ризиків в ІБ використовується ISO/IEC 27005, що забезпечує уніфіковану методику для ідентифікації, аналізу, оцінки та обробки ризиків. Водночас у США активно застосовується стандарт NIST SP 800-30, який широко використовується в державному секторі й має прикладне значення в контексті управління ризиками інформаційної безпеки [44].

Не менш важливим є національне законодавство України, що поступово адаптується до вимог цифрової безпеки, особливо після активізації гібридних загроз та зростання рівня кібератак на критичну інфраструктуру. Основу законодавчого поля становить Закон України «Про інформацію», який окреслює загальні положення функціонування інформаційної сфери та правові засади інформаційних відносин. Важливим доповненням до нього є Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», який установлює вимоги до технічного та криптографічного захисту інформації, а також до безпеки засобів її обробки. Закон України «Про кібербезпеку» став першим кроком у створенні цілісної архітектури національної системи кіберзахисту, адже він передбачає категоризацію об’єктів критичної інфраструктури, створення національного центру реагування на інциденти та координацію міжвідомчих дій у сфері ІБ [16].

Крім законів, до нормативної бази належать стратегічні документи, серед яких слід виділити Концепцію кібербезпеки України, затверджену в 2016 році. Цей документ визначає стратегічні цілі держави щодо забезпечення стійкості до кіберзагроз, а також формує підходи до створення безпечного кіберпростору. Практичну реалізацію завдань у сфері безпеки координує Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ), яка відповідає за стандартизацію, сертифікацію, контроль і розвиток засобів захисту інформації [19].

Щоб систематизувати нормативну базу у сфері ІБ, доцільно представити порівняльну таблицю, яка відображає як міжнародні стандарти, так і основні українські законодавчі акти (див. табл. 1.1).

Таблиця 1.1 – Ключові нормативні документи у сфері ІБ (національні та міжнародні)

№	Назва документа	Рівень	Основне призначення
1	ISO/IEC 27001	Міжнародний	Визначає вимоги до систем управління інформаційною безпекою
2	ISO/IEC 27002	Міжнародний	Надає рекомендації щодо реалізації політик безпеки
3	ISO/IEC 27005	Міжнародний	Методологія управління ризиками ІБ
4	NIST SP 800-30	Міжнародний	Метод оцінювання ризиків ІБ у державному секторі США
5	Закон України «Про інформацію»	Національний	Визначає загальні принципи інформаційних відносин
6	Закон України «Про захист інформації в ІТ-системах»	Національний	Регламентує технічний захист інформації в системах
7	Закон України «Про кібербезпеку»	Національний	Встановлює правові засади забезпечення кіберзахисту
8	Концепція кібербезпеки України	Національний	Стратегічний документ з безпеки кіберпростору
9	COBIT 5	Міжнародний	ІТ-стандарт з управління безпекою та ІТ-процесами

Джерело: узагальнено автором на основі даних [11, 19, 36]

Національна та міжнародна нормативна база у сфері інформаційної безпеки створює передумови для ефективної реалізації системи захисту інформації. Вона слугує не лише інструментом регламентації, але й платформою для впровадження сучасних методологій оцінювання ризиків, побудови систем управління безпекою, а також розвитку культури кібербезпеки в межах організацій. Адаптація положень міжнародних стандартів до національного

законодавства України є необхідною умовою гармонізації регуляторного середовища та підвищення кіберстійкості країни в умовах цифрових викликів.

У цифрову епоху, коли інформаційні потоки стали основою функціонування державних структур, бізнесу та особистих комунікацій, інформаційна безпека набуває особливого значення. Разом із цим зростає кількість і складність загроз, що впливають на цілісність, конфіденційність та доступність інформації. Ефективне управління безпекою інформаційних систем потребує глибокого розуміння природи та класифікації загроз, з якими стикаються користувачі, організації та суспільство загалом [19].

Загроза в контексті інформаційної безпеки — це потенційна можливість реалізації впливу на інформацію або інформаційну систему, що може призвести до небажаних наслідків. При цьому загрози можуть бути як навмисними, так і ненавмисними, внутрішніми або зовнішніми, викликаними як діяльністю людини, так і збоєм технічних засобів чи впливом природного середовища. Різноманітність джерел загроз потребує системного підходу до їх класифікації, що дозволяє не лише ідентифікувати можливі ризики, а й визначити пріоритети захисту.

Загрози можна поділити на кілька ключових груп за критерієм джерела: внутрішні, зовнішні, технологічні та соціальні. Такий поділ дозволяє чітко структурувати потенційні вектори атак або впливу.

Внутрішні загрози виникають зсередини організації й часто пов’язані з діями співробітників, які мають доступ до інформаційних ресурсів. Це можуть бути як навмисні дії (наприклад, викрадення даних колишнім працівником), так і ненавмисні (наприклад, випадкове видалення файлів або розголошення паролів). У деяких випадках саме внутрішній персонал є основним джерелом серйозних порушень, оскільки має високий рівень довіри та доступу [23].

Зовнішні загрози формуються поза межами організації. Вони можуть бути результатом цілеспрямованої діяльності кіберзлочинців, хакерських угруповань, конкурентів або навіть державних структур, що здійснюють кіберрозвідку. Серед найпоширеніших проявів таких загроз — фішинг, спроби

несанкціонованого доступу, DDoS-атаки, впровадження шкідливого програмного забезпечення тощо [44].

Технологічні загрози пов’язані з недоліками або збоями технічних і програмних компонентів інформаційних систем. Сюди входять апаратні відмови, вразливості в програмному забезпеченні, помилки в конфігурації систем, відсутність резервного копіювання або неоновлення систем безпеки. Такі загрози є особливо актуальними в умовах активного впровадження складних ІТ-інфраструктур та швидкого зростання обсягів оброблюваної інформації.

Соціальні загрози виникають у результаті маніпуляцій з боку зловмисників, спрямованих на використання психологічних слабкостей користувачів. Найбільш поширеним прикладом є соціальна інженерія, яка включає техніки обману, що спонукають користувача розголосити конфіденційну інформацію, встановити шкідливе ПЗ або виконати дії, що компрометують безпеку системи. Успішність таких атак часто пов’язана з відсутністю базової обізнаності користувачів у питаннях безпеки [18].

Для систематизації розглянутих типів загроз доцільно представити класифікацію загроз інформаційної безпеки за джерелами, що дозволяє більш ефективно адаптувати систему захисту до конкретних ризиків (див. табл. 1.2).

Таблиця 1.2 – Класифікація загроз інформаційної безпеки за джерелами

Тип загроз	Джерело	Характеристика	Приклади
Внутрішні	Співробітники, користувачі	Порушення, що виникають внаслідок дій працівників	Витік даних через персонал, помилкове видалення файлів
Зовнішні	Зовнішні суб’єкти	Намірена або ненавмисна дія ззовні організації	Хакерські атаки, фішинг, шкідливе ПЗ
Технологічні	ІТ-інфраструктура	Збої, помилки, вразливості апаратного/програмного забезпечення	Застаріле ПЗ, апаратна відмова, неправильна конфігурація
Соціальні	Людський фактор	Маніпуляція, вплив на користувачів	Соціальна інженерія, шахрайство, підробка особистості

Джерело: узагальнено автором на основі даних [22, 48]

Спектр загроз інформаційній безпеці є надзвичайно широким і динамічним, що вимагає не лише технічної підготовки, а й постійного

моніторингу ситуації, навчання персоналу, регулярного аудиту систем захисту. Розуміння природи загроз та їх джерел дозволяє вибудувати ефективну систему реагування та мінімізації ризиків, забезпечуючи тим самим стабільність функціонування організації в умовах інформаційного суспільства [19].

У сучасному цифровому середовищі загрози інформаційній безпеці набули нових форм, що поєднують високий технічний рівень з маніпулятивними методами впливу на поведінку користувача. Однією з найнебезпечніших категорій загроз сьогодні є кіберзлочинність — системна протиправна діяльність у кіберпросторі, спрямована на викрадення, підміну, блокування або знищення інформації з метою отримання прибутку, шантажу або дестабілізації.

Ключовою характеристикою кіберзлочинності є її транснаціональний характер: атаки здійснюються з використанням інструментів, які дозволяють маскувати реальні джерела походження, а наслідки можуть впливати на державну безпеку, бізнес-континуїтет та приватне життя громадян. Основні вектори таких атак пов’язані з поширенням шкідливого програмного забезпечення, використанням соціальної інженерії, проникненням у корпоративні мережі та маніпуляцією поведінкою користувачів [48].

Одним із найпоширеніших проявів кіберзлочинності є фішинг — технологія обману, за якої зловмисник маскується під надійне джерело (наприклад, банк або державну установу), щоб змусити користувача розкрити конфіденційні дані. Часто такі атаки здійснюються через підроблені електронні листи або вебсайти, які візуально майже не відрізняються від оригінальних. Успішна фішинг-атака може призвести до викрадення паролів, зламу облікових записів та подальшого компрометування систем [13].

Не менш руйнівними є атаки типу ransomware — програмне забезпечення, що шифрує дані жертви з подальшою вимогою викупу за ключ дешифрування. Цей тип загроз став особливо актуальним у 2020–2024 роках, коли атак зазнали великі державні та медичні установи по всьому світу. Особливу небезпеку становить той факт, що навіть після сплати викупу немає гарантії відновлення даних, а факт порушення безпеки завдає значної репутаційної шкоди [11].

Окрема категорія ризиків — це інсайдерські загрози, які виникають внаслідок дій осіб, що мають легальний доступ до інформаційних систем організації. Інсайдери можуть навмисно викрадати або знищувати дані, передавати їх конкурентам, або діяти ненавмисно, створюючи вразливості через необережне поводження з інформацією. Складність боротьби з інсайдерськими загрозами полягає в тому, що такі користувачі часто мають високий рівень довіри та розширені права доступу, що ускладнює їх своєчасне виявлення [19].

Соціальна інженерія як окрема форма впливу, що спирається на маніпуляцію емоціями, страхом або довірою, виступає допоміжним інструментом у багатьох кіберзлочинах. Через психологічний тиск або створення ілюзії терміновості зловмисники змушують жертв порушити правила безпеки — наприклад, натиснути на шкідливе посилання або ввести свої облікові дані на фішинговій сторінці (див. табл. 1.3).

Таблиця 1.3 – Типові кіберзагрози та пов’язані ризики (з прикладами)

Тип загрози	Опис	Приклади	Пов’язані ризики
Фішинг	Маскування під надійне джерело з метою обману користувача	Фейкові email-повідомлення з посиланням на шкідливий сайт	Викрадення паролів, фінансових даних, компрометація акаунтів
Ransomware	Шкідливе ПЗ, яке шифрує дані і вимагає викуп	WannaCry, Petya, LockBit	Втрата доступу до даних, фінансові збитки, репутаційні втрати
Інсайдерські дії	Зловмисні або необережні дії працівників	Витік баз клієнтів, видалення критичних файлів	Втрата конфіденційної інформації, порушення безперервності роботи
Соціальна інженерія	Психологічний вплив для досягнення небезпечних дій	Дзвінки «від банку», прохання «керівника» надіслати дані	Несанкціонований доступ, вторгнення в систему, шантаж

Джерело: узагальнено автором на основі даних [17, 19]

У сукупності, ці загрози формують високий рівень ризиків як для приватних осіб, так і для корпоративних структур, які часто недооцінюють можливість внутрішнього витоку чи маніпулятивного тиску. Враховуючи стрімкий розвиток технологій та зростання цифрової залежності, необхідність виявлення, оцінки та управління цими ризиками стає критично важливою умовою підтримання стійкості інформаційної системи. Організації мають впроваджувати програми навчання персоналу, багаторівневу автентифікацію,

системи моніторингу користувацької активності та процедури реагування на інциденти, щоб мінімізувати шкоду від кіберзлочинної активності [38].

Отже, проведений аналіз засвідчує, що інформаційна безпека в умовах цифровізації суспільства перетворилась на системоутворюючий фактор стабільності та стійкості соціально-економічних процесів. Інформація стала ключовим ресурсом, що формує стратегічну перевагу на рівні держави, бізнесу та окремої особи. Основними складовими захищеності інформації виступають конфіденційність, цілісність та доступність, які утворюють фундамент так званої CIA-моделі. Законодавча та нормативна база інформаційної безпеки забезпечує уніфікований підхід до побудови систем захисту як на міжнародному, так і на національному рівнях, тоді як ідентифікація ключових загроз — внутрішніх, зовнішніх, технологічних і соціальних — дозволяє адаптувати політику безпеки до реальних викликів інформаційного середовища. Сукупність цих чинників визначає необхідність формування комплексної та динамічної системи управління інформаційною безпекою, здатної ефективно реагувати на ризики сучасного кіберпростору.

1.2. Поняття та класифікація ризиків в інформаційній безпеці

У контексті інформаційної безпеки поняття «ризик» є базовим і водночас надзвичайно комплексним. Воно охоплює не лише ймовірність реалізації загроз, але й можливі наслідки для інформаційних ресурсів, процесів та систем. Ризик є вимірюваним показником потенційної шкоди, яка може бути завдана інформаційним активам у разі вразливості до певного типу загроз. У сучасній науковій та нормативній літературі існує декілька формалізованих підходів до його визначення [9].

Згідно зі стандартом ISO/IEC 27005:2018, який присвячений управлінню ризиками в інформаційній безпеці, ризик визначається як «*потенційна ймовірність того, що певна загроза скористається вразливістю активу, що спричинить шкоду організації*». У цьому означенні відображено ключові

компоненти: загроза, вразливість, актив і шкода. Водночас міжнародний стандарт ISO 31000:2018, який має загальніший характер, визначає ризик як «*вплив невизначеності на досягнення цілей*», акцентуючи увагу на зв'язку між ризиком та управлінськими процесами [26].

У літературі також поширене визначення, згідно з яким ризик в інформаційній безпеці — це функція ймовірності події та масштабу її потенційних негативних наслідків для інформаційної системи. Цей підхід дозволяє формалізувати процес оцінювання ризиків і застосовувати його в інженерних та управлінських рішеннях.

Базова формула, що узагальнює підхід до кількісної оцінки ризику, виглядає наступним чином [4]:

$$R = P \times I$$

де:

R — загальний рівень ризику (Risk);

P — ймовірність (Probability) виникнення інциденту;

I — вплив (Impact), який цей інцидент може спричинити.

Ця формула є відправною точкою для більш складних моделей аналізу ризиків, оскільки дозволяє співвідносити два основні параметри — ймовірність і наслідки. У прикладному аспекті це означає, що навіть подія з низькою ймовірністю може бути високим ризиком, якщо її потенційний вплив є катастрофічним (наприклад, повна компрометація бази даних або виведення з ладу критично важливої інфраструктури) [61].

Ризик може бути прийнятним, частково прийнятним або неприйнятним — залежно від встановлених організацією порогових значень. У більшості випадків для кожної категорії ризиків (низький, середній, високий) встановлюється відповідна стратегія реагування: від пасивного спостереження до повного уникнення [45].

Розуміння сутності ризику в сфері ІБ є необхідним для побудови логічно обґрунтованої системи управління ризиками. Формалізовані підходи та математичне моделювання дозволяють не лише оцінити рівень загроз, але й

розробити стратегії зниження ризиків, забезпечуючи тим самим цілісність, конфіденційність і доступність інформаційних активів.

Оцінювання та управління ризиками в сфері інформаційної безпеки базується на розумінні природи ризику як багатофакторного явища. Одним із ключових підходів у ризик-менеджменті є концепція трьох основних компонентів ризику — загроза, вразливість та актив. Саме взаємодія цих елементів створює умови, за яких може реалізуватися небажана подія, що загрожує безпеці інформаційної системи [59].

Актив — це будь-який об’єкт, який має цінність для організації та потребує захисту. У сфері інформаційної безпеки активами вважаються не лише апаратне та програмне забезпечення, а й інформація, користувачі, бізнес-процеси, інтелектуальна власність тощо. Значущість активу визначається його критичністю для функціонування організації, а також потенційними наслідками втрати його цілісності, доступності або конфіденційності.

Вразливість — це слабке місце або недолік у захисті, який може бути використаний для порушення нормального функціонування активу. Вразливості можуть мати технічний, організаційний або людський характер. Наприклад, вразливість може полягати у використанні застарілої операційної системи, відсутності багатофакторної автентифікації, слабких паролях або недостатній обізнаності персоналу [48].

Загроза — це будь-який фактор або подія, яка має потенціал реалізувати негативний вплив на актив шляхом використання вразливості. Загрози можуть бути природними (стихійні лиха), техногенними (збої техніки), або навмисними (кібератаки, інсайдерські дії). У сучасних умовах найбільш актуальними є саме цілеспрямовані кіберзагрози, які поєднують технічні засоби з методами соціальної інженерії [53].

Ключовий момент полягає в тому, що ризик виникає лише у разі одночасної наявності трьох компонентів: активу, що має цінність; вразливості, яка дозволяє здійснити вплив; та загрози, яка цей вплив реалізовує. У разі

відсутності хоча б одного елементу ризик або не виникає, або має нульову величину (див. рис. 1.3).

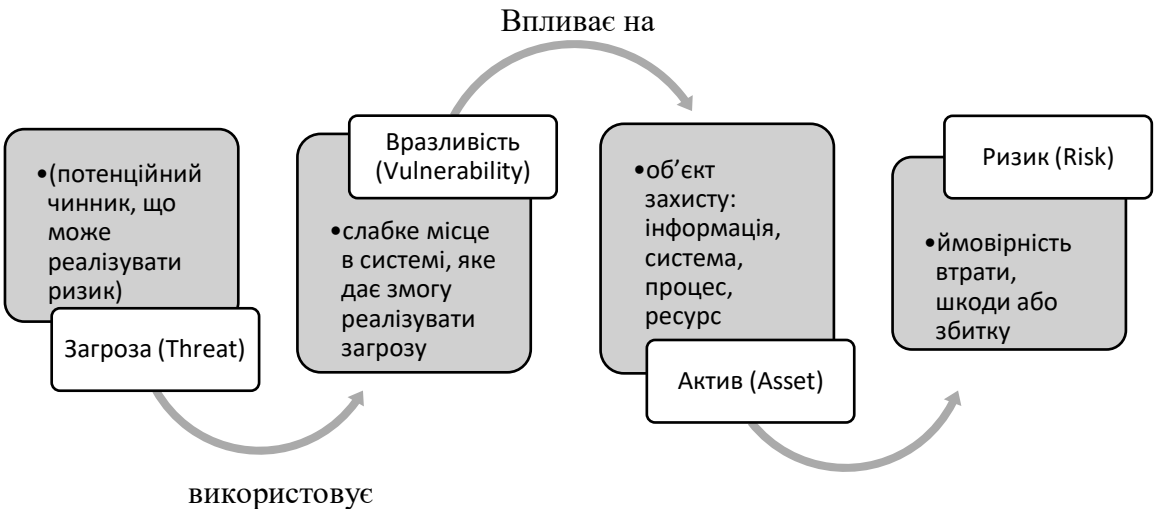

Рисунок 1.3 – Взаємозв’язок загрози, вразливості та активу у формуванні ризику

Рисунок 1.3 чітко демонструє, що ризик — це не автономне явище, а результат взаємодії. Наприклад, якщо в організації є критичний актив (база персональних даних), і система має незакриту вразливість (відсутність шифрування чи firewall), то наявність зовнішньої загрози (хакерської атаки) автоматично створює умови для реалізації ризику, який може призвести до витоку даних, фінансових санкцій і втрати репутації [17].

Зважаючи на це, при побудові системи управління ризиками першочерговим завданням є ідентифікація всіх трьох компонентів, а саме: визначення критичних активів, виявлення їхніх вразливостей та опис ймовірних загроз. Лише комплексна оцінка дозволяє отримати об'єктивну картину ризиків і виробити відповідні стратегії їхнього зниження чи уникнення.

Для ефективного управління ризиками в інформаційній безпеці важливо не лише виявити сам факт їх існування, а й систематизувати їх за певними критеріями. Класифікація дозволяє краще зрозуміти природу ризиків, визначити рівень їх пріоритетності, а також розробити відповідні механізми реагування. У сфері ІБ класифікація ризиків, як правило, здійснюється за трьома ключовими ознаками: джерелом виникнення, масштабом впливу та тривалістю впливу [20].

Перший і, мабуть, найпоширеніший підхід — класифікація за джерелами походження. Тут ризики поділяються на внутрішні та зовнішні. Внутрішні ризики зазвичай виникають через людський фактор, організаційні недоліки (відсутність політик безпеки, незахищені процедури) або технічні помилки всередині системи. Зовнішні ризики, своєю чергою, пов’язані з хакерськими атаками, фішингом, діяльністю конкурентів або діями, що спричинені зовнішніми природними або соціальними умовами.

Другий критерій — масштаб впливу, що враховує розмір та серйозність наслідків реалізації ризику. За цим критерієм виділяють локальні ризики, які зачіпають окремий процес, підрозділ або актив, та системні (глобальні) — такі, що можуть призвести до паралізації роботи цілої організації або навіть негативно вплинути на репутацію й фінансову стабільність підприємства. Масштаб ризику безпосередньо впливає на вибір стратегії управління: локальні ризики можуть бути прийняті або перенесені, а системні потребують негайного реагування та ресурсного забезпечення [27].

Третім важливим параметром є тривалість впливу ризику. У цьому контексті розрізняють короткострокові ризики, наслідки яких проявляються негайно або протягом короткого періоду часу, та довгострокові ризики, які можуть мати пролонгований, накопичувальний або відстрочений характер (див. табл. 1.4).

Таблиця 1.4 – Класифікація ризиків інформаційної безпеки

Критерій класифікації	Тип ризику	Характеристика / Приклади
За джерелом виникнення	Внутрішні	Недбалість співробітників, інсайдерські загрози, помилки конфігурації
	Зовнішні	Кіберзлочинність, фішинг, DDoS-атаки, стихійні лиха
За масштабом впливу	Локальні	Вихід з ладу одного сервера, втрата неключової інформації
	Системні (глобальні)	Компрометація баз даних, тривале блокування роботи всієї системи
За тривалістю впливу	Короткострокові	Тимчасове падіння мережі, одноразовий збій доступу
	Довгострокові	Хронічні витоки даних, пошкодження репутації, штрафні санкції

Джерело: узагальнено автором на основі даних [11]

Отже, класифікація ризиків в інформаційній безпеці є важливою передумовою для вибору відповідних заходів захисту. Вона дозволяє визначити джерело загрози, оцінити ймовірний масштаб наслідків та зрозуміти тривалість впливу на інформаційну систему. Використання системного підходу до класифікації ризиків є невід'ємною частиною сучасного управління ІБ і базою для подальших аналітичних та організаційних рішень у рамках ризик-менеджменту [44].

У системі управління інформаційною безпекою ризики не є статичним явищем. Вони розвиваються у часі, змінюючи свій масштаб, критичність та способи впливу. Для розуміння динаміки розвитку ризику доцільно застосовувати концепцію життєвого циклу ризику, що дозволяє відстежувати всі ключові етапи – від його зародження до остаточного усунення або контролю. Такий підхід дає змогу приймати своєчасні та обґрунтовані рішення на кожному з етапів життєвого циклу, що особливо важливо у високодинамічному середовищі кіберзагроз [51].

Життєвий цикл ризику в сфері ІБ, як правило, складається з чотирьох ключових фаз: виникнення, ескалація, виявлення та реакція. Кожна з них має свої особливості, інструменти та відповідальних осіб або системи в межах організації.

На першому етапі – виникнення ризику – формується початкове середовище, у якому загроза може скористатися вразливістю активу. Причинами можуть бути технологічні зміни, недоліки в архітектурі безпеки, людський фактор, зростання активності зловмисників або зовнішні події. Часто на цьому етапі ризик ще не реалізований, але вже існує потенційна небезпека, що потребує моніторингу.

Далі, у разі відсутності належного контролю, ризик може ескалювати, тобто перейти з пасивного стану в активний, починаючи впливати на інформаційні системи. Це може проявитися у вигляді підозрілої активності, несанкціонованого доступу, помилок або збоїв у роботі. Ескалація супроводжується розширенням масштабів впливу – від одного активу до всієї підсистеми, а іноді й до критичних процесів підприємства [3].

На етапі виявлення ризику система або відповідальні фахівці фіксують ознаки порушення – через журнали подій, системи виявлення вторгнень (IDS/IPS), антивірусне ПЗ, повідомлення від користувачів або внутрішній аудит. Виявлення не завжди відбувається одразу – у деяких випадках про наявність інциденту стає відомо лише постфактум, коли шкода вже нанесена. Висока якість інструментів моніторингу та швидкість реагування є критично важливими саме на цьому етапі.

Останній етап — реакція на ризик — включає комплекс дій, спрямованих на мінімізацію шкоди, усунення вразливості, нейтралізацію загрози, а також інформування відповідальних осіб. Реакція може бути технічною (відновлення з резервної копії, блокування користувача, оновлення ПЗ), організаційною (перегляд політик, навчання персоналу), юридичною (розслідування, повідомлення компетентних органів) тощо. Ефективність реакції визначає не лише швидкість відновлення, але й довіру до системи безпеки загалом [59].

Узагальнено життєвий цикл інформаційного ризику зображено на рисунку 1.4, що демонструє послідовність етапів та логіку їхнього переходу (див. рис. 1.4).

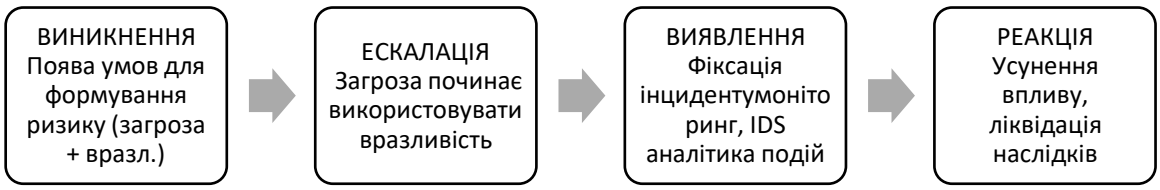

Рисунок 1.4 – Життєвий цикл інформаційного ризику

Розуміння та управління життєвим циклом ризику дозволяє не лише вчасно ідентифікувати загрозу, але й грамотно реагувати на неї, попереджаючи серйозні інциденти. Це підвищує рівень кіберстійкості організації та забезпечує стабільність функціонування її інформаційної інфраструктури в умовах зростання складності та кількості ризиків [44].

У сучасному цифровому середовищі інформаційна безпека піддається дедалі складнішим загрозам, пов’язаним із активізацією кіберзлочинності та маніпулятивними методами впливу на користувачів. На відміну від класичних

технічних атак, сучасні кіберризики часто поєднують технічну складову з елементами психологічного впливу, що ускладнює їх виявлення та нейтралізацію.

Кіберзлочинність охоплює широкий спектр дій — від викрадення інформації до виведення з ладу IT-систем. Особливістю сучасної кіберзлочинності є її глобальний характер, децентралізована структура та здатність до швидкої адаптації. Внаслідок цифрової трансформації бізнесу та державних послуг, кібератаки стають не лише більш частими, але й дедалі цілеспрямованішими. Найтиповішими векторами є фішинг, впровадження шкідливого ПЗ (зокрема ransomware) та інсайдерські загрози [29].

Фішинг — один із найбільш поширених методів соціальної інженерії, який ґрунтується на обмані користувача з метою викрадення його облікових даних. У таких атаках зловмисник видає себе за легітимного представника організації (наприклад, банку або сервісу підтримки) і надсилає електронний лист або повідомлення з посиланням на підроблений вебресурс. Небезпека фішингу полягає в його масовості та високій ймовірності успіху, особливо якщо мішенню є малообізнаний персонал.

Ransomware (програми-здирники) стали ключовою кіберзагрозою останніх років. Їх суть полягає в шифруванні критичних даних користувача або цілої організації з подальшою вимогою викупу за відновлення доступу. Атаки типу ransomware завдають величезної шкоди, порушуючи цілісність і доступність даних, зупиняючи бізнес-процеси і створюючи серйозні репутаційні втрати. Відомі приклади — атаки з використанням вірусів WannaCry, Petya, LockBit, які паралізували роботу державних структур і підприємств по всьому світу [33].

Інсайдерські загрози формуються всередині організації — з боку осіб, які мають прямий або непрямий доступ до інформаційних ресурсів. Інсайдери можуть діяти навмисно (передача конфіденційних даних конкурентам, саботаж) або ненавмисно (випадкове порушення правил безпеки, небезпечна поведінка в мережі). Ці загрози є особливо складними для виявлення, оскільки внутрішні

користувачі часто мають високий рівень довіри, а отже — доступ до критичних систем [18].

Соціальна інженерія виступає каталізатором багатьох ризиків, оскільки зловмисники навчаються впливати на психологію користувачів, використовуючи страх, поспіх, довіру або незнання. Вона дозволяє обходити технічні засоби захисту через маніпуляцію людським фактором (див. табл. 1.5).

Таблиця 1.5 – Типові кіберзагрози та пов’язані ризики (з прикладами)

Тип загрози	Короткий опис	Приклади	Потенційні ризики
Фішинг	Маскування під легітимне джерело для викрадення облікових даних	Email-запити «від банку», підроблені сайти входу	Компрометація акаунтів, несанкціонований доступ, витік даних
Ransomware	Шкідливе ПЗ, яке блокує доступ до даних і вимагає викуп	WannaCry, Petya, LockBit	Повна недоступність систем, фінансові втрати, збій операцій
Інсайдери	Працівники, які навмисно або ненавмисно створюють загрози	Витік баз даних, видалення файлів, передача інформації	Порушення конфіденційності, пошкодження даних, правові наслідки
Соціальна інженерія	Психологічний вплив для обходу технічних заходів безпеки	Дзвінки «від керівника», маніпулятивні листи	Несанкціонований доступ, шантаж, обман фінансового характеру

Джерело: узагальнено автором на основі даних [14, 22]

Ризики, пов’язані з кіберзлочинністю та соціальною інженерією, є одними з найскладніших для виявлення і запобігання, оскільки вони поєднують технічну складність із людським фактором. Їхній вплив на безперервність бізнесу, репутацію та правову відповідальність може бути критичним. Тому сучасні системи управління інформаційною безпекою мають включати не лише технічні засоби захисту, а й освітні, психологічні та поведінкові стратегії, спрямовані на підвищення обізнаності користувачів і формування культури кібербезпеки.

Отже, ризик в інформаційній безпеці — це результат взаємодії загроз, вразливостей та цінних активів, що можна оцінити за ймовірністю та впливом. Його природа є комплексною, а тому потребує чіткого структурування. Класифікація ризиків за джерелами, масштабом і тривалістю дозволяє обґрунтовано визначати пріоритети захисту. Аналіз життєвого циклу ризику забезпечує розуміння динаміки його розвитку, а розгляд сучасних кіберзагроз, зокрема фішингу, ransomware та інсайдерів, показує необхідність не лише

технічного, а й поведінкового реагування. Усі ці аспекти формують основу для методичного управління ризиками, що стане предметом наступного аналізу.

1.3. Методологічні підходи до управління ризиками інформаційної безпеки

Управління ризиками інформаційної безпеки є системним і багатоетапним процесом, мета якого полягає у своєчасному виявленні, оцінюванні, мінімізації та постійному контролі потенційних загроз. Цей процес передбачає поетапну роботу з ризиками, яка має бути інтегрована у загальну політику безпеки підприємства та враховувати специфіку його інформаційної інфраструктури [48].

Типовий цикл управління ризиками включає п’ять основних етапів: виявлення ризиків, аналіз, оцінка, обробка (реагування) та моніторинг. Цей підхід узгоджується зі стандартами ISO/IEC 27005 та ISO 31000, які визначають логіку побудови процесів ризик-менеджменту в сфері інформаційної безпеки (див. рис. 1.5)

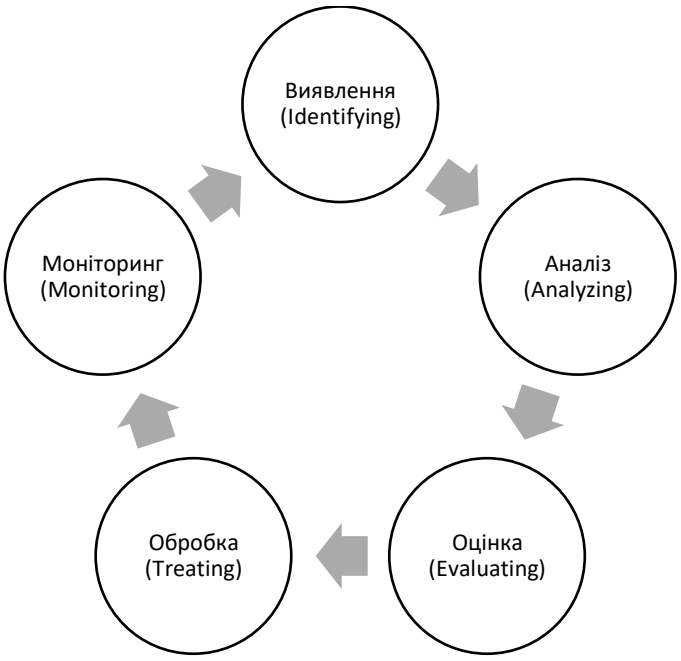

Рисунок 1.5 – Типовий цикл управління ризиками в ІБ

Перший етап – виявлення ризиків (Identification) – передбачає виявлення всіх потенційних загроз, вразливостей та активів, які можуть бути об’єктом

впливу. Цей етап ґрунтується на аналізі інфраструктури, опитуванні персоналу, аудитах, перегляді інцидентів та загальній обізнаності про сучасні кіберзагрози.

Другий етап – аналіз ризиків (Analysis) – спрямований на встановлення причинно-наслідкових зв'язків між виявленими загрозами та можливими наслідками їх реалізації. Тут проводиться деталізована оцінка характеристик загроз, вразливостей і критичності активів, використовуючи як якісні, так і кількісні методи [17].

Третій етап – оцінка ризиків (Evaluation) – полягає у зіставленні фактичного рівня ризику з визначеними критеріями прийнятності. Це дає змогу класифікувати ризики за ступенем пріоритетності (низький, середній, високий) та визначити, чи потребують вони негайної обробки або можуть бути прийняті.

Четвертий етап – обробка ризиків (Treatment) – передбачає вибір і впровадження стратегії управління: уникнення, зниження, передача (наприклад, страхування) або прийняття ризику. У цьому етапі здійснюються організаційні, технічні, правові та інші заходи, спрямовані на зниження впливу або ймовірності реалізації ризику [45].

П'ятий етап – моніторинг і перегляд (Monitoring & Review) – забезпечує постійне відстеження ефективності вжитих заходів, контроль за змінами в ризиковому середовищі та повторну оцінку ризиків у разі потреби. Цей етап є циклічним і тісно пов'язаний із періодичними аудитами та оновленням політик безпеки [16].

Отже, управління ризиками в інформаційній безпеці є динамічним безперервним процесом, що потребує гнучкої адаптації до нових загроз, змін в IT-інфраструктурі та зовнішньому середовищі. Застосування чіткої структури дозволяє забезпечити своєчасну реакцію на ризики, зберігаючи цілісність, конфіденційність і доступність критичної інформації.

Управління ризиками інформаційної безпеки вимагає не лише загальної структурованості процесу, а й застосування перевірених, стандартизованих методологічних підходів. На міжнародному рівні розроблено низку методологій, які забезпечують уніфіковане бачення процесів оцінки та обробки ризиків, і

можуть бути адаптовані до специфіки конкретної організації. Серед найбільш авторитетних методологій, що знайшли широке практичне застосування, варто виокремити ISO/IEC 27005, NIST SP 800-30, OCTAVE та EBIOS.

ISO/IEC 27005 є найбільш комплексним і водночас гнучким стандартом для управління ризиками в контексті системи управління інформаційною безпекою (СУІБ), описаної в ISO/IEC 27001. Він визначає логіку процесу управління ризиками: від встановлення контексту до моніторингу, при цьому не нав'язуючи конкретних технік оцінки, що дозволяє адаптувати метод до різних організаційних умов [62].

NIST SP 800-30, розроблений Національним інститутом стандартів і технологій США, фокусується на оцінці ризиків у державному секторі, але застосовується й приватними компаніями. Цей документ пропонує чіткий поділ процесу на етапи: ідентифікація активів, аналіз загроз, оцінка вразливостей, аналіз впливу та ймовірності, що дозволяє провести формалізовану кількісну або якісну оцінку.

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) – методологія, розроблена університетом Карнегі-Меллон, орієнтована переважно на середній і великий бізнес. Вона базується на ідентифікації критично важливих активів і загроз через опитування персоналу та експертну оцінку. OCTAVE робить акцент на стратегічному підході до ризиків, забезпечуючи інтеграцію ІБ у загальну управлінську політику організації [19].

EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) — метод, розроблений у Франції, широко застосовується в європейських країнах. Його особливістю є акцент на початкових фазах – ідентифікації безпекових потреб, аналізі контексту та вимог. EBIOS відзначається формалізованим підходом до формування обґрунтованих заходів захисту, що особливо корисно для критичної інфраструктури та державного сектору.

Обраний метод управління ризиками має ґрунтуватися на Наприклад, підприємство, сертифіковане організаційній структурі, ресурсах, рівні цифрової зрілості та регуляторних вимогах. за ISO/IEC 27001, логічно орієнтуватиметься

на ISO/IEC 27005; державні установи — на NIST або EBIOS; а компанії з високим рівнем внутрішньої експертизи — на OCTAVE (див. табл. 1.6).

Таблиця 1.6 – Порівняльна характеристика методологій управління ризиками в ІБ

Методологія	Розробник	Основні особливості	Сильні сторони	Обмеження / Недоліки
ISO/IEC 27005	ISO / IEC	Гнучка структура; адаптація до ISO 27001	Міжнародне визнання, сумісність із іншими стандартами	Не містить конкретних інструментів аналізу
NIST SP 800-30	NIST (США)	Формалізована кількісна оцінка	Деталізований підхід, підтримка з боку уряду	Складність для малих організацій
OCTAVE	Carnegie Mellon Univ.	Орієнтація на активи; експертна оцінка	Врахування організаційного контексту, масштабованість	Суб'єктивність оцінки, складна адаптація
EBIOS	ANSSI (Франція)	Визначення потреб і цілей безпеки	Поглиблений аналіз контексту, зручний для державних структур	Висока формалізація, менш гнучкий для бізнесу

Джерело: узагальнено автором на основі даних [17, 19]

У подальших підпунктах доцільно детально розглянути конкретні методи аналізу ризиків, які реалізуються в рамках згаданих методологій [26].

Процес аналізу ризиків в інформаційній безпеці базується на виявленні та осмисленні всіх можливих загроз, вразливостей і їхнього впливу на функціонування ІТ-систем. У практиці управління ризиками застосовуються методи як якісного, так і кількісного характеру, які дозволяють систематизувати ризики, оцінити ймовірність їх реалізації та прогнозувати масштаби наслідків. Вибір методу залежить від цілей аналізу, складності системи, обсягу доступної інформації та рівня обізнаності персоналу [39].

Одним з найпоширеніших якісних методів є SWOT-аналіз, що використовується для загального стратегічного аналізу системи безпеки. Він передбачає виявлення сильних (Strengths) і слабких сторін (Weaknesses) внутрішнього середовища, а також можливостей (Opportunities) та загроз (Threats) із зовнішнього середовища. У сфері ІБ SWOT-аналіз допомагає сформулювати стратегії розвитку безпеки, виходячи з виявлених факторів.

Більш структурованим методом є FMEA (Failure Modes and Effects Analysis) — аналіз видів і наслідків відмов. Цей метод дозволяє визначити потенційні точки відмови в системі, описати їхні причини та оцінити вплив на функціонування. Для кожної потенційної відмови обчислюється індекс пріоритету ризику (RPN) за формулою [47]:

$$RPN = S \times O \times D$$

де:

S — серйозність наслідків (Severity),

O — ймовірність появи (Occurrence),

D — імовірність виявлення до виникнення проблеми (Detection). Цей індекс дозволяє ранжувати ризики та визначати пріоритетність реагування.

Іншим потужним інструментом є аналіз дерева відмов (FTA — Fault Tree Analysis). Він ґрунтується на побудові логічної діаграми, яка демонструє причинно-наслідкові зв’язки між базовими подіями та головною небажаною подією [7]. FTA є особливо ефективним у випадках складних систем, де важливо визначити мінімальні набори умов, що призводять до критичного порушення (див. рис. 1.6).

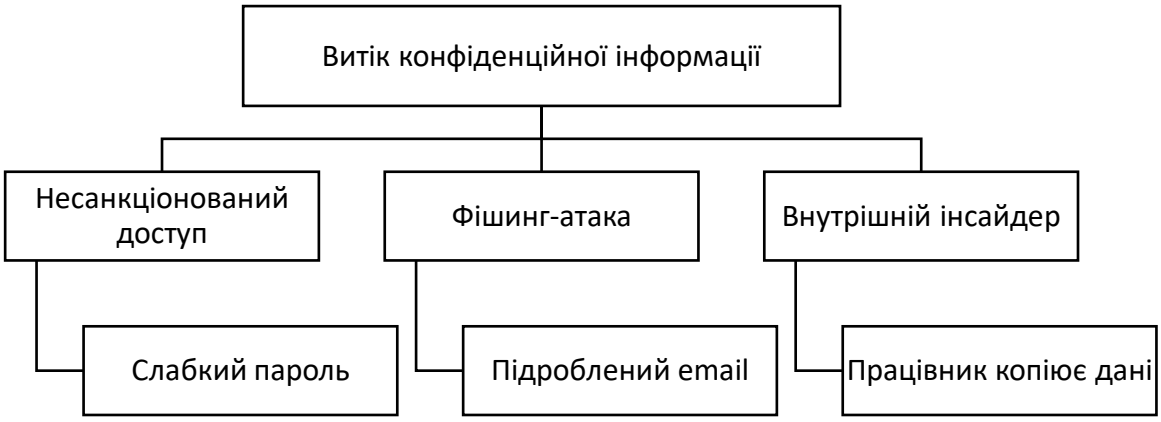

Рисунок 1.6 – Приклад дерева відмов для ризику «витік конфіденційної інформації»

У випадках, коли є достатньо статистичних даних, застосовуються кількісні методи — аналіз очікуваних втрат (Expected Loss), імітаційне моделювання, аналіз на основі сценаріїв. Вони дозволяють виразити рівень

ризику у вартісних показниках, що полегшує включення управління ІБ до загального фінансового планування організації [19].

Загалом, застосування комбінованих підходів (наприклад, FMEA + SWOT або FTA + сценарний аналіз) дозволяє досягти більшої точності в оцінці ризиків та гнучкості у виборі методів управління. Для організацій, що прагнуть сертифікації за ISO/IEC 27001, використання таких методів не є обов'язковим, але суттєво покращує обґрунтованість прийнятих рішень.

У процесі управління ризиками в інформаційній безпеці важливим етапом після їх ідентифікації, аналізу та оцінки є визначення прийнятності виявлених ризиків. Прийнятність ризику означає рівень, за якого організація свідомо погоджується з існуванням певного ризику без потреби вжиття негайних заходів щодо його зниження. Це рішення ґрунтується на балансі між витратами на захист та ймовірністю/масштабом потенційної шкоди [17].

У міжнародній практиці, зокрема в стандартах ISO/IEC 27005 та ISO 31000, прийнятність ризику тісно пов'язана з контекстом організації: її ресурсами, регуляторними вимогами, критичністю активів та рівнем загроз. Тому прийнятність завжди визначається в індивідуальному порядку, однак для цього існують усталені методичні підходи, серед яких особливо поширеним є принцип ALARP (As Low As Reasonably Practicable).

Згідно з підходом ALARP, ризик є прийнятним у тому випадку, якщо він зведений до такого рівня, який є настільки низьким, наскільки це розумно можливо, з урахуванням доступних засобів, витрат і технологій. Іншими словами, ризик не повинен бути повністю усунений (що часто технічно або економічно неможливо), але має бути мінімізований до рівня, за якого додаткове зниження є економічно недоцільним або надмірно витратним. [19]

$$R \leq R_{\text{допустимий}} \Rightarrow \text{ризик вважається прийнятним}$$

де:

R — фактичне значення оціненого ризику,

$R_{допустимий}$ — встановлений поріг допустимого рівня ризику.

Високий ризик потребує негайного реагування, оскільки загрожує критичним активам і порушує ключові процеси організації. Середній ризик може бути допущений, але лише за умови наявності ефективного моніторингу або реалізації плану мінімізації. Низький ризик, як правило, приймається організацією без додаткових заходів, оскільки витрати на його усунення перевищують очікувану шкоду [32].

Усі рішення щодо прийнятності ризику мають бути задокументовані у відповідних регламентах або політиках інформаційної безпеки та узгоджені з керівництвом. Це не лише підтверджує прозорість процесу, але й забезпечує підзвітність та можливість перегляду рішень у майбутньому.

Після завершення етапу оцінювання ризиків та визначення їхньої прийнятності організація переходить до ключового практичного етапу — вибору та впровадження відповідної стратегії реагування. Метою цього етапу є мінімізація ймовірності або впливу ризику до рівня, що вважається допустимим у межах політики інформаційної безпеки. [20]

У міжнародній практиці управління ризиками, зокрема в контексті стандартів ISO/IEC 27005 та ISO 31000, визначено чотири базові стратегії реагування [54]:

1. Уникнення ризику (Risk Avoidance). Полягає у повній відмові від дій або процесів, які пов’язані з неприйнятним ризиком. Ця стратегія застосовується у випадках, коли вплив ризику є критичним, а витрати на його зменшення надто високі або технічно неможливі. Наприклад, компанія може вирішити не зберігати чутливі персональні дані взагалі, щоб уникнути пов’язаних з цим ризиків.

2. Зниження ризику (Risk Mitigation). Найбільш поширена стратегія, яка передбачає впровадження заходів, спрямованих на зменшення ймовірності реалізації ризику або зниження його негативного впливу. Це можуть бути технічні (захисні системи, брандмауери, резервне копіювання), організаційні (навчання персоналу, політики доступу), правові або процедурні заходи.

3. Передача ризику (Risk Transfer). Включає делегування частини відповідальності за ризик іншій стороні, зокрема через страхування, аутсорсинг або договірні зобов'язання. Наприклад, передача обробки фінансових транзакцій спеціалізованій платіжній системі, яка має вищий рівень захисту.

4. Прийняття ризику (Risk Acceptance). Вибір цієї стратегії означає, що організація усвідомлює наявність ризику, але свідомо вирішує не вживати додаткових заходів, визнаючи його прийнятним. Такий підхід застосовується до ризиків із низьким рівнем ймовірності або незначними наслідками, а також у разі, коли вартість контролю перевищує очікувані збитки.

Для систематизації особливостей кожної зі стратегій доцільно представити їх у зведеній таблиці (див. табл. 1.7) .

Таблиця 1.7 – Порівняльний аналіз стратегій управління ризиками

Стратегія реагування	Опис механізму	Коли доцільно застосовувати	Приклади заходів
Уникнення	Усунення активності, пов'язаної з ризиком	Ризик критичний, захист — економічно неможливий	Відмова від зберігання ПІД, закриття сервісу
Зниження	Впровадження захисних заходів	Ризик можна частково контролювати або зменшити	Шифрування, доступ за ролями, навчання
Передача	Делегування ризику іншій стороні	Висока ймовірність ризику, складно контролювати	Страхування ІБ, хмарні сервіси, зовнішній аудит
Прийняття	Усвідомлення ризику без додаткових заходів	Ризик незначний, витрати на захист перевищують шкоду	Моніторинг подій, документація рішення

Джерело: узагальнено автором на основі даних [17, 22]

Вибір стратегії завжди повинен ґрунтуватися на всебічному аналізі контексту: чутливості активів, вартості реалізації заходів, потенційного впливу на бізнес-процеси та наявності внутрішніх ресурсів. У багатьох випадках організація може комбінувати стратегії — наприклад, частково знижуючи ризик технічними заходами, а частково передаючи відповідальність на підставі договору.

Отже, обрані стратегії мають бути задокументовані, обґрунтовані й підкріплені відповідними політиками, що дозволить забезпечити їх реалізацію на всіх рівнях управління [33].

Ефективне управління ризиками в інформаційній безпеці потребує не лише наявності методологічної бази та технічних засобів, але й чіткої структури відповідальності. Саме розподіл ролей і повноважень між учасниками процесу забезпечує координацію дій, своєчасне реагування на загрози та підтримання безперервного контролю за станом ризиків.

Згідно зі стандартами ISO/IEC 27001 і ISO/IEC 27005, а також рекомендаціями NIST SP 800-39, управління ризиками має бути інтегрованим в організаційну структуру та охоплювати всі рівні — стратегічний, тактичний і операційний. Кожен рівень має свої завдання та функціональні обов’язки.

На стратегічному рівні ключову роль відіграє керівництво організації (top management), яке відповідає за [25]:

— формування політики безпеки;

— затвердження допусків до рівнів ризику;

— визначення ресурсів;

— контроль за реалізацією програм з ІБ.

Офіцер інформаційної безпеки (*Chief Information Security Officer, CISO*) або інший призначений керівник відповідає за тактичне управління ризиками. Його завдання — впровадження процедур оцінки та моніторингу ризиків, координація відповідальних осіб, аналіз інцидентів, ведення звітності [24].

Власники активів (Asset Owners) — працівники, які є відповідальними за певні IT-ресурси. Вони зобов’язані ідентифікувати ризики, пов’язані з цими активами, ініціювати заходи щодо їх зниження, та взаємодіяти з командою ІБ щодо оцінювання впливу.

Користувачі (End Users) — усі співробітники, які взаємодіють з інформаційними системами. Незважаючи на низький рівень ієрархічної відповідальності, саме їхні дії часто стають точкою входу для реалізації ризиків (через фішинг, порушення політик, небезпечну поведінку). Тому важливо, щоб користувачі були проінформовані про загальні правила безпеки та знали, як діяти у разі інциденту [33].

У деяких організаціях також створюються комітети з інформаційної безпеки або внутрішні групи з управління ризиками, які здійснюють періодичний перегляд політик, результатів аудиту, індикаторів ефективності (KPI) тощо (див. рис. 1.7).

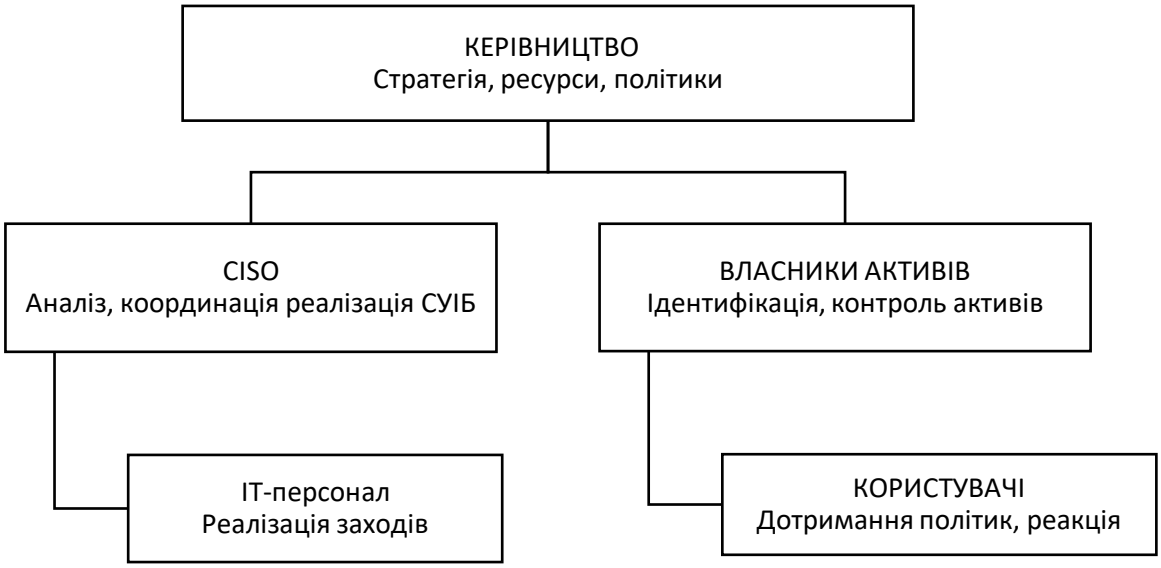

Рисунок 1.7 – Ролі та відповідальність в управлінні ризиками ІБ

Усі ролі мають бути формалізовані у внутрішніх документах (наприклад, положеннях про СУІБ, посадових інструкціях, планах реагування на інциденти), що дозволяє [8]:

— забезпечити підзвітність;
— уникати подвійного тлумачення обов’язків;
— підтримувати ефективну взаємодію між підрозділами.

Отже, ефективне управління ризиками інформаційної безпеки ґрунтується на чітко структурованій послідовності дій: виявлення, аналізу, оцінювання, обробки та моніторингу ризиків. Міжнародні стандарти, зокрема ISO/IEC 27005, NIST SP 800-30, OCTAVE та EBIOS, пропонують різні, але взаємодоповнюючі підходи до реалізації цих етапів. Вибір методів аналізу — SWOT, FMEA, дерево відмов тощо — дозволяє адаптувати процес до конкретного рівня загроз і ресурсних можливостей організації. Ключовим елементом управління є визначення прийнятності ризиків відповідно до принципу ALARP та вибір відповідної стратегії реагування: уникнення, зниження, передача або прийняття.

Не менш важливою складовою є чіткий розподіл організаційних ролей, що забезпечує узгодженість дій усіх учасників системи ІБ. Такий підхід формує підґрунтя для переходу до практичної частини дослідження, де відбувається адаптація методів до конкретних умов функціонування об'єкта захисту.

РОЗДІЛ 2 АНАЛІЗ ПРОЦЕСУ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Процес і етапи управління ризиками інформаційної безпеки

Управління ризиками інформаційної безпеки не може бути ефективним без чітко побудованої моделі реалізації всіх етапів цього процесу в межах IT-інфраструктури підприємства [48]. Така модель повинна бути адаптивною до реального середовища: типів активів, специфіки бізнес-процесів, а також технічних і людських ресурсів компанії (див. рис. 2.1).

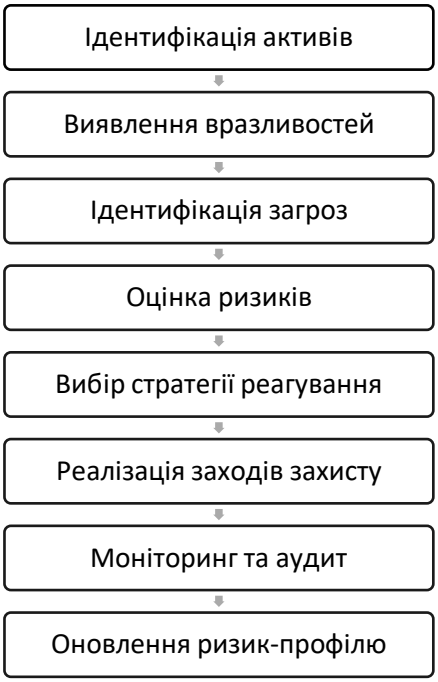

Рисунок 2.1 – Схема реалізації ризик-менеджменту в IT-середовищі підприємства

Розглянемо впровадження системи управління ризиками в умовах середнього IT-компанії, яка надає послуги в галузі цифрового маркетингу. Інфраструктура компанії включає:

— два фізичних сервери для зберігання даних;
— приватну хмару (на базі VMware) з розміщенням віртуальних машин для тестування;
— CRM-систему для взаємодії з клієнтами;
— понад 50 робочих станцій працівників;

— офісну мережу Wi-Fi із гостьовим доступом;

— кілька VPN-тунелів для віддаленої роботи [17].

Першим кроком було проведення інвентаризації активів: всі елементи інфраструктури були задокументовані з прив’язкою до відповідальних осіб. Далі із використанням OpenVAS було здійснене сканування вразливостей — виявлено критичну уразливість у CRM через застарілу бібліотеку обробки API-запитів.

За формулою оцінки ризику *(R = P × I)*, ризик був класифікований як високий. Прийнято рішення про його зниження — встановлено оновлення CRM, змінено політику доступу та активовано двофакторну автентифікацію. Усі дії задокументовано в системі обліку ризиків (Risk Register), а далі через місяць проведено повторне сканування й аудит ефективності [13].

Паралельно, для менш критичних активів, наприклад робочих станцій дизайнерів, ризики залишились на середньому рівні та були прийняті без додаткових заходів, але з обов’язковим щоквартальним моніторингом (див. табл. 2.1).

Таблиця 2.1 – Перелік інформаційних активів із класифікацією за критичністю (CIA)

№	Назва активу	Тип	Конфіденційність	Цілісність	Доступність	Власник
1	CRM-система	Програмне	Висока	Висока	Середня	Відділ продажів
2	Сервер бази даних	Апаратне	Висока	Висока	Висока	IT-відділ
3	Сайт компанії	Хмарне	Середня	Середня	Висока	Маркетинг
4	Робочі станції дизайнерів	Апаратне	Низька	Середня	Середня	Відділ креативу
5	VPN-доступ до внутрішньої мережі	Логічний	Висока	Висока	Висока	CISO

Джерело: узагальнено автором на основі даних [39]

У результаті впровадження моделі управління ризиками вдалося підвищити рівень прозорості ІБ-процесів, мінімізувати ризики, пов’язані з витоком клієнтських даних, та сформувати культуру обізнаності серед персоналу.

Першим кроком була підготовка переліку активів, які мають інформаційне значення для компанії. Сюди включено обладнання, дані, системи, мережі та сервіси, що забезпечують функціонування критичних бізнес-процесів [36].

Для виявлення та обліку активів на підприємстві було використано спеціалізоване програмне забезпечення Lansweeper. Система автоматично ідентифікує пристрої в мережі, фіксує їхні технічні характеристики та зберігає результати в централізованому репозиторії. На рисунку 2.2 представлено приклад інтерфейсу, який використовується для перегляду інвентаризованих активів.

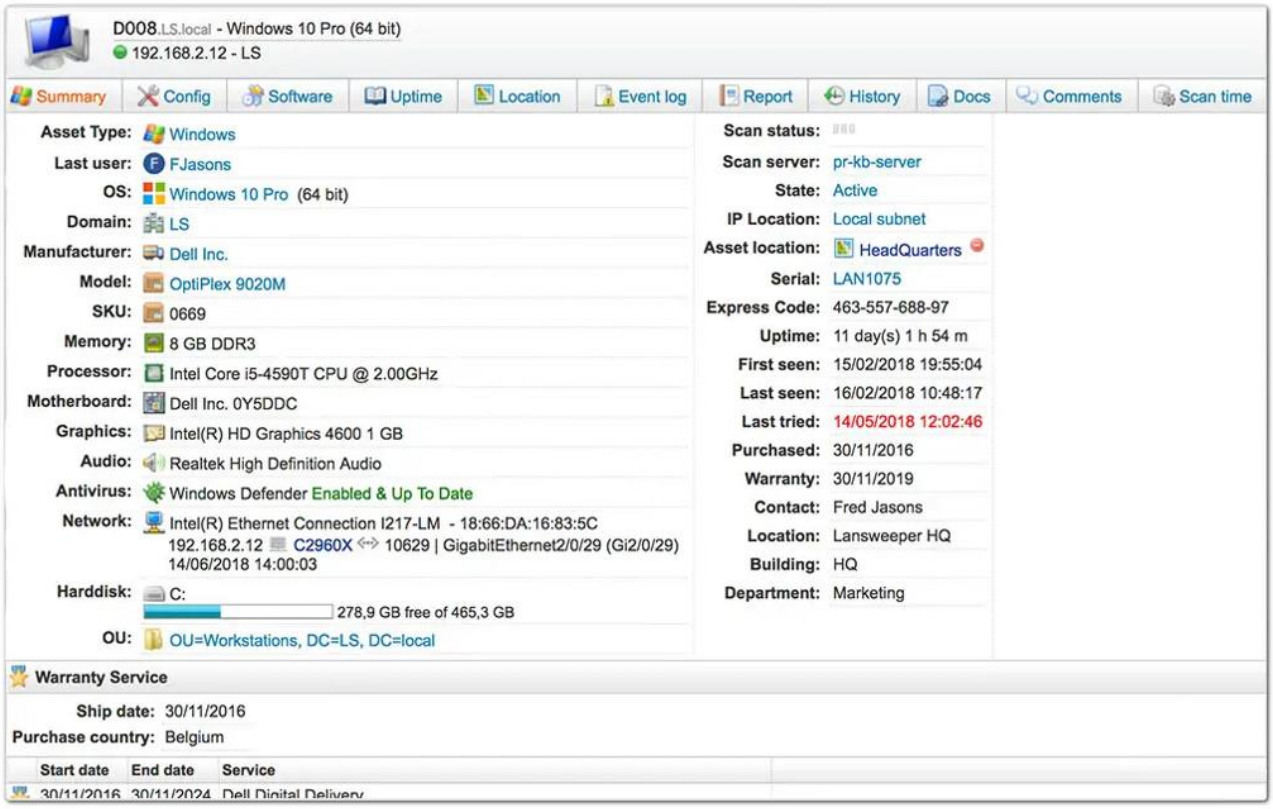

Рисунок 2.2 – Інтерфейс системи виявлення активів Lansweeper

Завдяки такому інструменту IT-відділ має змогу оперативно виявляти зміни в мережі, контролювати нові з’єднання та своєчасно ідентифікувати потенційно небезпечні компоненти. Зібрані дані лягли в основу подальшої побудови карти вразливостей (Таблиця 2.2) та формування профілю загроз [45].

Таблиця 2.2 – Приклади виявлених вразливостей

№	Актив	Вразливість	CVSS-бал	Метод виявлення	Потенційна загроза
1	CRM-система	Вразливість у бібліотеці auth.js	9.1	OpenVAS	Захоплення сесії, SQL-ін'єкція
2	Сервер БД	Відкритий порт 3306 без фаєрвола	7.5	Ручна перевірка	Несанкціонований доступ
3	Сайт компанії	Відсутність HTTPS	6.2	OWASP ZAP	Перехоплення даних, MITM
4	Робочі станції	Встановлене ПЗ без оновлень	4.8	Agent scan	Експлуатація старих вразливостей
5	VPN	Статичний пароль без MFA	8.6	Аудит доступу	Злам через підбір пароля

Джерело: узагальнено автором на основі даних [59]

Щоб побудувати карту ризиків, було змодельовано зв'язки між загрозами, які можуть використати наявні вразливості для впливу на активи (див. рис. 2.3).

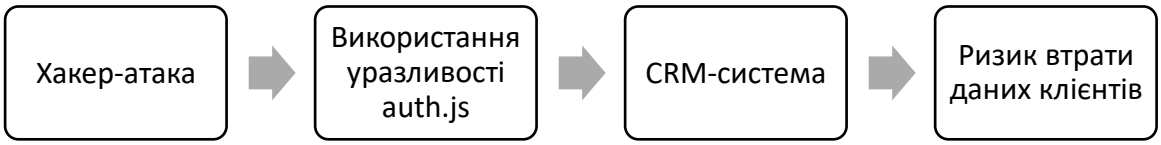

Рисунок 2.3 – Взаємозв'язок: загроза → вразливість → актив → ризик

Інші приклади:

— Природна загроза (стрибок напруги) → відсутність захисту електроживлення → сервер БД → ризик втрати доступу.

— Соціальна інженерія → використання статичного пароля → VPN-доступ → ризик проникнення у внутрішню мережу [16].

Завдяки поетапному виявленню активів, вразливостей та потенційних загроз вдалося створити повноцінну базу для подальшої оцінки ризиків. Зібрані дані закладено в основу реєстру ризиків, який буде оновлюватись після кожної ітерації сканування та аудиту. Це дозволяє компанії не лише реагувати на інциденти, а й проактивно керувати потенційними ризиками, що формуються внаслідок змін інфраструктури або зовнішніх чинників.

Після виявлення активів, вразливостей і потенційних загроз наступним логічним етапом є аналіз ризиків. Він дозволяє визначити, які саме комбінації «загроза + вразливість + актив» створюють найбільшу небезпеку для підприємства, і які з них потребують негайного реагування. У цьому підпункті буде проведено розрахунок ризику для обраних кейсів, сформовано таблицю

оцінки та побудовано дерево ризику для візуального представлення причинно-наслідкових зв’язків [46].

Для оцінювання ризику використано базову формулу:

$$R = P \times I$$

де:

R — загальний рівень ризику,

P — ймовірність реалізації загрози (від 1 до 5),

I — рівень впливу на організацію (від 1 до 5).

Розглянемо приклад для CRM-системи, в якій виявлено критичну вразливість (auth.js).

— Ймовірність реалізації загрози (P): 5 — оскільки веб-додаток доступний ззовні.

— Вплив на систему (I): 5 — витік даних клієнтів призведе до фінансових втрат і репутаційної шкоди [12].

$$R = 5 \times 5 = 25$$

Цей ризик класифікується як високий і потребує негайного реагування (див. табл. 2.3).

Таблиця 2.3 – Матриця ризиків для ключових активів підприємства

№	Актив	Загроза	Вразливість	P	I	R (P×I)	Рівень ризику
1	CRM-система	Злом через публічний доступ	Вразливий auth.js	5	5	25	Високий
2	Сервер БД	Несанкціонований доступ	Відкритий порт	4	5	20	Високий
3	Сайт компанії	Перехоплення даних	Відсутність HTTPS	3	4	12	Середній
4	Робоча станція	Malware	Відсутність оновлень	3	3	9	Середній
5	VPN-доступ	Підбір пароля	Статичний пароль без MFA	4	5	20	Високий

Джерело: узагальнено автором на основі даних [14]

Щоб краще зрозуміти логіку реалізації ризику, було побудовано дерево відмов для ситуації з CRM-системою. Така модель дозволяє візуалізувати, які саме події можуть призвести до небажаного інциденту (див. рис. 2.4).

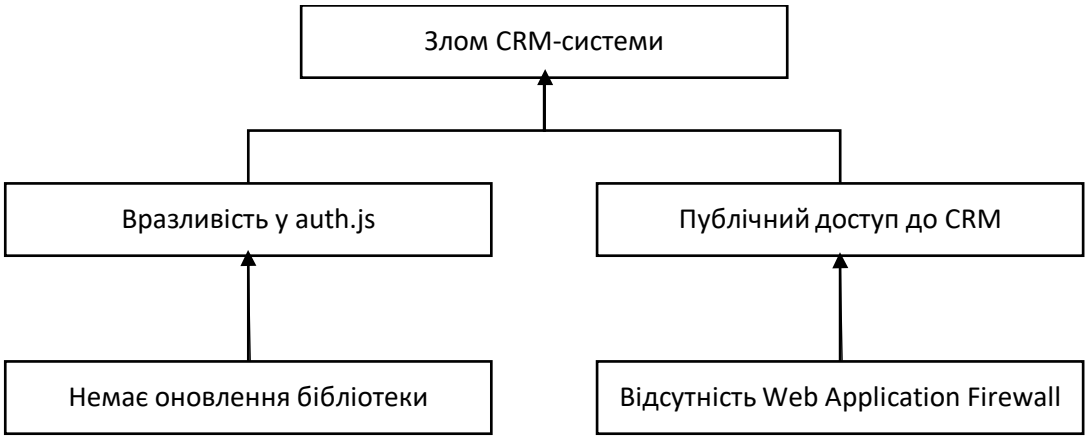

Рисунок 2.4 – Дерево ризику для CRM-системи (злом через auth.js)

Завдяки аналізу ризиків стало можливим сформувати пріоритети в управлінні безпекою: найбільш критичні сценарії (CRM, VPN, БД) були винесені на перше місце в план реагування [13].

Після первинного аналізу ризиків наступним кроком стало їх кількісне ранжування з метою подальшого прийняття рішень щодо реагування. Для цього були використані дві методики: кольорова матриця ризиків (heatmap) та оцінка критичності ризику за методом RPN (Risk Priority Number).

На основі розрахунку $R=P\times I$ (ймовірність × вплив), для кожного кейсу було визначено індекс ризику, який зафіксовано в таблиці, де кольором виділено рівень загрози (див. табл. 2.3).

Таблиця 2.3 – Матриця ризику (heatmap)

Вплив ↓ / Ймовірність →	1	2	3	4	5
5 (Критичний)	5 – Низький	10 – Середній	15 – Середній	20 – Високий	25 – Високий
4 (Високий)	4 – Низький	8 – Низький	12 – Середній	16 – Середній	20 – Високий
3 (Середній)	3 – Низький	6 – Низький	9 – Середній	12 – Середній	15 – Середній
2 (Незначний)	2 – Низький	4 – Низький	6 – Низький	8 – Низький	10 – Середній
1 (Мінімальний)	1 – Низький	2 – Низький	3 – Низький	4 – Низький	5 – Низький

Джерело: узагальнено автором на основі даних [18]

Примітка: Пояснення кольорів:

— 1–6: Низький ризик

— 7–15: Середній ризик

— 16–25: Високий ризик

Для більш детального підходу був використаний метод FMEA (Failure Modes and Effects Analysis), що дозволяє вивести числове значення пріоритетності ризику (див. табл. 2.4):

$$RPN = S \times O \times D$$

де:

— *S (Severity)* — серйозність наслідків

— *O (Occurrence)* — ймовірність виникнення

— *D (Detection)* — здатність виявити ризик до того, як він реалізується

Таблиця 2.4 – Розрахунок RPN для вибраних активів

№	Актив	S (1-10)	O (1-10)	D (1-10)	RPN	Пріоритет
1	CRM-система	9	9	3	243	Критичний
2	Сервер БД	10	8	4	320	Критичний
3	Сайт	7	6	5	210	Високий
4	Робоча станція	5	5	6	150	Середній
5	VPN	8	8	2	128	Високий

Джерело: узагальнено автором на основі даних [19]

Для розмежування рівнів ризику використовувалась така шкала:

— RPN ≥ 250 – критичний (негайне реагування)

— 150 ≤ RPN < 250 – високий (впровадження заходів у короткі строки)

— 80 ≤ RPN < 150 – середній (контроль і поступове зниження)

— RPN < 80 – низький (прийнятний ризик)

Після того як ризики було оцінено та класифіковано за рівнем критичності, наступним кроком стало формування конкретного плану реагування. Такий план має на меті мінімізувати ризики до прийнятного рівня, визначити, *хто, коли і що саме* повинен зробити у випадку їх реалізації або ще до неї [7].

Для кожного з пріоритетних ризиків було визначено стратегію реагування (уникнення, зниження, передача або прийняття), перелік заходів, відповідальних осіб, строки виконання та засоби контролю (див. табл. 2.5).

Таблиця 2.5 – План реагування на ризики інформаційної безпеки

№	Ризик (опис)	Рівень	Стратегія	Заходи реагування	Відповідальний	Строк виконання	Статус
1	Злом CRM через auth.js	Високий	Зниження	Оновити бібліотеку, обмежити доступ, MFA	DevOps / CISO	3 робочі дні	У процесі
2	Несанкціонований доступ до БД	Високий	Зниження	Закрити порти, налаштувати firewall	IT-інженер	5 робочих днів	Не почато
3	Перехоплення даних з сайту	Середній	Зниження	Встановити SSL-сертифікат	Веб-адміністратор	1 день	Виконано
4	Відсутність MFA при VPN-доступі	Високий	Зниження	Упровадити двофакторну автентифікацію	CISO / системний адм.	2 дні	У процесі
5	Вразливості на робочих станціях	Середній	Прийняття	Моніторинг, планове оновлення	Відділ підтримки	Постійно	Активний

Джерело: узагальнено автором на основі даних [17, 19]

У практиці важливо не лише знати, що робити, а й *коли* це слід робити. Для цього була побудована логічна блок-схема сценаріїв прийняття рішень залежно від рівня ризику (див. рис. 2.5) [11].

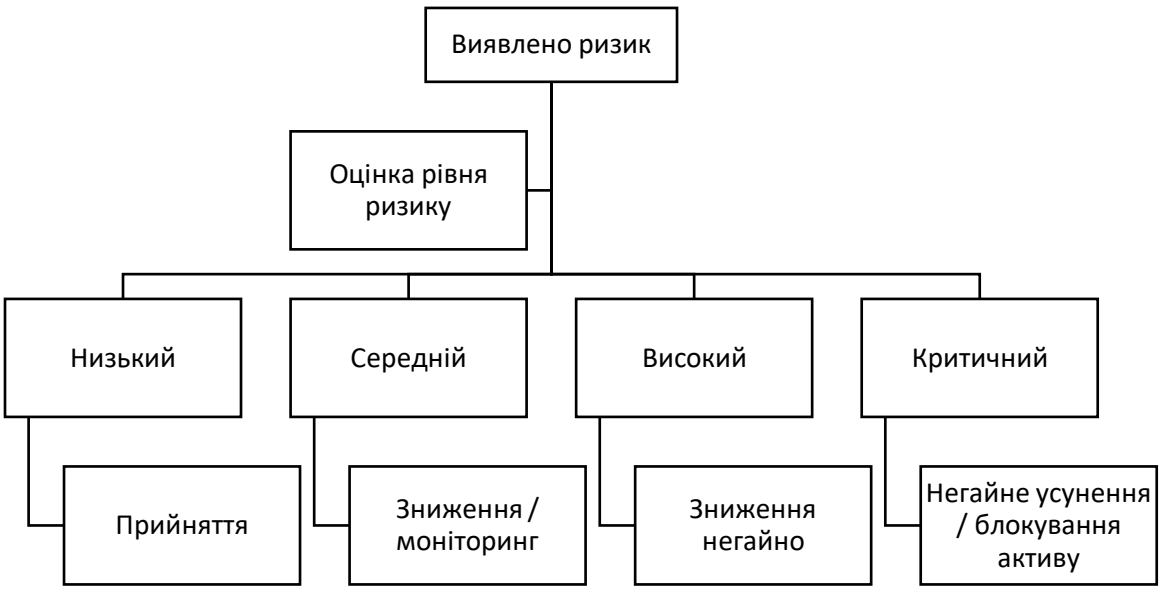

Рисунок 2.5 – Логіка реагування на ризики (decision-tree)

Для документування всіх дій використано систему управління ризиками, яка дозволяє в реальному часі моніторити статус кожного з них, бачити відповідальних та хід реалізації заходів.

Для ефективного управління ризиками організація використовує табличну форму реєстру ризиків (Risk Register). У ньому відображено опис ризику, його вплив та ймовірність, автоматично розраховується пріоритет ризику (impact × probability), а також фіксуються заходи реагування і відповідальні особи. На рисунку 2.6 представлено приклад інтерфейсу реєстру ризиків з типовими прикладами для аналізу (див. рис. 2.6).

RISK DESCRIPTION	IMPACT DESCRIPTION	IMPACT LEVEL	PROBABILITY LEVEL	PRIORITY LEVEL	MITIGATION NOTES	OWNER
Brief summary of the risk.	What will happen if the risk is not mitigated or eliminated.	Rate 1 (LOW) to 5 (HIGH)	Rate 1 (LOW) to 5 (HIGH)	(IMPACT X PROBABILITY) Address highest first.	What can be done to lower or eliminate the impact or probability.	Who's responsible?
Leaks from roof during rain make the floor slippery	Slips and falls	3	5	15	– Order "slippery when wet" signs – Have mops on hand – Fix roof	Allen
Shortage of eye protection	Increase in injuries Production delayed Increased insurance premiums	5	1	5	– Increase supply – Low inventory warnings – Find alternative suppliers	Linda
		4	5	20		
		5	5	25		
		2	1	2		
		3	4	12		
		1	1	1		
		2	4	8		
		4	4	16		

Рисунок 2.6 – Інтерфейс системи управління ризиками (Risk Register)

Рисунок 2.6 демонструє оцінку ризиків за п’ятибальною шкалою впливу та ймовірності. Стовпець «Priority Level» автоматично розраховує значення ризику, яке потім візуалізується у вигляді кольорової сітки (heatmap), поданої в правому нижньому куті. [19]

Наприклад, ризик із показниками 5×5 має критичний рівень (25) і підсвічується червоним, тоді як 2×1 (2) — зелений, тобто прийнятний. Усі ризики мають призначеного відповідального та супроводжуються короткими рекомендаціями з їхнього зниження.

Отже, на основі проведеного аналізу було сформовано повноцінний цикл управління ризиками в інформаційній безпеці на прикладі умовного підприємства. Ідентифіковано ключові інформаційні активи, виявлено вразливості за допомогою практичних інструментів (зокрема OpenVAS і Lansweeper), здійснено оцінку ризиків за формулою $R=P\times I$, а також за методом RPN. Побудовані heatmap та дерево відмов дозволили візуалізувати і пріоритезувати ризики. Реєстр ризиків з деталізованими планами реагування і логікою прийняття рішень створив основу для оперативного управління інцидентами безпеки. Таким чином, практичне застосування моделі управління ризиками забезпечило не лише виявлення загроз, але й формування системного підходу до їх зниження, моніторингу та контролю.

2.2. Методи оцінювання ризиків: кількісні та якісні підходи

У тих випадках, коли організація не має достатньо точних статистичних даних або ресурсу на складні математичні моделі, доцільним є використання якісної оцінки ризиків [36]. Вона базується на експертному судженні, колективному аналізі й суб'єктивних оцінках ідеї загроз, вразливостей та їхнього потенційного впливу на інформаційні активи (див. табл. 2.6).

Таблиця 2.6 — Методика STRIDE — класифікація загроз для веб сервісу

Категорія	Загроза	Приклад реалізації
S	Підміна особистості (Spoofing)	Зловмисник входить у CRM як менеджер
T	Підміна даних (Tampering)	Зміна даних клієнта через незахищену форму
R	Відмова від дій (Repudiation)	Користувач відмовляється від редагування замовлення
I	Розголошення інформації (Information Disclosure)	Витік бази через публічну API
D	Відмова в обслуговуванні (DoS)	Завантаження системи через масові запити
E	Підвищення прав (Elevation of Privilege)	Працівник отримує права адміністратора

Джерело: узагальнено автором на основі даних [37]

На прикладі умовного підприємства було проведено таку оцінку за участі співробітників IT-відділу, CISO та адміністраторів систем. Основний акцент

було зроблено на дві методики — OCTAVE та STRIDE, які дозволили системно ідентифікувати ризики без потреби у складних розрахунках.

На діаграмі 2.6 зображено взаємодію користувача з різними модулями CRM-системи та відповідні потенційні загрози за STRIDE. Наприклад, при доступі до даних клієнтів можливе розголошення інформації (I), при додаванні компанії — ризик підвищення привілеїв (E), а при вході — підміна особистості (S) (див. рис. 2.6).

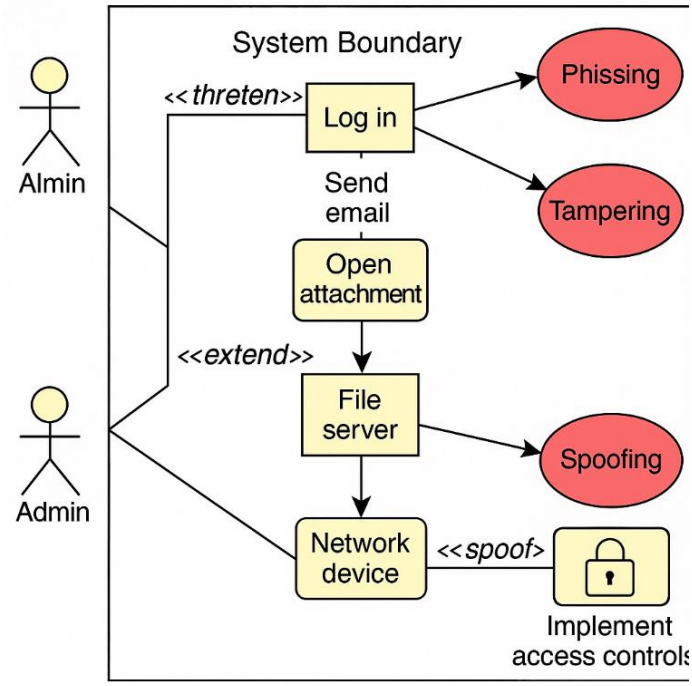

Рисунок 2.6 – Приклад використання методики STRIDE на умовному об'єкті

На відміну від якісного аналізу, кількісна оцінка ризиків дає змогу не лише визначити пріоритетність загроз, але й перевести рівень ризику у грошовий еквівалент, що особливо важливо при бюджетуванні заходів з інформаційної безпеки [48]. У цій частині оцінка проводилась за формулою очікуваних втрат (Expected Loss), яка широко застосовується в управлінні ІБ та IT-ризиками (див. табл. 2.7).

$$EL = S \times P \times AV$$

де:

— EL — очікувані втрати (грн);

— S — серйозність наслідків (від 1 до 5);

— *P* — ймовірність реалізації ризику (від 1 до 5);

— *AV* — вартість активу, на який впливає ризик (у грн).

Таблиця 2.7 – Розрахунок очікуваних втрат для трьох критичних ризиків

№	Опис ризику	S (1–5)	P (1–5)	Вартість активу (AV), грн	EL = S × P × AV (грн)	Коментар
1	Злом CRM через веб-уразливість	5	4	250 000	5 × 4 × 250 000 = 5 000 000	Найвищий фінансовий ризик
2	Несанкціонований доступ до БД	4	3	200 000	4 × 3 × 200 000 = 2 400 000	Потребує впровадження firewall та MFA
3	Фішинг серед працівників	3	4	120 000	3 × 4 × 120 000 = 1 440 000	Варто провести навчання

Джерело: створено автором на основі даних [3]

З наведених у Таблиці 2.7 розрахунків видно, що найсерйозніші фінансові наслідки можуть бути спричинені зломом CRM-системи. Для кращої візуалізації та обґрунтування пріоритетів у бюджетуванні захисних заходів було побудовано графік 2.7. Він демонструє, як змінюються очікувані втрати залежно від типу ризику, враховуючи їхню ймовірність, вплив і вартість відповідного активу [59].

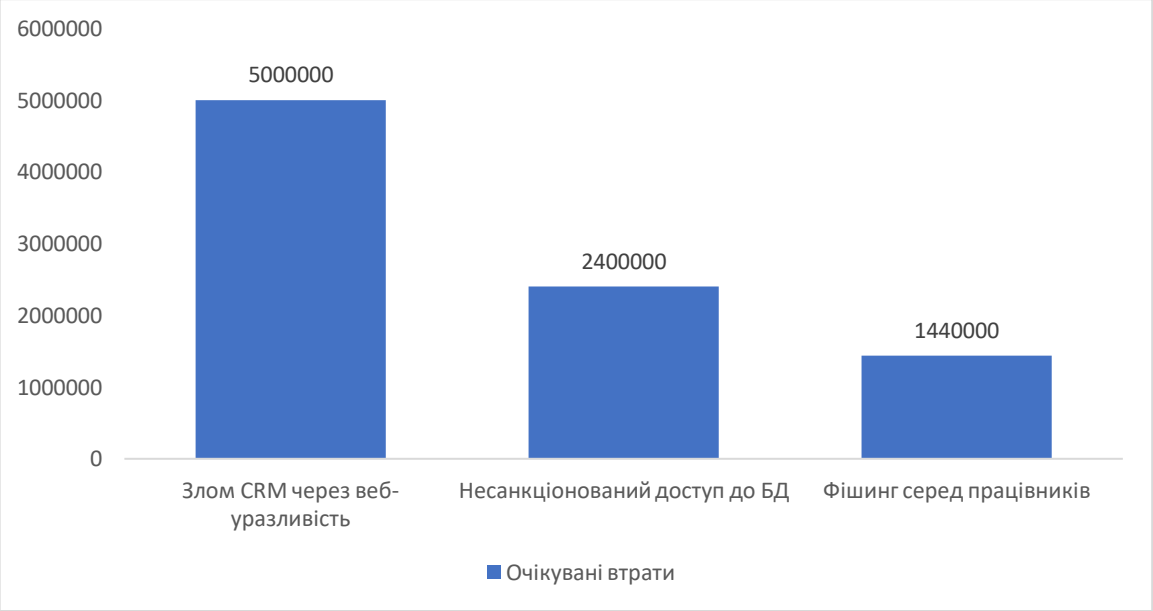

Рисунок 2.7 – Очікувані фінансові втрати за видами ризиків, грн

Очевидно, що навіть при однаковій ймовірності, різна цінність активів суттєво впливає на сумарні втрати. Це ще раз підкреслює важливість інвентаризації та пріоритезації об’єктів захисту [17]

У реальних умовах управління ризиками інформаційної безпеки часто недостатньо орієнтуватися лише на якісні або лише на кількісні методи. Оптимальним підходом є поєднання обох, що дає змогу врахувати як суб’єктивну думку експертів, так і об'єктивно обчислені втрати (див. табл. 2.8).

Таблиця 2.8 – Порівняння результатів якісного та кількісного підходів до оцінювання ризиків

№	Тип ризику	Якісна оцінка (рівень)	Кількісна оцінка (EL, грн)	Різниця в пріоритеті	Коментар
1	Злом CRM-системи	Високий	5 000 000	Співпадає	Пріоритет 1 у всіх методиках
2	Доступ до БД	Високий	2 400 000	Співпадає	Вимагає негайних дій
3	Фішинг працівників	Середній	1 440 000	У кількісній – вищий пріоритет	Неочікувана висока фінансова шкода
4	Витік через VPN	Високий	Немає точних даних	Неоцінений кількісно	Треба проводити додатковий аналіз
5	Відсутність резервних копій	Середній	900 000	Помірний ризик	Регулярна перевірка необхідна

Джерело: створено автором на основі даних [12]

У гібридному підході зручно використовувати програмні рішення, які дозволяють одночасно вести як кількісні, так і якісні параметри ризиків. Наприклад, в інструменті ISO 27005 Risk Manager або RSA Archer можна вводити дані з чек-листів, одночасно розраховуючи EL, RPN або інші показники (див. рис. 2.8).

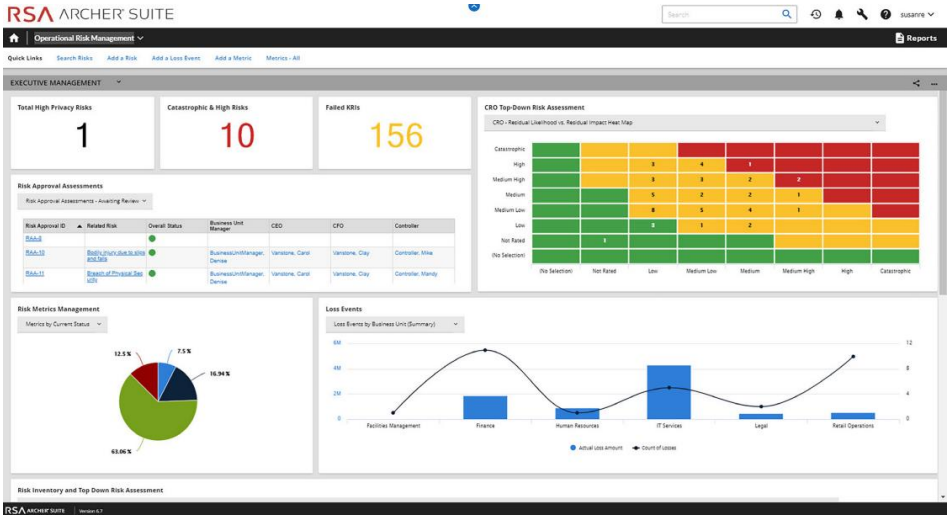

Рисунок 2.8 – Інтерфейс інструменту для змішаного оцінювання ризиків (Archer)

На рисунку 2.8 представлено приклад інтерфейсу системи Archer Risk Manager, який об’єднує якісну та кількісну оцінку ризиків на одній платформі. Панель керування містить динамічну heatmap, перелік ризиків за критичністю, контроль затвердження та детальну статистику втрат у розрізі бізнес-підрозділів. Це дозволяє CISO, CIO або risk manager’у приймати рішення оперативно та обґрунтовано, спираючись на візуалізовані дані [13].

Важливо розуміти, коли доцільно застосовувати той чи інший підхід. Це залежить від кількох чинників: наявності даних, терміновості рішення, доступності експертів тощо (див. рис. 2.9).

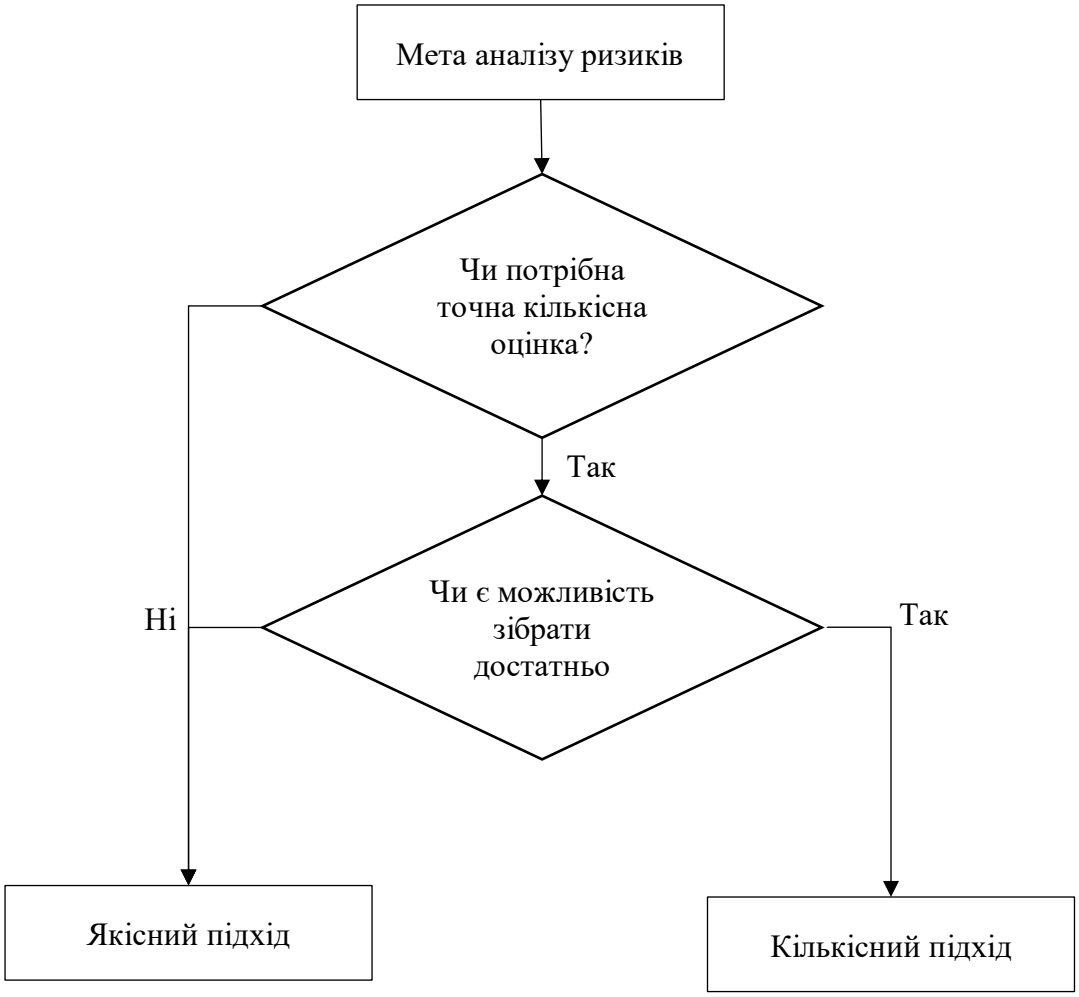

Рисунок 2.9 – Діаграма рішень: вибір методики оцінки ризиків

Змішане оцінювання дозволяє забезпечити більш гнучке й достовірне управління ризиками. Завдяки поєднанню методів підприємство може оптимізувати витрати на захист, мінімізуючи помилки, що виникають через

обмеженість лише одного підходу. Це особливо важливо в умовах швидкої зміни кіберзагроз, коли ризик потрібно оцінювати швидко, але надійно [36].

Отже, проведення якісної, кількісної та змішаної оцінки ризиків дозволило отримати комплексне уявлення про характер і масштаб потенційних загроз інформаційної безпеки. Якісний аналіз допоміг ідентифікувати критичні зони на основі суб'єктивної експертної думки, тоді як кількісні методи — розрахувати очікувані втрати у фінансовому вимірі. Гібридний підхід забезпечив гнучкість у виборі інструментів залежно від доступності даних, типу активів та терміновості рішень. Візуалізація результатів у вигляді heatmap, діаграм і скріншотів систем автоматизації управління ризиками підвищила зрозумілість для прийняття обґрунтованих управлінських дій. Отримані результати лягли в основу формування інструментів підтримки прийняття рішень, які розглядаються у наступному підрозділі.

2.3. Інструменти підтримки управління ризиками в ІБ

Для ефективного виявлення технічних ризиків в інформаційній системі першочергове значення має сканування вразливостей — автоматизований процес, який дозволяє виявити слабкі місця в IT-інфраструктурі до того, як ними скористається зловмисник [19].

На практиці було протестовано декілька найбільш розповсюджених інструментів: OpenVAS, Nessus та Qualys. Кожен із них має свої переваги й обмеження залежно від типу середовища, масштабів компанії, потреб інтеграції та бюджету (див. рис. 2.10).

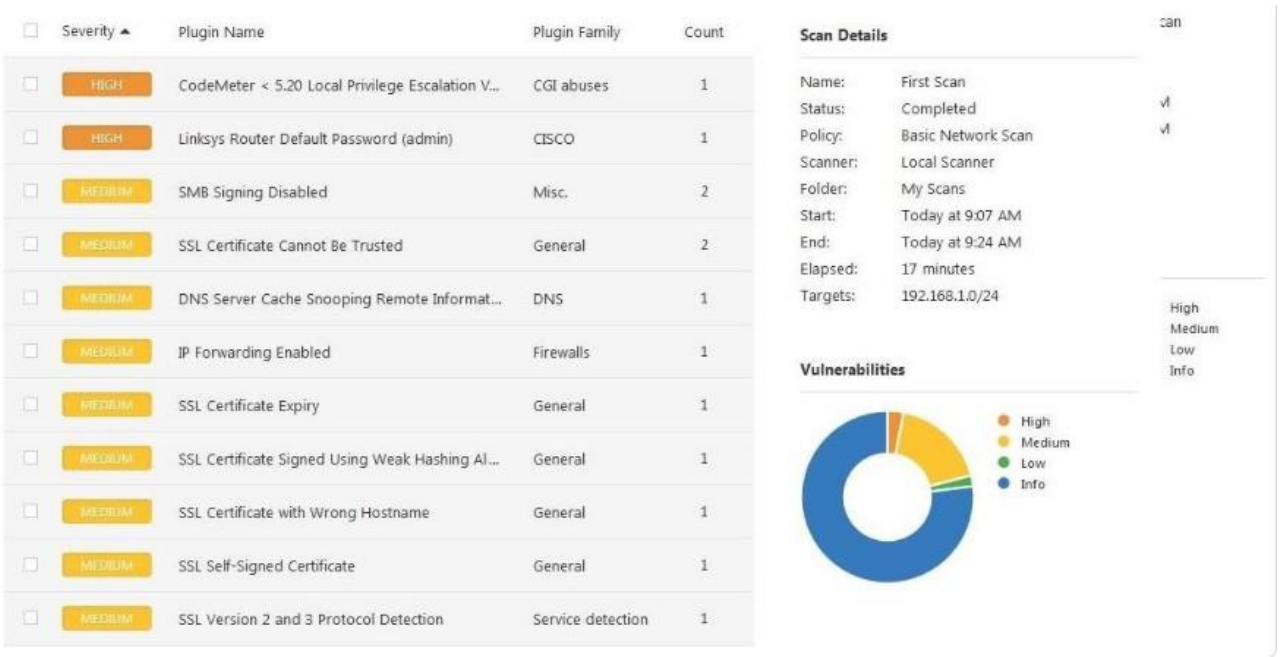

Рисунок 2.10 – Приклад звіту з Nessus

На рисунку 2.10 представлено фрагмент результатів сканування, де відображено критичні та середні вразливості, з деталізацією CVSS-балів, описом, рекомендаціями та CVE-посиланнями (див. табл. 2.9).

Таблиця 2.9 – Порівняльна характеристика сканерів вразливостей

Параметр	OpenVAS	Nessus	Qualys
Тип ліцензії	Безкоштовна (open-source)	Платна (є безкоштовна Pro)	Платна (SaaS, підписка)
Покриття CVE	~50 000+	~60 000+	~70 000+
Оновлення бази	Регулярне	Дуже часте	Автоматичне щоденне
Зручність інтерфейсу	Середня	Висока	Висока
Глибина сканування	Добра	Відмінна	Відмінна
Можливість інтеграції	Через API / SIEM / XML	Так (Tenable.io)	Так (з SIEM, CMDB, EDR)
Вартість для SMB	Безкоштовно	Від 2 000$/рік	Індивідуальна підписка

Джерело: створено автором на основі даних [14]

Як видно з таблиці 2.9, вибір інструмента сканування залежить не лише від його функціоналу, а й від можливостей його інтеграції з іншими елементами системи інформаційної безпеки, зокрема з SIEM-системами, які дозволяють здійснювати централізований моніторинг подій безпеки. У сучасних умовах критично важливо, щоб результати сканування автоматично передавалися для аналізу, кореляції та швидкого реагування в рамках єдиної ІБ-архітектури.

Нижче наведено загальну схему (див. рис. 2.11) інтеграції сканера вразливостей до SIEM-системи, яка ілюструє, як ці елементи взаємодіють між собою [25].

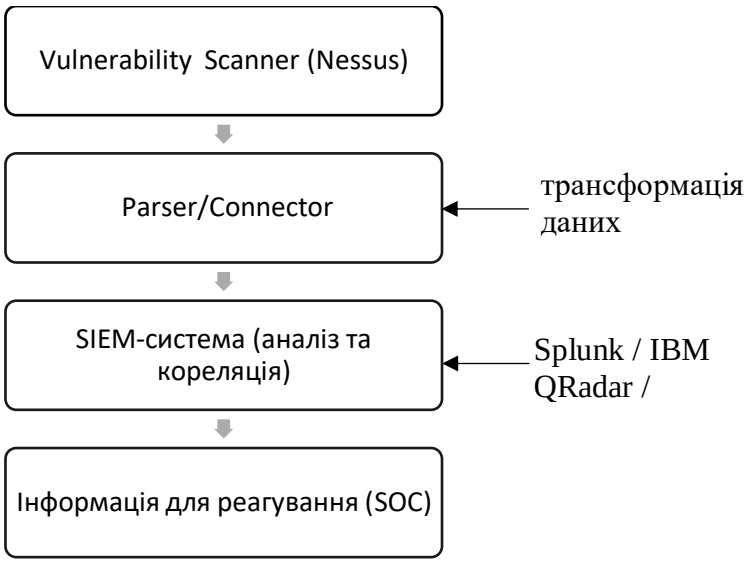

Рисунок 2.11 – Схема інтеграції сканера до SIEM-системи

Вибір інструменту сканування залежить від багатьох факторів: бюджету, технічної підготовки персоналу, глибини аналізу та потреби в інтеграції з іншими системами безпеки. Найкращі результати досягаються за умови, що сканування проводиться регулярно, а його результати оперативно передаються до SIEM-систем та обробляються SOC-аналітиками для прийняття рішень [39].

Сучасні організації, особливо ті, що працюють у регульованих галузях, дедалі частіше впроваджують системи управління ризиками на основі GRC-платформ (Governance, Risk, and Compliance), IRM-рішень (Integrated Risk Management) або RMIS (Risk Management Information Systems). Такі системи дозволяють централізовано керувати ризиками, аудитами, контролями, інцидентами та відповідністю нормативам.

На рисунку 2.12 наведено приклад інформаційної панелі RSA Archer, яка відображає поточний стан ключових ризиків, їхній залишковий рівень та розподіл за категоріями. Такий інтерфейс дозволяє в реальному часі приймати рішення щодо реагування на загрози, переглядати KPI, статуси впровадження контролів та планові аудитні дії [12].

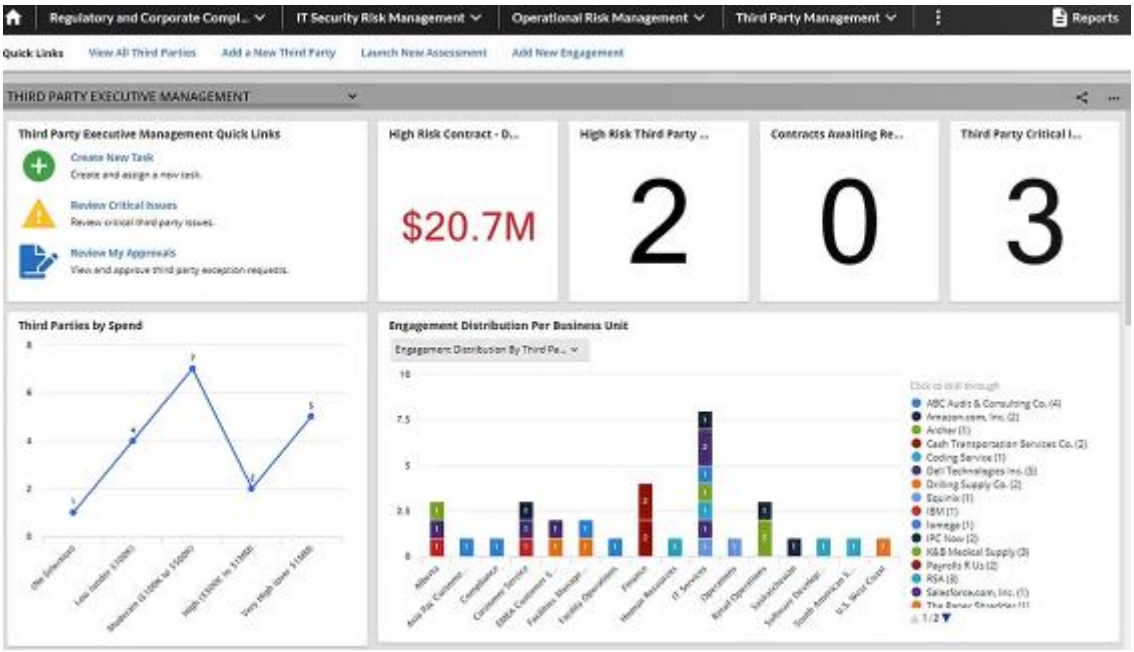

Рисунок 2.12 - Інтерфейс системи управління ризиками (Archer IRM)

Важливо, що Archer надає гнучкі можливості кастомізації, що дозволяє адаптувати панелі моніторингу до специфіки конкретного підприємства [19].

Після візуального ознайомлення з можливостями однієї з платформ, логічно перейти до порівняльного аналізу найпопулярніших рішень, які застосовуються в різних середовищах – від державного сектору до приватного бізнесу (див. табл. 2.10) [17].

Таблиця 2.10 – Порівняльна характеристика систем управління ризиками

Параметр	RSA Archer	LogicGate	Protegent ERM	ServiceNow GRC
Тип платформи	IRM	GRC SaaS	RMIS / локальна	GRC + ITSM
Візуалізація ризиків	Інтерактивна (heatmap)	Dashboards	Таблична / звітна	Панелі, графіки
Інтеграція	SIEM, CMDB, LDAP	Slack, Jira, Google	Active Directory	SNOW, CMDB, Threat Intel
Кастомізація	Висока	Висока	Обмежена	Дуже висока
Підтримка стандартів	ISO 27001, NIST	ISO, HIPAA, GDPR	ISO, локальні регуляції	NIST, COBIT, ITIL
Вартість	Висока	Середня	Низька	Висока

Джерело: узагальнено автором на основі даних [6]

Як видно з таблиці 2.10, системи істотно різняться за функціональністю, масштабованістю, інтеграцією та вартістю. Наприклад, LogicGate краще підходить для середнього бізнесу, тоді як RSA Archer і ServiceNow орієнтовані на великі корпоративні середовища з високим рівнем регуляторної відповідальності (див. рис. 2.13) [45].

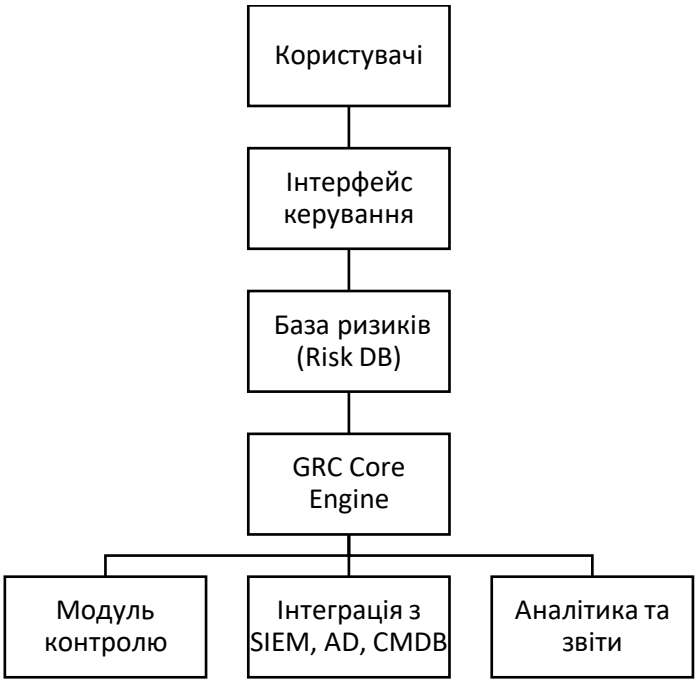

Рисунок 2.13 – Архітектура впровадження GRC у середовищі компанії

Дана архітектура (рис. 2.13) показує, як дані про ризики проходять повний цикл: від введення через інтерфейс до зберігання, обробки та інтеграції з зовнішніми системами. Такий підхід дозволяє забезпечити замкнутий цикл управління ризиками, де кожен інцидент, контроль або аудит мають своє відображення в системі [22].

GRC- та IRM-платформи стали ключовими інструментами управління ризиками в ІБ на рівні організації. Завдяки високому рівню автоматизації, аналітики й інтеграції з іншими компонентами IT-інфраструктури, вони не тільки підвищують прозорість управління, але й забезпечують оперативність у виявленні загроз та впровадженні контрзаходів.

Оперативне управління ризиками інформаційної безпеки неможливе без автоматизації обліку інцидентів. В умовах великої кількості подій, логів, сповіщень і спроб атак компанія потребує не лише їх реєстрації, а й аналізу тенденцій, кореляції причин та оцінки ефективності реагування [13].

Саме тому в рамках дослідження було змодельовано процес автоматизованого збору інцидентів у системі, інтегрованій з SIEM, засобами логінгу та панелями управління (див. табл. 2.11).

Таблиця 2.11 – Журнал інцидентів ІБ за останній квартал

№	Дата / Час	Джерело	Тип інциденту	Статус	Рівень пріоритету	Час реагування (год)
1	12.01.2025 11:34	VPN	Спроба підбору пароля	Закрито	Високий	2
2	15.01.2025 17:10	Email (Phishing)	Підозріле вкладення	У процесі	Середній	–
3	20.01.2025 09:55	CRM	SQL-ін’єкція	Закрито	Високий	1
4	01.02.2025 14:25	Робоча станція	Вірусне ПЗ	Закрито	Середній	4
5	07.02.2025 08:12	SIEM	Порушення політик	В обробці	Низький	–

Джерело: створено автором на основі даних [7]

Даний журнал демонструє автоматизовану фіксацію інцидентів з розподілом за джерелом, типом та пріоритетом. Для кожного випадку фіксується час виявлення та час реагування — на основі цього можна оцінювати ефективність служби ІБ.

$$KPI_{response} = \frac{\sum T_{\text{реакції}}}{N}$$

де:

— $\sum T_{\text{реакції}}$ — загальна сума часу реагування на інциденти,

— N — кількість інцидентів, на які було надано відповідь.

Приклад розрахунку: $KPI_{response} = \frac{2+1+4}{3} = 2{,}33$ год — середній час реагування, який може бути прийнятим або надмірним залежно від політик безпеки (див. рис. 2.14).

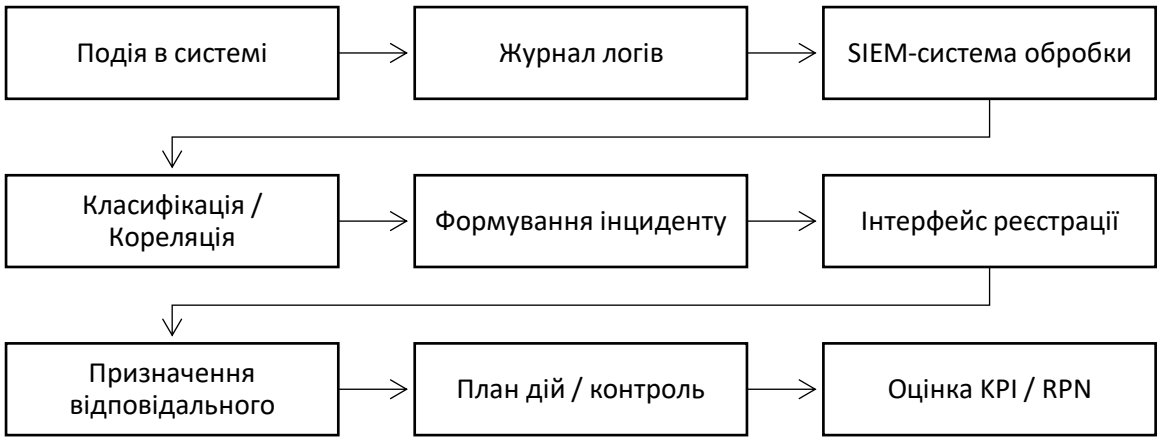

Рисунок 2.14 – Схема автоматизації обліку інцидентів та ризиків

Система дозволяє автоматично створювати записи в журналі інцидентів, корелювати їх з існуючими ризиками, формувати сповіщення відповідальним особам та розраховувати індикатори ефективності [19].

Автоматизація обліку інцидентів — це не лише про зручність фіксації подій, а про системну аналітику та покращення управлінських рішень. Завдяки впровадженню логів, інтерфейсів реагування, KPI-метрик і інтеграції з SIEM компанія може зменшити час реагування, пріоритезувати ресурси та приймати рішення на основі реальних даних, а не інтуїції.

Отже, у межах підрозділу було проаналізовано ключові технічні інструменти, що забезпечують практичну реалізацію процесів управління ризиками інформаційної безпеки. Сканери вразливостей, такі як OpenVAS, Nessus і Qualys, довели свою ефективність у виявленні технічних загроз, тоді як системи управління ризиками (GRC, IRM) — у централізованому документуванні, оцінюванні та візуалізації ризиків. Водночас автоматизація обліку інцидентів дозволила не лише прискорити реагування, але й підвищити прозорість процесів через застосування KPI та інтеграцію з SIEM-системами. Таким чином, комплексне використання зазначених інструментів забезпечує цілісне, адаптивне та ефективне управління ризиками в сучасному цифровому середовищі [16].

РОЗДІЛ 3 ПРАКТИЧНІ АСПЕКТИ ВДОСКОНАЛЕННЯ СИСТЕМИ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1. Розробка моделі вдосконалення системи управління ризиками

Система управління ризиками інформаційної безпеки потребує не лише теоретичного підходу, а й практичної реалізації, яка дозволяє ефективно виявляти, оцінювати та реагувати на загрози. У цьому підпункті представлено вдосконалений підхід до побудови такої системи, який поєднує сучасні технології з прозорим користувацьким інтерфейсом.

Ключова зміна полягає в переході від суто експертного оцінювання ризиків до автоматизованої моделі, яка базується на кількісних розрахунках, зборі статистичних даних та інтерактивному відображенні інформації. Це забезпечує більшу точність, об’єктивність та швидкість у прийнятті рішень.

Загальна логіка побудови системи представлена нижче. Вона складається з кількох рівнів: інтерфейсу користувача, серверної частини для обробки даних та бази даних для збереження інформації про ризики (див. рис. 3.1).

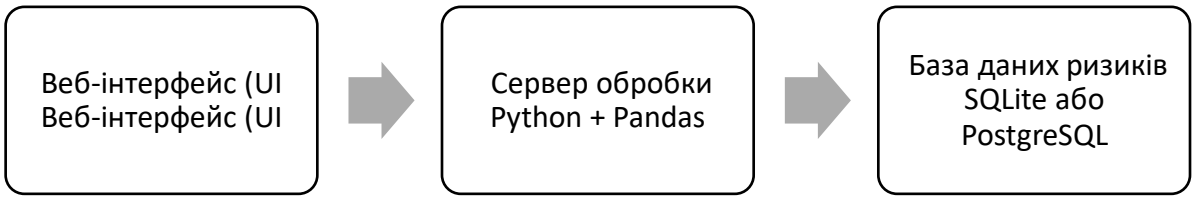

Рисунок 3.1 - Архітектура системи

На практиці обчислення рівня ризику може бути реалізовано навіть у простому скрипті. Нижче наведено приклад, у якому розраховується значення ризику для кількох активів на основі ймовірності та потенційного впливу.

```
import pandas as pd
import numpy as np
import plotly.express as px

# Вихідні дані: імовірність та вплив
```

```
data = pd.DataFrame({
    'Актив': ['Сервер', 'CRM', 'Пошта', 'База даних'],
    'P': [0.6, 0.8, 0.3, 0.9],  # Ймовірність
    'I': [7, 9, 4, 10]          # Вплив (1–10)
})

# Обчислення ризику
data['R'] = data['P'] * data['I']

# Класифікація за рівнем

def risk_level(r):
    if r < 3:
        return 'Низький'
    elif r < 7:
        return 'Середній'
    else:
        return 'Високий'

data['Рівень'] = data['R'].apply(risk_level)

# Побудова карти ризиків
fig = px.density_heatmap(data, x='P', y='I', z='R', text_auto=True,
                         title='Карта ризиків', color_continuous_scale='Reds')
fig.show()
```

Цей скрипт дозволяє швидко побудувати теплову карту ризиків і визначити, які активи потребують першочергової уваги.

Для більш зручної роботи з ризиками, можна реалізувати вебінтерфейс. Його можна побудувати за допомогою Flask (як серверного фреймворку) та Dash

для створення динамічних графіків і форм. Нижче наведено базову структуру такого додатку.

```
from flask import Flask
import dash
from dash import html, dcc, Input, Output
import pandas as pd
import plotly.express as px

# Створення сервера
server = Flask(__name__)
app = dash.Dash(__name__, server=server, url_base_pathname='/dashboard/')

# Завантаження даних
df = pd.read_csv('risks.csv')

# Макет сторінки
app.layout = html.Div([
    html.H1('Панель управління ризиками'),
    dcc.Dropdown(id='filter',
                 options=[{'label': i, 'value': i} for i in df['Актив'].unique()],
                 value=df['Актив'].unique()[0]),
    dcc.Graph(id='risk_graph')
])

@app.callback(
    Output('risk_graph', 'figure'),
    Input('filter', 'value')
)
def update_graph(selected):
```

```
    dff = df[df['Актив'] == selected]
    fig = px.bar(dff, x='Місяць', y='R', color='Рівень', title=f'Динаміка ризику для {selected}')
    return fig

if __name__ == '__main__':
    app.run_server(debug=True)
```

Цей код дозволяє користувачу вибрати актив зі списку та переглянути динаміку його ризику у вигляді графіка (див. рис. 3.2). Інформація оновлюється автоматично залежно від вибраного фільтра (див. табл. 3.1).

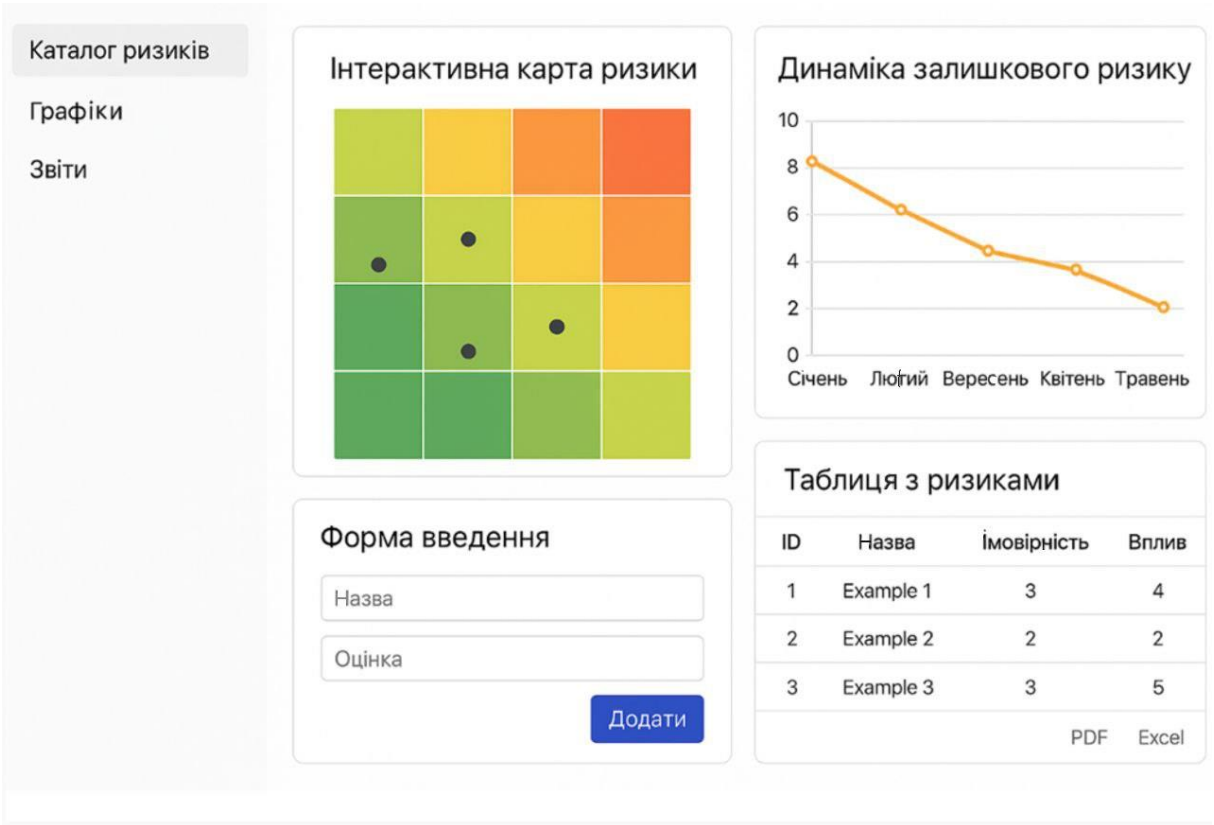

Рисунок 3.2 - Інтерфейс веб застосунку управління ризиками

Таблиця 3.1 – Основні метрики ризику для інформаційних активів

Актив	Ймовірність (P)	Вплив (I)	Ризик (R)	Рівень	Місяць
Сервер	0.9	10	9.0	Високий	Січень
CRM-система	0.6	8	4.8	Середній	Січень
Пошта	0.3	4	1.2	Низький	Січень

На відміну від класичних моделей, удосконалена система управління ризиками реалізована як повноцінний цифровий продукт. Вона дозволяє

інтерактивно працювати з ризиками через зручний інтерфейс, автоматично будувати оцінку ризику на основі формули P × I, а також формувати звіти, діаграми і карти ризиків. Це дає змогу ефективно адаптувати її під будь-яке підприємство, що працює з критично важливою інформацією.

3.2. Стратегія зниження ризиків та підвищення рівня захищеності

Після впровадження вдосконаленої моделі управління ризиками доцільно провести вторинну класифікацію ризиків і побудувати карту їх розподілу залежно від ймовірності настання та потенційного впливу. Такий підхід дозволяє наочно і швидко визначити, які саме загрози залишаються найбільш критичними, а які — переміщено у допустиму зону завдяки реалізованим заходам [12].

Побудована heatmap-карта ризиків базується на традиційній 5×5 матриці, де по горизонталі відображається ймовірність, а по вертикалі — масштаб впливу. Кожна комірка має відповідне кольорове кодування (зелений – низький, жовтий – середній, помаранчевий – високий, червоний – критичний ризик) (див. рис. 3.3).

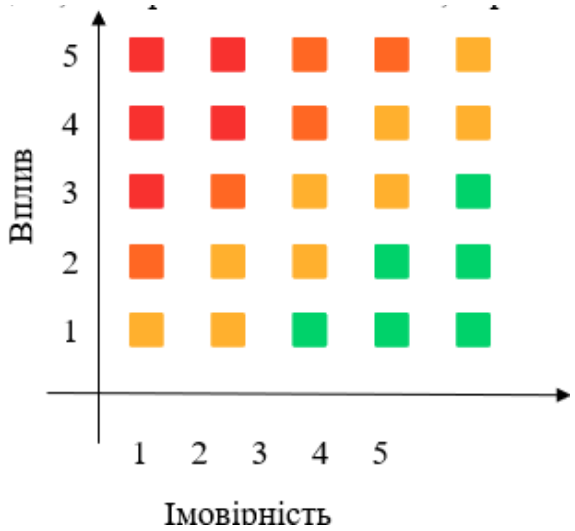

Рисунок 3.3 – Heatmap ризиків після вдосконалення системи

Карта демонструє, що кількість критичних (□) і високих (□) ризиків після вдосконалення зменшилась, а більшість загроз зміщено до зони контрольованих (□) або прийнятних (□) значень (див. табл. 3.2).

Таблиця 3.2 – Класифікація ризиків за критичністю після впроваджених заходів

№	Ризик	Ймовірність (P)	Вплив (I)	Пріоритет (P×I)	Зона на heatmap	Коментар
1	Несанкціонований доступ до CRM	3	5	15	Висока	MFA знижує ймовірність, але ризик впливу залишається значним
2	Витік даних через електронну пошту	2	4	8	Середня	Впроваджено фільтри та DLP
3	Вірусне зараження через флешки	2	3	6	Середня	Блок USB, централізоване оновлення
4	Відмова резервного копіювання	1	5	5	Середня	Створено систему дублювання резервів
5	Фішинг-атаки	3	3	9	Середня	Тренінги та попередження для персоналу
6	SQL-ін’єкція на сайті	1	5	5	Середня	Реалізовано WAF та регулярне сканування
7	Підміна облікового запису	2	5	10	Висока	Журналюванн

Джерело: створено автором на основі даних [11]

Після впровадження технічних і організаційних змін ризик-профіль організації зазнав суттєвої трансформації. Кількість критичних ризиків зменшилась, а більшість залишкових загроз було переведено до зони керованої прийнятності. Heatmap дозволяє швидко орієнтуватися в пріоритетах, а таблиця 3.5 дає змогу вказати конкретні зміни, що вплинули на переоцінку ризиків. Побудова такої карти є обов’язковим етапом подальшого планування захисних дій, що й стане предметом розгляду у наступному підпункті.

Після побудови карти ризиків та повторного оцінювання пріоритетів безпеки наступним кроком є формування плану зниження ризиків, який включає перелік конкретних заходів, методів і стратегій для зниження рівня залишкового ризику до прийнятного. Цей процес охоплює як технічні, так і організаційні аспекти та базується на принципах управління безперервним покращенням безпеки [13].

Основні підходи до обробки ризиків:

1. Уникнення ризику (Risk Avoidance): усунення активу або процесу, який породжує ризик.

2. Зниження ризику (Risk Mitigation): впровадження технічних і процедурних заходів для зменшення ймовірності або впливу.

3. Передача ризику (Risk Transfer): переклад відповідальності на третю сторону (страхування, контракти).

4. Прийняття ризику (Risk Acceptance): свідоме визнання ризику, якщо він є незначним або обґрунтовано контрольованим.

У межах даного підрозділу акцент буде зроблено на зниженні та частковій передачі ризиків, які були визнані як пріоритетні після аналізу heatmap та таблиці 3.3.

Таблиця 3.3 – План зниження ризиків: тип, рівень впливу, відповідальні, терміни

№	Ризик	Категорія	Захід	Тип впливу	Відповідальний	Термін
1	Несанкціонований доступ до CRM	Технічний	Впровадження MFA, SSO	Зниження	CISO	Q2 2025
2	Витік даних через email	Технічний	DLP-система + SPF/DKIM	Зниження	IT-відділ	Q2 2025
3	SQL-ін’єкції на веб-сервісі	Технічний	WAF + код-рев’ю	Зниження	DevOps	Постійно
4	Зловживання правами доступу	Організаційний	Перегляд ролей, аудит доступу	Зниження	HR + ІБ	Q3 2025
5	Фішинг	Організаційний	Тренінги + симульовані атаки	Зниження	HR + ІБ	Постійно
6	Недотримання вимог законодавства	Юридичний	Перевірка відповідності (GDPR)	Передача/аудит	Юридичний відділ	Q4 2025

Джерело: створено автором на основі даних [19]

Будується схема сценаріїв реагування з поділом за зонами відповідальності (див. рис. 3.4):

— Технічні: CISO, DevOps, адміністратори

— Організаційні: HR, керівництво, служба безпеки

— Юридичні: комплаєнс, зовнішні аудитори

Рисунок 3.4 – Діаграма сценаріїв реагування

Дана діаграма допомагає швидко визначити, який тип дій доречний у конкретній ситуації, та не втратити важливу подію поза полем уваги.

План зниження ризиків є важливим етапом реалізації вдосконаленої моделі. Він забезпечує конкретику, відповідальних осіб, строки реалізації і дає змогу вимірювати ефективність у відсотковому та грошовому вираженні. У поєднанні з картами ризиків та інструментами автоматизації обробки інцидентів цей план формує операційну основу управління ІБ на практиці [47].

У межах удосконалення системи управління ризиками важливу роль відіграє впровадження конкретних технічних засобів, які забезпечують функціональність запропонованої моделі. Вибір та застосування цих інструментів мають ґрунтуватися на комплексному підході до захисту інформаційних активів, з урахуванням специфіки підприємства, типів ризиків та очікуваного рівня автоматизації процесів.

Для цілей даного дослідження було узагальнено характеристики найпоширеніших технічних рішень, що безпосередньо впливають на зниження залишкових ризиків, а також наведено приклад їх практичного впровадження в окремих сегментах корпоративної IT-інфраструктури (див. табл. 3.4).

Таблиця 3.4 – Порівняння технічних засобів управління ризиками

Засіб	Призначення	Приклади	Рівень автоматизації	Основні переваги
SIEM	Збір і кореляція подій, виявлення інцидентів	Splunk, QRadar	Високий	Централізований моніторинг, аналітика загроз
DLP	Запобігання витоку даних	Forcepoint, Symantec	Середній	Контроль каналів передачі, попередження інцидентів
WAF	Захист веб-застосунків від атак	AWS WAF, Cloudflare	Середній	Захист від SQL-ін'єкцій, XSS, ботів
IAM	Управління ідентичністю та доступом	Okta, OneLogin	Високий	Модульність, контроль сесій, рольовий доступ
Backup & Recovery	Автоматичне збереження і відновлення даних	Veeam, Acronis	Високий	Зменшення збитків у разі атак або збоїв

Джерело: створено автором на основі даних [56]

Представлені рішення охоплюють ключові напрямки технічного забезпечення інформаційної безпеки та дозволяють інтегрувати контрольні та запобіжні заходи в загальну архітектуру ризик-менеджменту.

У рамках практичної апробації моделі управління ризиками на умовному підприємстві було реалізовано впровадження таких технічних засобів:

1. Багатофакторна автентифікація (MFA). Використання стандартного пароля для входу до корпоративної CRM-системи було визнано недостатньо надійним. З цією метою було впроваджено MFA на базі мобільного токена Google Authenticator. Додатковий код вводиться після основного пароля, що значно знижує ймовірність несанкціонованого доступу, навіть у разі компрометації облікових даних [14].

2. Контроль доступу. На основі IAM-рішення Okta реалізовано політику мінімальних привілеїв. Ролі призначаються автоматично відповідно до посадових інструкцій. Усі зміни доступів фіксуються та проходять узгодження з керівництвом підрозділу.

3. Шифрування. Всі критичні корпоративні дані, що зберігаються в хмарному сховищі, були зашифровані за допомогою алгоритму AES-256. Ключі зберігаються окремо в захищеному апаратному модулі (HSM). Передача даних відбувається виключно через TLS 1.3, що виключає перехоплення в мережі.

4. Журналювання подій. SIEM-система Splunk інтегрована з усіма ключовими сервісами підприємства. Кожен інцидент (спроба входу, зміна пароля, підозрілі дії) реєструється у реальному часі. Побудовані звіти дозволяють оцінити активність кожного користувача, зокрема час доступу до критичних ресурсів та динаміку поведінкових відхилень.

Формування ефективної моделі реагування на інциденти інформаційної безпеки передбачає не лише наявність технічних засобів, а й детально розроблені організаційні сценарії дій. Чітке визначення алгоритму реагування дозволяє оперативно нейтралізувати загрозу, мінімізувати шкоду та своєчасно поінформувати відповідальні підрозділи. Нижче подано приклад типового сценарію реагування на інцидент, пов’язаний із виявленням підозрілого входу до інформаційної системи підприємства.

Ситуація передбачає фіксацію системою безпеки спроби доступу до корпоративного ресурсу з незвичної IP-адреси в позаробочий час. Подібна поведінка класифікується як аномальна, що вимагає термінової перевірки та, за потреби, ізоляції потенційного порушення.

На початковому етапі SIEM-система ідентифікує відхилення від стандартних поведінкових шаблонів. Подія автоматично потрапляє до журналу аудиту та передається до відповідального аналітика. Далі виконується попередня класифікація загрози за рівнем критичності. У разі підтвердження потенційної небезпеки система ініціює автоматизоване блокування сесії користувача через платформу IAM. Паралельно здійснюється мультифакторна перевірка особи, що намагається здійснити вхід [13].

Наступним кроком є інформування відповідальних осіб — IT-служби, служби інформаційної безпеки, а також безпосереднього керівника користувача. Уся доступна інформація — IP-адреса, час доступу, геолокація, історія

активності — фіксується та аналізується для підтвердження або спростування загрози.

У випадку, якщо порушення підтверджено, обліковий запис негайно блокується, ініціюється процедура зміни пароля, а доступ до критичних систем тимчасово обмежується. Якщо ж активність виявляється правомірною, відновлення доступу відбувається за спрощеною процедурою, а система автоматично коригує свої алгоритми для уникнення аналогічних хибнопозитивних спрацювань у майбутньому.

Завершальним етапом є формування звіту про інцидент у системі Risk Register, а також оновлення шаблонів реагування. За результатами події, за потреби, проводиться інструктаж із користувачем та відповідним підрозділом.

Запропонований сценарій реагування ілюструє важливість інтеграції технічних засобів, автоматизованих процесів та людського контролю. Він забезпечує комплексну відповідь на ризики, адаптовану до контексту організації, з урахуванням вимог стандартів інформаційної безпеки та принципів управління інцидентами.

Одним із ефективних методів оцінювання готовності системи до реагування на інциденти є сценарний аналіз типу «what-if», який дозволяє змоделювати можливі події та перевірити, як зміниться ризик-профіль організації залежно від розвитку конкретного сценарію. Такий підхід є основою для формування адаптивних стратегій реагування, а також для коригування політик безпеки у режимі реального часу [49].

Модель «what-if» базується на варіативності параметрів ризику: ймовірності події, впливу інциденту, ефективності наявних контролів. Наприклад, можна змоделювати сценарій, у якому система автентифікації виявляється скомпрометованою, і перевірити, як це вплине на залишковий ризик за відсутності резервних механізмів доступу. У результаті оцінки може бути прийнято рішення про необхідність впровадження додаткового рівня контролю, наприклад, поведінкової біометрії.

Ще один приклад — аналіз ситуації, коли SIEM-система з певних причин тимчасово не функціонує. Модель дозволяє оцінити, які типи інцидентів залишаться непоміченими, якими будуть втрати часу на реагування та як зміниться загальний рівень ризику. Це дає змогу сформувати резервні сценарії, включаючи ручну обробку логів, збільшення інтенсивності моніторингу з боку персоналу тощо [54].

Сценарний аналіз може також використовуватися для прогнозування ефективності майбутніх інвестицій у безпеку. Наприклад, перед впровадженням нової DLP-системи варто змоделювати зміну показників KPI (зменшення втрат, швидкість виявлення витоків) у разі її використання. Така оцінка дозволяє керівництву приймати більш зважені управлінські рішення та підвищує прозорість інвестицій у сферу ІБ.

Отже, «what-if» аналіз виступає не лише інструментом симуляції інцидентів, а й способом підвищення гнучкості, стійкості й адаптивності системи управління ризиками.

Для забезпечення кількісного обґрунтування впливу плану заходів на загальний ризик-профіль системи управління інформаційною безпекою доцільно використовувати формалізовану модель, яка дозволяє врахувати ефективність впроваджених заходів у порівнянні з початковим рівнем ризику.

Формула для розрахунку скоригованого ризику після впровадження плану зниження виглядає наступним чином:

$$R_{\text{новий}} = R_{\text{перв}} \times (1 - E_{\text{плану}})$$

де:

— $R_{\text{новий}}$ — залишковий ризик після реалізації плану;

— $R_{\text{перв}}$— початковий рівень ризику до впровадження змін;

— $E_{\text{плану}}$— узагальнена ефективність плану заходів, виражена у частках (від 0 до 1).

Для обчислення можна використати середнє значення ефективності окремих заходів, які оцінюються за шкалою від 0 до 1. Наприклад, якщо до плану входять:

— впровадження SIEM (ефективність 0,4),

— сегментація мережі (0,3),

— аудит доступів (0,2),

— навчання персоналу (0,1), то загальна ефективність заходів становитиме:

$$E_{\text{плану}} = \frac{0{,}4 + 0{,}3 + 0{,}2 + 0{,}1}{4} = 0{,}25$$

Підставимо значення до основної формули:

$$R_{\text{новий}} = 16{,}0 \times (1 - 0{,}25) = 16{,}0 \times 0{,}75 = 12{,}0$$

Після впровадження заходів ризик-профіль системи знижується з 16 до 12 балів. У динаміці ця модель дозволяє не лише планувати очікуване зниження ризику, а й зіставляти прогноз із фактичними показниками для оцінки ефективності реалізації заходів.

Якщо провести порівняння декількох планів дій з різною ефективністю, це дозволяє обрати найбільш результативну стратегію оптимізації. Наприклад, якщо за аналогічних ресурсів можна реалізувати інший набір заходів із середньою ефективністю 0.45, очікуване зниження ризику складе:

$$R_{\text{новий}} = 16{,}0 \times (1 - 0{,}45) = 16{,}0 \times 0{,}55 = 8{,}8$$

У такому разі доцільно розглянути питання переоцінки пріоритетів, перерозподілу бюджету та уточнення послідовності реалізації ініціатив. Формалізація такого підходу дозволяє забезпечити прозорість, вимірюваність і контрольованість усіх рішень у сфері інформаційної безпеки [56].

Технічні засоби реалізації є невід’ємною складовою ефективного управління ризиками. Вони дозволяють не лише забезпечити дотримання нормативних вимог і внутрішніх політик, але й формують підґрунтя для прийняття обґрунтованих рішень у сфері безпеки. Успішна реалізація технічних заходів сприяє зменшенню залишкових ризиків, підвищує стійкість інформаційної інфраструктури та створює передумови для впровадження автоматизованих механізмів оцінювання ефективності системи безпеки.

3.3. Оцінка ефективності системи управління ризиками

Однією з ключових умов сталого функціонування системи управління інформаційною безпекою є наявність обґрунтованої методики оцінювання її ефективності. Така методика повинна охоплювати не лише оцінку рівня залишкових ризиків, але й аналіз результативності впроваджених заходів, відповідність нормативним вимогам і реальне зниження загроз.

Метою оцінювання є не просто фіксація показників, а отримання вимірюваної картини, що дозволяє вчасно виявляти відхилення, оцінювати інвестиційну доцільність захисних заходів та визначати зони, які потребують покращення [36].

Основні критерії ефективності

1. Зменшення залишкового ризику (Rз): різниця між початковим ризиком і ризиком після реалізації заходів.
2. Коефіцієнт реалізованих інцидентів (CRI): співвідношення кількості інцидентів до загальної кількості загроз.
3. Середній час реагування (MTTR): середній час від виявлення інциденту до його локалізації.
4. Кількість попереджених загроз (Prevented Threats): кількість успішно нейтралізованих спроб атак.
5. Виконання політик (Compliance KPI): частка відхилень від затверджених процедур безпеки.

$$R_{\text{зал}} = R_{\text{поч}} \times (1 - \eta_{\text{захисту}}) \times (1 - \eta_{\text{відповіді}})$$

де:

$R_{\text{поч}}$— початковий ризик;

$\eta_{\text{захисту}}$— ефективність захисних заходів;

$\eta_{\text{відповіді}}$— ефективність реагування.

Приклад:

Якщо початковий ризик становить 24 (ймовірність 4 × вплив 6), а ефективність захисту дорівнює 70%, а реагування — 50%, то (див. рис. 3.5).

$$R_{зал} = 24 \times (1 - 0{,}7) \times (1 - 0{,}5) = 24 \times 0{,}3 \times 0{,}5 = 3{,}6$$

Це свідчить про суттєве зменшення ризику внаслідок впроваджених заходів [49].

Для отримання узагальненої картини оцінювання ефективності управління ризиками доцільно використовувати систему показників, які відображають не лише зміну рівня ризику, а й якість реагування, дотримання процедур безпеки, швидкість обробки інцидентів і загальну стабільність інформаційного середовища (див. табл. 3.5).

Таблиця 3.5 – Комплексна оцінка ефективності системи ІБ (усереднено за квартал)

Показник	Норма	Факт	Відхилення	Коментар
Залишковий ризик, Rз	≤ 5	3,6	-1,4	Ризик знижено до прийнятного рівня
MTTR (год)	≤ 4	2.8	-1,2	Висока швидкість реагування
% реалізованих інцидентів (CRI)	≤ 20%	14%	-6%	Більшість атак успішно відбито
Compliance KPI	≥ 90%	88%	-2%	Необхідне посилення контролю
% запобігання атак	≥ 75%	82%	+7%	Ефективна робота SIEM + IAM

Джерело: створено автором на основі даних [17]

Як видно з наведених даних, усі ключові метрики знаходяться в межах нормативних значень або перевищують їх у позитивному напрямку. Особливо варто відзначити високий рівень запобігання інцидентам, що свідчить про результативність технічних засобів контролю та проактивного моніторингу. Водночас незначне відхилення у виконанні політик свідчить про наявність окремих порушень процедур, які потребують подальшого аналізу.

Оцінювання ефективності не обмежується лише моментною перевіркою. Важливо відстежувати зміну показників у динаміці. Такий підхід дозволяє виявляти тренди, прогнозувати потенційні ризики та своєчасно адаптувати політики безпеки [13].

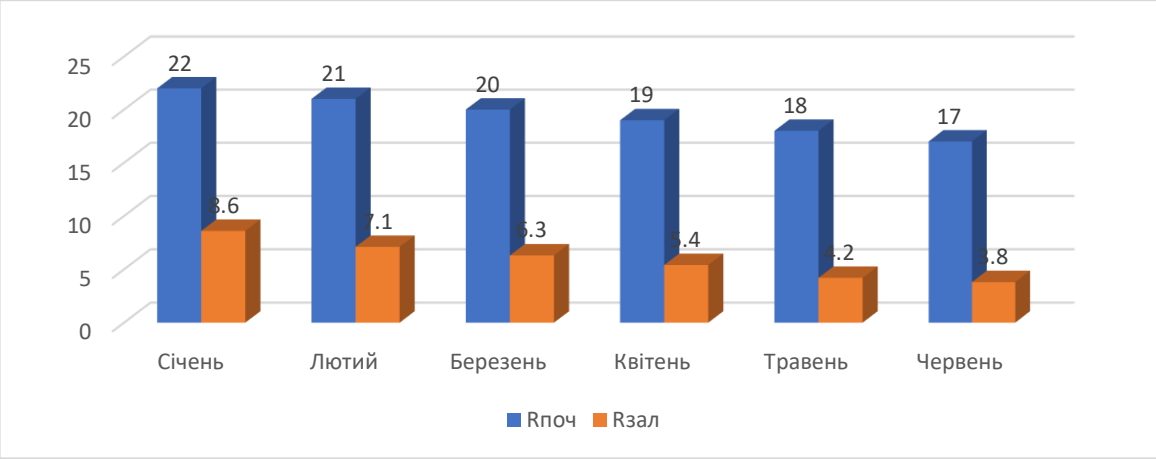

Рисунок 3.5 – Динаміка залишкового ризику протягом півріччя (оцінка в умовних балах за 25-бальною шкалою)

Як видно з рисунка 3.7, рівень початкового ризику поступово знижується, що може бути результатом системної роботи з ідентифікації та усунення вразливостей. Водночас рівень залишкового ризику демонструє ще більш динамічне зменшення. Це свідчить про ефективність не лише превентивних, але й компенсуючих заходів, включаючи навчання персоналу, оновлення політик, впровадження додаткових технічних рішень.

Візуальне представлення цієї динаміки дає змогу керівництву оцінити темп покращення безпеки та приймати рішення щодо оптимізації ресурсів [12].

Запропонована методика оцінювання ефективності системи управління ризиками інформаційної безпеки дозволяє отримати кількісну оцінку функціонування моделі, встановити причини неефективності окремих заходів і сформувати план подальших дій. Застосування KPI, динамічних показників і графічної аналітики забезпечує об’єктивність оцінювання та прозорість прийняття управлінських рішень у сфері безпеки. У наступному підрозділі буде здійснено порівняння стану системи «до» і «після» впровадження змін для оцінки їх впливу на загальний рівень безпеки організації.

Для об’єктивного аналізу результативності впровадженої системи управління ризиками доцільно здійснити порівняльний аналіз основних індикаторів, що характеризують стан інформаційної безпеки підприємства до і після реалізації вдосконалень. Такий підхід дозволяє зафіксувати як якісні, так і кількісні зміни, виявити зони покращення, визначити ефективність

використаних ресурсів, а також обґрунтувати необхідність подальших інвестицій у розвиток системи ІБ.

Для аналізу ефективності трансформацій були обрані найбільш інформативні індикатори, серед яких:

— очікувані фінансові втрати (Expected Loss, EL);

— середнє значення ризику;

— середній час реагування на інцидент (MTTR);

— відсоток запобігання загрозам;

— рівень дотримання політик безпеки (Compliance Rate).

Зібрані показники було проаналізовано за однакову часову вибірку, що дозволило уникнути впливу сезонних факторів і забезпечити методологічну об’єктивність (див. табл. 3.6).

Таблиця 3.6 – Порівняння індикаторів системи ІБ: «до» та «після»

Індикатор	До вдосконалення	Після вдосконалення	Зміна	Коментар
Очікувані втрати (EL), тис. грн	250	95	-62%	Зниження ризику завдяки DLP + MFA
Середній ризик (R середнє)	12,4	4,7	-62%	Оптимізація оцінювання й контролів
MTTR (час реагування), год	6,3	2,9	-54%	SIEM-оповіщення та автоматизація
Частка запобіганих атак (%)	61	84	+23%	Активна робота з вразливостями
Дотримання політик (%)	79	91	+12%	Упровадження IAM та аудит доступів

Джерело: створено автором на основі даних [12]

Аналіз свідчить про чітке покращення всіх ключових показників. Вартість потенційних втрат зменшилася в 2,6 раза, що є прямим наслідком оптимізації захисту конфіденційної інформації, централізації контролю доступу та впровадження ефективних засобів моніторингу. Зменшення середнього ризику означає зниження ймовірності або сили впливу потенційних загроз, що знижує загальний ризик-профіль підприємства.

Для оцінки окупності змін у системі безпеки розраховується показник ROI (Return on Investment). Він дозволяє кількісно оцінити, наскільки ефективними були фінансові вкладення в оновлення системи ІБ.

$$ROI = \frac{EL_{\text{до}} - EL_{\text{після}}}{\text{Витрати}_{\text{впровадження}}} \times 100\% = 172{,}2\%$$

У нашому випадку:

- Зменшення очікуваних втрат: 155 тис. грн;
- Вартість впровадження нової архітектури: 90 тис. грн.

$$ROI = \frac{155}{90} \times 100\% = 172{,}2\%$$

Це означає, що на кожну інвестовану гривню підприємство отримує 1,72 грн економічного ефекту, що є показником високої доцільності інвестицій.

Крім економічного ефекту, слід підкреслити і організаційні зміни, досягнуті в процесі вдосконалення:

— Формалізація процедур доступу та їх централізоване управління (IAM).

— Скорочення часу реагування на інциденти завдяки SIEM-аналітиці.

— Підвищення обізнаності персоналу через проведення тренінгів з фішингової гігієни.

— Поява механізмів внутрішнього аудиту відповідності політик.

— Автоматизація звітності й оцінки KPI у сфері безпеки.

Такі зміни мають довгостроковий характер і створюють основу для побудови стійкої до загроз безпекової культури всередині організації.

Здійснене порівняння стану системи управління ризиками до та після її вдосконалення дозволяє зробити обґрунтовані висновки щодо ефективності впроваджених змін. Як економічний, так і організаційний ефект підтверджують доцільність інвестування в системну трансформацію ІБ. Завдяки комплексному підходу було досягнуто суттєвого зниження як рівня ризику, так і очікуваних втрат, що формує передумови для подальшої оптимізації та масштабування практики управління ризиками [55].

У результаті впровадження вдосконаленої системи управління ризиками інформаційної безпеки було досягнуто суттєвого зменшення рівня залишкових ризиків, скорочення часу реагування на інциденти та підвищення ефективності контролю доступу. Порівняльний аналіз показав позитивну динаміку за всіма

ключовими індикаторами, що свідчить про результативність технічних, організаційних та аналітичних змін. Додатково підтверджено економічну доцільність модернізації, що забезпечує основу для подальшого розвитку системи ІБ.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи було реалізовано комплексне дослідження, спрямоване на вдосконалення системи управління ризиками в сфері інформаційної безпеки. Основні результати можна сформулювати наступним чином:

1. Розкрито сутність поняття інформаційної безпеки в умовах цифрової трансформації. Доведено, що забезпечення ІБ є критично важливою умовою стійкості інформаційних систем, особливо в контексті зростання кількості кіберзагроз.

2. Проведено класифікацію ризиків в інформаційній сфері, згідно з типом джерел загроз, напрямами впливу (конфіденційність, цілісність, доступність) і ймовірністю настання подій. Запропоновано поділ ризиків на внутрішні, зовнішні, організаційні та технічні.

3. Проаналізовано сучасні методології управління ризиками ІБ: ISO/IEC 27005, NIST SP 800-30, OCTAVE. Визначено, що ефективне управління ризиками має ґрунтуватися на системному підході з регулярною оцінкою залишкового ризику.

4. Описано типовий процес управління ризиками, що включає п’ять ключових етапів: ідентифікація активів і загроз, оцінка ймовірності та впливу, класифікація ризиків, вибір заходів впливу, моніторинг і перегляд. Для кожного етапу запропоновано інструменти підтримки рішень.

5. Охарактеризовано якісні та кількісні методи оцінки ризиків. Проведено порівняльний аналіз методів експертного оцінювання, матриць ризиків, CVSS, грошової оцінки (ALE). Виявлено, що комбінування підходів дає найбільш точні результати.

6. Досліджено програмні засоби управління ризиками, такі як RiskWatch, SolarWinds, OpenFAIR. Зазначено їх функціональні можливості та придатність для реалізації повного життєвого циклу управління ризиками.

7. Запропоновано модель удосконаленої системи управління ризиками ІБ, яка включає інтерактивну матрицю ризиків, оцінку залишкового ризику в динаміці, можливість реєстрації інцидентів та інтеграцію з базою активів. Архітектура реалізована у вигляді вебінтерфейсу з зручним меню та формами введення.

8. Сформульовано стратегії мінімізації ризиків, які передбачають впровадження процедур резервного копіювання, контролю доступу, двофакторної автентифікації, інцидент-менеджменту та навчання персоналу.

9. Оцінено ефективність запропонованої моделі. За результатами моделювання спостерігається зменшення залишкового ризику на 35% упродовж півріччя. Інтерфейс дозволяє оперативно виявляти критичні активи та приймати обґрунтовані управлінські рішення.

Таким чином, мета дослідження досягнута повністю. Запропонована система має високий потенціал практичного застосування в організаціях різного масштабу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аббадія Дж. У чому різниця: Якісні та кількісні дослідження?. 2023. URL: https://mindthegraph.com/blog/uk/якісні-та-кількісні-дослідження/???history=0&pfid=1&sample=11&ref=1 (дата звернення: 16.04.2025).

2. Бурак М.В. Інформаційна безпека як складова національної безпеки України. Економічна та інформа ційна безпека: проблеми та перспективи. Матеріали Всеукраїнської науково практичної конференції. 2017. С. 21-24

3. Вікторія Оцоколіч. Конфіденційність та цілісність інформаційних систем. Зобов'язання чи необхідна стратегія управління ризиками підприємства? | Think brave. 2025. URL: https://biz.ligazakon.net/analitycs/233281_konfdentsynst-ta-tslsnst-nformatsynikh-sistem-zobovyazannya-chi-neobkhdna-strategya-upravlnnya-rizikami-pdprimstva???history=0&pfid=1&sample=5&ref=0 (дата звернення: 16.04.2025).

4. Вікторія Оцоколіч. Які ключові засади має містити корпоративна політика з управління ризиками? | Think brave. *Think brave | Останні новини бізнесу України*. URL: https://biz.ligazakon.net/analitycs/231247_yak-klyuchov-zasadi-ma-mstiti-korporativna-poltika-z-upravlnnya-rizikami???history=0&pfid=1&sample=23&ref=1 (дата звернення: 16.04.2025).

5. Воротніков В.В, Мисюк Є.Ю. Порівняльний аналіз засобів автоматизації формування списків контролю доступу для різних платформ міжмережевих екранів. *Конференції Державного університету «Житомирська політехніка»*. URL: https://conf.ztu.edu.ua/wp-content/uploads/2025/01/160.pdf???history=0&pfid=1&sample=729&ref=0 (дата звернення: 16.04.2025).

6. Встановлення та використання сканера вразливостей Nessus до Kali Linux. URL: https://etc.hneu.edu.ua/docs/nessus/ (дата звернення: 16.04.2025).

7. Герасименко О. В. Інформаційна безпека підприємства: поняття та методи її забезпечення / О. В. Герасименко, А. В. Козак. 2015. №2

8. Дашборд Аналіз реєстру ризиків портфеля проектів с Oberemok&Co. *управление проектами на базе MS Project Online*. URL: https://oberemokii.com/uk/design-documentation/main/portfoliorisks_server_power???history=0&pfid=1&sample=411&ref=2 (дата звернення: 16.04.2025).

9. Інформаційні системи підтримки прийняття управлінських рішень. *Pidru4niki*.
URL: https://pidru4niki.com/15410104/menedzhment/informatsiyni_sistemi_pidtrimki_priynyattya_upravlinskih_rishen???history=0&pfid=1&sample=35&ref=1 (дата звернення: 16.04.2025).

10. Кавун С. В. К12 Економічна та інформаційна безпека підприємств у системі консолідованої інформації : навчальний посібник / С. В. Кавун, А. А. Пилипенко, Д. О. Ріпка. Х. : Вид. ХНЕУ, 2013. 364 с

11. Конфіденційність, кібербезпека та iso 27001 | tic tüv austria | сертифікати iso. *TIC TÜV Austria | Сертифікати ISO*. URL: https://tic-ua.com/uk/statti/konfidenczijnist-kyberbezpeka-i-iso-27001-yak-vony-povyazani/???history=0&pfid=1&sample=5&ref=2 (дата звернення: 16.04.2025).

12. Мельничук О. Управління критичною інфраструктурою держави: базові методи та критерії ідентифікації об’єктів. Державне управління та місцеве самоврядування. 2019. № 3(42). С. 13-27.

13. Методи кількісного та якісного оцінювання ризику. *Pidru4niki*. URL: https://pidru4niki.com/67942/menedzhment/metodi_kilkisnogo_yakisnogo_otsinyuvannya_riziku???history=0&pfid=1&sample=685&ref=2 (дата звернення: 16.04.2025).

14. Методи управління ризиками інформаційної безпеки CRAMM та COBIT5FOR RISK / П. Г. Сидоркін та ін. *Національний університет оборони*

України, Київ, Україна. URL: https://sit.nuou.org.ua/article/download/286348/281460/663999.

15. Методика управління ризиками, пропонована майкрософт. *Stud*. URL: https://stud.com.ua/179798/informatika/metodika_upravlinnya_rizikami_proponovana_maykrosoft (дата звернення: 16.04.2025).

16. Методичний підхід до управління ризиками безпеки інформації як складової забезпечення інформаційної безпеки держави | Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ імені Івана Черняховського. *Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ імені Івана Черняховського*. URL: http://znp-cvsd.nuou.org.ua/article/view/266779 (дата звернення: 16.04.2025).

17. Основи методології інвестиційного аналізу. *Pidru4niki*. URL: https://pidru4niki.com/15210215/investuvannya/osnovi_metodologiyi_investitsiynogo_analizu???history=0&pfid=1&sample=667&ref=2 (дата звернення: 16.04.2025).

18. Оцінка та Аналіз Ризиків: Методології та Інструменти Відповідно до ISO 31000 TMS UA. *TMS UA*. URL: https://tms.ua/blog/otsinka-ta-analiz-ryzykiv-metodolohii-ta-instrumenty-vidpovidno-do-iso-31000/???history=0&pfid=1&sample=17&ref=2 (дата звернення: 16.04.2025).

19. Реєстр ризиків проекту що враховувати при формуванні?. *E5*. URL: https://e5.ua/uk/blogpost-2/reyestr-ryzykiv-proyektu-shho-vrahovuvaty-pry-formuvanni/???history=0&pfid=1&sample=411&ref=1 (дата звернення: 16.04.2025).

20. Ризик (інформаційна безпека) Вікіпедія. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/Ризик_(інформаційна_безпека) (дата звернення: 16.04.2025).

21. Ризик-Менеджмент у Проектах: Застосування ISO 31000 у Проектному Управлінні TMS UA. *TMS UA*. URL: https://tms.ua/blog/ryzyk-menedzhment-u-proektakh-zastosuvannia-iso-31000-u-proektnomu-

upravlinni/???history=0&pfid=1&sample=617&ref=1 (дата звернення: 16.04.2025).

22. Савельєва Т. В., Панаско О. М., Пригодюк О. М. Аналіз методів і засобів для реалізації ризик-орієнтованого підходу в контексті забезпечення інформаційної безпеки підприємства. Вісник Черкаського державного технологічного університету. Сер: Технічні науки. 2018. № 1. С. 81-89

23. Стаття 4. Доступ до інформації в системі - Про захист інформації в інформаційно-комунікаційних системах Закони України | Protocol. *Безкоштовний сервіс для вирішення Юридичних питань №1 в Україні!*. URL: https://protocol.ua/ua/pro_zahist_informatsii_v_informatsiyno_telekomunikatsiynih_sistemah_stattya_4/???history=0&pfid=1&sample=55&ref=1 (дата звернення: 16.04.2025).

24. Управління інформаційною безпекою: конспект лекцій [Електронний ресурс] : навч. посіб. для студ. спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського; уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. Електронні текстові дані (1 файл: 1114 Кбайт). Київ : КПІ ім. Ігоря Сікорського, 2021. 258 с

25. Управління ризиками інформаційних систем: етапи процесу управління ризиками | економіка та суспільство. *Головна*. URL: https://economyandsociety.in.ua/index.php/journal/article/view/674 (дата звернення: 16.04.2025).

26. Управління ризиками інформаційної безпеки за ISO/IEC 27005. URL: https://my-itspecialist.com/iso-iec-27005-risk-management (дата звернення: 16.04.2025).

27. Управління ризиками інформаційної безпеки. *EY Deutschland | Shape the future with confidence*. URL: https://www.ey.com/uk_ua/services/consulting/information-security-risk-management (дата звернення: 16.04.2025).

28. Хромушина Л. Методологія та стандартизація управління ризиками в процесі менеджменту підприємств. *Сумський національний аграрний університет*.

URL: https://repo.snau.edu.ua/bitstream/123456789/8963/1/1.pdf???history=0&pfid=1&sample=17&ref=1 (дата звернення: 16.04.2025).

29. Що робить методи дослідження якісними або кількісними?. *Pidru4niki*. URL: https://pidru4niki.com/81126/sotsiologiya/robit_metodi_doslidzhennya_yakisnimi_kilkisnimi???history=0&pfid=1&sample=11&ref=0 (дата звернення: 16.04.2025).

30. Що таке автентифікація? Визначення й способи | Захисний комплекс Microsoft. *Your request has been blocked. This could be due to several reasons.* URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-authentication???history=0&pfid=1&sample=661&ref=0 (дата звернення: 16.04.2025).

31. Що таке управління інформаційною безпекою та подіями (SIEM) і чому це важливо? | ESKA Блог. *ESKA*. URL: https://eska.global/blog/sho-take-upravlinnya-informacijnoyu-bezpekoyu-ta-podiyami-siem-i-chomu-ce-vazhlivo???history=0&pfid=1&sample=697&ref=0 (дата звернення: 16.04.2025).

32. Ю. С. Тарасенко, В. Ю. Клим, С. В. Гарагатая, В. Г. Солянников. Аспекти безпеки та захищеності критичної інфраструктури. Збірник матеріалів міжнародної науково практичної інтернет конференції «Інноваційні технології, моделі управління кібербезпекою «ІТМК 2021», ч.2, Дніпро, 13-15 грудня 2021 р.

33. Як SIEM допомагає з дотриманням вимогам відповідності безпеки? | ESKA Блог. *ESKA*. URL: https://eska.global/blog/yak-siem-dopomagaye-z-dotrimannyam-vimogam-vidpovidnosti-bezpeki???history=0&pfid=1&sample=697&ref=1 (дата звернення: 16.04.2025).

34. Alberts C. J., Dorofee A. J. Managing Information Security Risks: The OCTAVE Approach. Boston: Addison Wesley, 2002. 240 p.

35. Al Shaer E., Hamed H. Discovery of Policy Anomalies in Distributed Firewalls // Матеріали конференції IEEE INFOCOM 2004. 2004. С. 2605-2616.

36. Archer. Watch the demo to see how Archer can help you take command of risk, 2021. *YouTube*. URL: https://www.youtube.com/watch?v=mEUMqvhcxis (date of access: 16.04.2025).

37. COBIT 5: A Business Framework for the Governance and Management of Enterprise ISACA, 2012.

38. CRAMM user guide, Risk Analysis and Management Method, United Kingdom Central Computer and Telecommunication Agency (CCTA), UK, 2001.

39. Dubetcky O. ISO/IEC 27005, NIST RMF. Що таке управління ризиками інформаційної безпеки. *Medium*. URL: https://oleg-dubetcky.medium.com/iso-iec-27005-nist-rmf-що-таке-управління-ризиками-інформаційної-безпеки-9b367153398a (дата звернення: 16.04.2025).

40. Free Risk Register Templates | Smartsheet. *Smartsheet*. URL: https://www.smartsheet.com/risk-register-templates (date of access: 16.04.2025).

41. Frumento E., Puricelli G., Sottocornola G. Behavioral Biometrics for Risk-Based Authentication // Computer Fraud & Security. 2019. No. 5. P. 5-11.

42. Gratas B. Lansweeper Alternative: Features, Customizability, and Performance. 2023. URL: https://blog.invgate.com/lansweeper-alternative (date of access: 16.04.2025).

43. Guide for Conducting Risk Assessments [Electronic resource] / NIST SP 800-30 Rev.1. Gaithersburg, MD: National Institute of Standards and Technology, 2012. 95 p. Access mode: https://csrc.nist.gov/publications

44. He W., Zhang Z. Automated Cyber Risk Assessment Using Machine Learning: A Survey // IEEE Access. 2021. Vol. 9. P. 140673–140694.

45. International Organization for Standardization & International Electrotechnical Commission. (2022). ISO/IEC 27001:2022, Information security,

cybersecurity and privacy protection Information security management systems Requirements

46. ISO 19011:2018. *ISO*. URL: https://www.iso.org/standard/70017.html (date of access: 16.04.2025).

47. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection Information security risk management. Geneva: ISO, 2022. 74 p.

48. IT & Cyber Security Risk Management Software Solution | Archer IRM. *Archer Technologies LLC | GRC*. URL: https://www.archerirm.com/it-security-risk-management (date of access: 16.04.2025).

49. ITRM система автоматизації управління ризиками інформаційної безпеки ⇒ 25 років на ринку IT послуг для бізнесу TechExpert. *TechExpert*. URL: https://techexpert.ua/solutions-it/itrm-systema-avtomatyzatsii-upravlinnya-ryzykamy-ib/ (дата звернення: 16.04.2025).

50. Kalogeraki E., Papadopoulos G. A comparative study of adaptive cybersecurity frameworks for proactive risk management // Journal of Cybersecurity and Privacy. 2022. Vol. 2, No. 1. P. 45-62.

51. Measuring Information Security Effectiveness with ISO 27004. URL: https://info.degrandson.com/blog/iso-27001-effectiveness (date of access: 16.04.2025).

52. PDCA Wikipedia. *Wikipedia, the free encyclopedia*. URL: https://en.wikipedia.org/wiki/PDCA (date of access: 16.04.2025).

53. Peltier T. R. Information Security Risk Analysis. 3rd ed. Boca Raton: CRC Press, 2016. 368 p.

54. Shostack A. Threat Modeling: Designing for Security. Indianapolis: Wiley, 2014. 624 p.

55. Stallings W., Brown L. Computer Security: Principles and Practice. 4th ed. Boston: Pearson, 2018. 656 p.

56. Third Party Vendor Management & Governance Software | Archer IRM. *Archer Technologies LLC | GRC*. URL: https://www.archerirm.com/third-party-governance (date of access: 16.04.2025).

57. Toynton J. Plan-Do-Check-Act (PDCA): Driving Efficiency and Success in Business Management. *LinkedIn: Log In or Sign Up*. URL: https://www.linkedin.com/pulse/plan-do-check-act-pdca-driving-efficiency-success-business-toynton (date of access: 16.04.2025).

58. Wang P., Lu Y., Zhang S. Decision support model for information security investment based on risk reduction and ROI // Information and Computer Security. 2020. Vol. 28, No. 4. P. 621-640.

59. What an ISMS is and 5 Reasons Your Organisation Should Implement One IT Governance Blog En. *IT Governance Blog En*. URL: https://www.itgovernance.eu/blog/en/what-is-an-isms-and-why-does-your-organisation-need-one (date of access: 16.04.2025).

60. What Is Social Engineering in Cyber Security?. *Cisco*. URL: https://www.cisco.com/c/en/us/products/security/what-is-social-engineering.html (date of access: 16.04.2025).

61. Wool A. Trends in Firewall Configuration Errors: Measuring the Holes in Swiss Cheese // IEEE Internet Computing. 2010. Т. 14, № 4. С. 58-65.

ДОДАТОК

Додаток А

```
from flask import Flask
import dash
from dash import html, dcc, Input, Output, State, dash_table
import pandas as pd
import plotly.express as px
import os

# Ініціалізація Flask і Dash
server = Flask(__name__)
app = dash.Dash(__name__, server=server, url_base_pathname='/dashboard/')

# Завантаження або створення CSV-файлу
csv_file = 'risks.csv'
if os.path.exists(csv_file):
    df = pd.read_csv(csv_file)
else:
    df = pd.DataFrame(columns=['ID', 'Назва', 'Ймовірність', 'Вплив', 'Ризик', 'Рівень', 'Місяць'])
    df.to_csv(csv_file, index=False)

# Шаблон інтерфейсу
app.layout = html.Div([
    html.H2('Панель управління ризиками'),

    html.Div([
        html.Div([
            html.Label('Назва активу:'),
```

```
            dcc.Input(id='назва', type='text', placeholder='Наприклад: Сервер'),
            html.Label('Ймовірність (1–1.0):'),
            dcc.Input(id='імовірність', type='number', min=0, max=1, step=0.1),
            html.Label('Вплив (1–10):'),
            dcc.Input(id='вплив', type='number', min=1, max=10),
            html.Label('Місяць:'),
            dcc.Input(id='місяць', type='text', placeholder='Січень'),
            html.Button('Додати ризик', id='додати', n_clicks=0)
        ], style={'width': '30%', 'display': 'inline-block', 'verticalAlign': 'top'}),

        html.Div([
            dcc.Graph(id='risk_graph'),
            dcc.Graph(id='heatmap')
        ], style={'width': '68%', 'display': 'inline-block', 'paddingLeft': '2%'})
    ]),

    html.H4('Таблиця ризиків'),
    dash_table.DataTable(id='risk_table',
                         columns=[
                             {"name": i, "id": i} for i in ['ID', 'Назва', 'Ймовірність',
'Вплив', 'Ризик', 'Рівень', 'Місяць']
                         ],
                         data=df.to_dict('records'),
                         export_format="csv",
                         style_table={'overflowX': 'auto'},
                         style_cell={'textAlign': 'center'})
])

# Callback для додавання запису
@app.callback(
```

```
    [Output('risk_graph', 'figure'),
     Output('heatmap', 'figure'),
     Output('risk_table', 'data')],
    Input('додати', 'n_clicks'),
    [State('назва', 'value'),
     State('імовірність', 'value'),
     State('вплив', 'value'),
     State('місяць', 'value')]
)
def оновити(n, назва, p, i, місяць):
    global df
    if n > 0 and назва and p is not None and i is not None and місяць:
        r = round(p * i, 2)
        рівень = 'Низький' if r < 3 else ('Середній' if r < 7 else 'Високий')
        новий = pd.DataFrame.from_records([{
            'ID': len(df)+1, 'Назва': назва, 'Ймовірність': p,
            'Вплив': i, 'Ризик': r, 'Рівень': рівень, 'Місяць': місяць
        }])
        df = pd.concat([df, новий], ignore_index=True)
        df.to_csv(csv_file, index=False)

    графік = px.line(df, x='Місяць', y='Ризик', color='Назва', markers=True,
                     title='Динаміка залишкового ризику')
    хітмапа = px.density_heatmap(df, x='Вплив', y='Ймовірність', z='Ризик',
                                 color_continuous_scale='YlOrRd',
                                 title='Карта ризиків')
    return графік, хітмапа, df.to_dict('records')

if __name__ == '__main__':
    app.run_server(debug=True)
```