НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

До захисту допущено

Завідувач кафедри
_____**Дмитро ЛАНДЕ**

(підпис)

«20» червня 2025 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Системи, технології та математичні методи кібербезпеки»
спеціальності 125 «Кібербезпека»

на тему: Метод оцінки ризиків в кіберсистемах на основі аналізу інцидентів та їх поширення

Виконав (-ла): здобувач вищої освіти **IV** курсу, групи ФБ-12

Шестопалов Олександр Костянтинович

(прізвище, ім'я, по батькові) (підпис)

Керівник роботи: Полуциганова Вікторія Ігорівна д. філос., асистент, асистент кафедри інформаційної безпеки

(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові) (підпис)

Рецензент Терещенко Іван Миколайович доцент, к.ф-м.н.

(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище, ім'я, по батькові) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Здобувач вищої освіти _____
(підпис)

Київ – 2025 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – перший
(бакалаврський) Спеціальність – 125
«Кібербезпека»
Освітньо-професійна програма «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Дмитро ЛАНДЕ
(підпис)
«20» червня 2025 р.

ЗАВДАННЯ
на дипломну роботу здобувачу вищої освіти

Шестопалову Олександру Костянтиновичу
(прізвище, ім’я, по батькові)

1. Тема роботи. Метод оцінки ризиків в кіберсистемах на основі аналізу інцидентів та їх поширення;

   керівник роботи Полуциганова Вікторія Ігорівна д. філос.,

   асистент, асистент кафедри інформаційної безпеки;

   (прізвище, ім’я, по батькові, науковий ступінь, вчене звання)

   затверджені наказом по університету від «26» травня 2025 р. № 1761-С

2. Термін подання роботи здобувачем вищої освіти «13» червня 2025 р.

3. Вихідні дані до роботи: Попередні дослідження та відомості за темою роботи;

4. Зміст роботи: Теоретичні відомості про існуючі методи оцінки

ризиків, їх порівняння та аналіз. Розробка та створення власного методу оцінки ризиків в кіберсистемах.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо): презентація;

6. Дата видачі завдання: 01.03.2025;

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Отримання завдання для дипломної роботи	01.03.2025	Виконав
2	Огляд літературних джерел	01.03.2025 - 09.03.2025	Виконав
3	Робота над першим розділом	10.03.2025 - 23.03.2025	Виконав
4	Розробка методу оцінки ризиків	24.03.2025 - 29.03.2025	Виконав
5	Робота над другим розділом	30.03.2025 - 13.04.2025	Виконав
6	Проходження переддипломної практики	14.04.2025 - 18.05.2025	Виконав
7	Створення прикладу використання метода	19.05.2025 - 26.05.2025	Виконав
8	Робота над третім розділом	26.05.2025 - 07.06.2025	Виконав
9	Створення презентації для передзахисту диплому	08.06.2025 - 12.06.2025	Виконав
10	Передзахит дипломної роботи	13.06.2025	Виконав
11	Внесення остаточних правок	14.06.2025 - 19.06.2025	Виконав
12	Захист дипломної роботи	20.06.2025	Виконав

Здобувач вищої освіти _____ Олександр Шестопалов
(підпис) (**Власне ім'я, ПРІЗВИЩЕ**)

Керівник роботи _____ Вікторія Полуциганова
(підпис) (**Власне ім'я, ПРІЗВИЩЕ**)

РЕФЕРАТ

Дипломна робота має обсяг 68 сторінок; містить 11 рисунків, 11 таблиць, 13 формул, 20 джерел та 1 додаток.

Метою роботи є розробка методу оцінки ризиків у кіберсистемах на основі аналізу інцидентів та їх поширення. У роботі проведено аналіз існуючих методологій оцінки ризиків, визначено їхні переваги та недоліки, а також розроблено метод оцінки ризиків, який враховує вразливості, загрози, інциденти та їхній вплив на кіберсистеми.

Основу методу становить кількісна оцінка ризиків з урахуванням ймовірності інцидентів, їхнього впливу та поширення в системі, що дозволяє ідентифікувати критичні точки та прогнозувати потенційні збитки. Розроблено алгоритм оцінки, який включає побудову матриці поширення інцидентів та розрахунок ризиків у фінансовому еквіваленті. Ефективність методу підтверджена експериментально на прикладі моделювання кіберзагроз для різних типів активів (цифрова інформація, програмне забезпечення, апаратне забезпечення, сервери, мережева інфраструктура, хмарні сервіси).

Отримані результати мають практичну цінність і можуть бути використані для вдосконалення систем управління кіберрисками в організаціях, а також для розробки стратегій захисту інформаційних систем.

Результати роботи апробовані на XXIII Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених, опубліковані у збірнику матеріалів конференції.

Ключові слова: кібербезпека, оцінка ризиків, кіберсистеми, вразливості, загрози, поширення інцидентів, кількісний аналіз, матриця ризиків, інформаційна безпека.

ABSTRACT

The thesis has a volume of 68 pages; contains 11 figures, 11 tables, 13 formulas, 20 sources and 1 appendix.

The purpose of the work is to develop a method for assessing risks in cyber systems based on the analysis of incidents and their spread. The work analyzes existing risk assessment methodologies, identifies their advantages and disadvantages, and also develops its own risk assessment method, which takes into account vulnerabilities, threats, incidents and their impact on cyber systems.

The basis of the method is a quantitative assessment of risks taking into account the probability of incidents, their impact and spread in the system, which allows identifying critical points and predicting potential losses. An assessment algorithm has been developed, which includes building an incident spread matrix and calculating risks in financial terms. The effectiveness of the method has been experimentally confirmed on the example of modeling cyber threats for different types of assets (digital information, software, hardware, servers, network infrastructure, cloud services).

The results obtained have practical value and can be used to improve cyber risk management systems in organizations, as well as to develop strategies for protecting information systems.

The results of the work were tested at the XXIII All-Ukrainian Scientific and Practical Conference of Students, Postgraduate Students and Young Scientists, and published in the conference proceedings.

Keywords: cybersecurity, risk assessment, cyber systems, vulnerabilities, threats, incident propagation, quantitative analysis, risk matrix, information security.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ 7
ВСТУП 8
1 ОГЛЯД ІСНУЮЧИХ ПІДХОДІВ ДО ОЦІНЮВАННЯ РИЗИКІВ У КІБЕРСИСТЕМАХ 10
1.1 CRAMM 10
1.2 NIST 13
1.3 ISO 27005 16
1.4 FAIR 20
1.5 OCTAVE 23
1.6 COBIT 26
1.7 Група стандартів ISO 31010 29
1.8 Порівняння 31
Висновки до розділу 1 35
2 РОЗРОБКА МЕТОДУ ОЦІНКИ РИЗИКІВ 37
2.1 Загальний вигляд та компоненти формули 37
2.2 Матриця поширення 46
2.3 Рекомендації щодо застосування метода 48
2.4 Етапи застосування методу 49
Висновки до розділу 2 54
3 ПРАКТИЧНЕ ВИКОРИСТАННЯ МЕТОДУ ОЦІНКИ РИЗИКУ 55
3.1 Визначення активів компанії та типів атак 55
3.2 Уточнення оцінки ризику на основі моделей порушника 56
3.3 Приклад розрахунку ризиків 56
Висновки до розділу 3 61
ВИСНОВКИ 63
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ 65
ДОДАТОК А 67

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

СУІБ – Система управління інформаційною безпекою.

DDoS – Distributed Denial of Service (Розподілена атака типу "відмова в обслуговуванні").

SQL Injection – Впорскування SQL-коду (тип атаки на бази даних).

XSS – Cross-Site Scripting (Міжсайтовий скриптинг).

CSRF – Cross-Site Request Forgery (Міжсайтова підробка запитів).

Кіберризик – потенційна загроза, пов'язана з інформаційними технологіями, яка може спричинити збитки.

Інцидент – подія, що порушує політику безпеки або загрожує цілісності, доступності чи конфіденційності інформації.

Фінансовий вплив – очікувані прямі й непрямі втрати у грошовому вираженні внаслідок реалізації ризику.

ВСТУП

По мірі розвитку інформаційних технологій сучасний світ стикається все з більшою кількістю та різноманітністю ризиків та кіберзагроз. Ефективність функціонування кіберсистем напряму залежить від їхньої здатності протистояти загрозам. Це зумовлює необхідність у вдосконаленні підходів до оцінювання ризиків у кіберсистемах, що дозволить більш ефективно протидіяти загрозам, мінімізуючи можливі збитки.

Оцінювання ризиків в кіберсистемах є важливим завданням, адже це дозволяє визначити найбільш критичні точки системи та запобігти можливим негативним наслідкам. Наявність вразливих елементів у кіберсистемах не лише сприяє успішності атак, але й ускладнює можливість захисту даних, що є важливим для всіх галузей. Оцінювання ризиків, яке спрямоване на мінімізацію наслідків експлуатації вразливостей стає нагальною потребою для безпечного функціонування інформаційних систем.

Актуальність роботи полягає в потребі вдосконалення існуючих методів оцінювання ризиків у інформаційних системах з урахуванням динамічних змін у сфері кібербезпеки, а також зростаючого різноманіття та складності загроз. Розробка нових підходів до оцінювання ризиків може істотно покращити рівень безпечності інформаційних систем та мереж, що є важливим для розвитку кібербезпеки як в Україні, так і на глобальному рівні.

Мета дослідження полягає в розробці методу оцінювання ризиків кіберсистем, враховуючи наявні вразливості, що дозволить підвищити захищеність кіберсистем та забезпечити оперативну реакцію на нові загрози і готовність до них.

Завдання дослідження:

1. Проведення аналізу вже існуючих підходів до оцінки ризиків в кіберсистемах.

2. Визначення основних видів ризиків та загроз, що характерні для сучасних кіберсистем.
3. Розробка моделі оцінювання ризиків.
4. Експериментальне підтвердження ефективності одержаної моделі.

Об’єктом дослідження є вразливості і загрози в інформаційних системах.

Предметом дослідження є методи оцінювання ризиків кіберсистем.

Методи дослідження. У роботі використано методи аналізу загроз і ризиків, моделювання вразливостей та ймовірнісні методи оцінки ризику. Метод аналізу використовується для вивчення поточного стану кібербезпеки та визначення потенційних загроз. Моделювання дозволяє створити алгоритмічні сценарії розвитку загроз, а ймовірнісні методи – розрахувати ймовірність реалізації ризиків і потенційні збитки.

Апробація результатів роботи: Результати дослідження були представлені на XXIII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (14 - 17.05.2024 р., м. Київ, Україна)[1], та підхід був розвинений в подальшій роботі.

1 ОГЛЯД ІСНУЮЧИХ ПІДХОДІВ ДО ОЦІНЮВАННЯ РИЗИКІВ У КІБЕРСИСТЕМАХ

Важливий етап у розумінні різних підходів до мінімізації загроз інформаційних систем – це загальні характеристики та порівняльний аналіз існуючих методик і підходів до оцінки ризиків та управління цими ризиками. У даному контексті варто було б розглянути основні методи та інструменти, які використовуються для виявлення, аналізу та управління ризиками, а також порівняти їх ефективність та застосовність в залежності від конкретних ситуацій та запитів. Не менш важливим є завдання оцінки різних методик на предмет того, як вони можуть забезпечити основні складові кібербезпеки: захищеність, конфіденційність, цілісність та доступність даних, а також їх здатність адаптуватися до змін та нових загроз. Тому важливе завдання – порівняти ці підходи за конкретними критеріями, які визначають їх результативність та застосовність в реальних умовах.

1.1 CRAMM

CRAMM[2] (CCTA Risk Analysis and Management Method) – це методологія управління ризиками, яку було створено в 1987 році Центральним комп’ютерним і телекомунікаційним агентством (CCTA), яке тепер перейменовано на Кабінет міністрів уряду Сполученого Королівства.

Методика CRAMM[3] стверджує, що ризик залежить від вартості активів, загроз і вразливостей. Значення цих параметрів оцінюються у серії інтерв’ю з власниками активів, користувачами системи, персоналом технічної підтримки та офіцером служби безпеки відділу. Результатом перевірки CRAMM є набір рекомендованих контрзаходів, які вважаються необхідними для боротьби з ризиками під час захисту інформації.

При правильному використанні CRAMM може надати низку переваг, найважливіша з яких у посібнику користувача CRAMM визначена як

можливість забезпечити метод, за допомогою якого можна виправдати витрати на безпеку та непередбачувані випадки. Ця заява відображає рух уряду Великобританії від стратегії уникнення ризиків до стратегії управління ризиками. Іншими словами, методика CRAMM допомагає стримати ризик і зменшити його до прийнятного рівня, а не намагатися усунути його будь-якою ціною. Ще одна перевага полягає в тому, що CRAMM допомагає визначити варіанти планування на випадок непередбачених ситуацій.

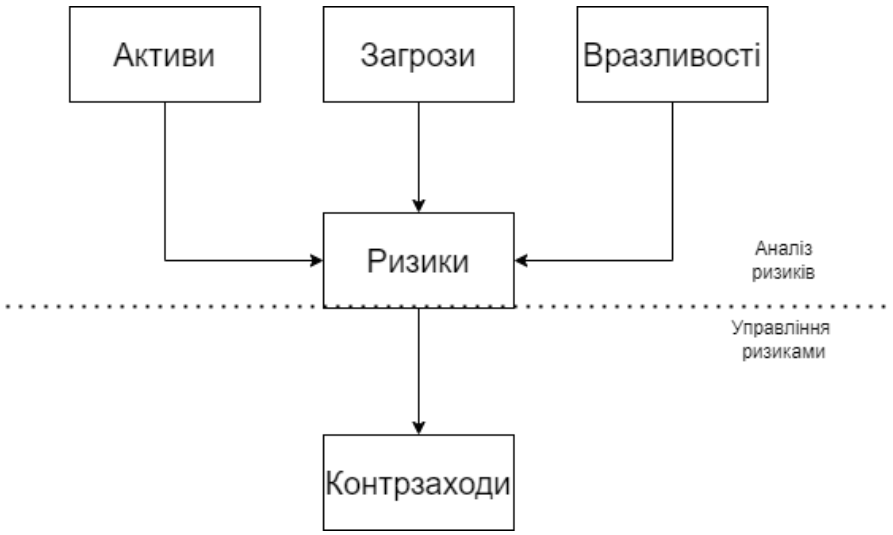

Рисунок 1.1 – Принцип роботи CRAMM

Методика CRAMM складається з трьох етапів, кожен з яких супроводжується об’єктивними анкетами та рекомендаціями. Перші два етапи визначають і аналізують ризики для системи. На третьому етапі пропонуються способи управління цими ризиками.

Три етапи CRAMM такі:

Етап 1

Встановлення цілей безпеки шляхом:

- Визначення меж для дослідження та оцінки ризику
- Виявлення та оцінка фізичних активів, які є частиною системи;
- Визначення «цінності» даних, які зберігаються, шляхом опитування користувачів про потенційні наслідки для бізнесу, які можуть виникнути через недоступність, знищення, розкриття чи модифікацію;

- Визначення та оцінка активів програмного забезпечення, які є частиною системи.

Етап 2

Оцінка ризиків для запропонованої системи та вимог до безпеки шляхом:

- Виявлення та оцінка типу та рівня загроз, які можуть вплинути на систему;
- Оцінка ступеня вразливості системи до виявлених загроз;
- Поєднання оцінок загроз і вразливості з вартістю активів для розрахунку показників ризиків.

Етап 3

Визначення та вибір контрзаходів, які співмірні з мірами ризиків, розрахованими на Етапі 2.

CRAMM містить дуже великий набір контрзаходів, який складається з понад 3000 детальних контрзаходів, організованих у понад сімдесят логічних груп.

CRAMM більше підходить для систем, які вже діють, а не для систем, які знаходяться в розробці. У той час як оцінка активів може здійснюватися напередодні остаточних пропозицій щодо розвитку, повна оцінка загрози/вразливості не може. Наприклад, під час інтерв'ю з оцінкою загроз, на такі запитання, як, яка тенденція кількості збоїв системного чи мережевого програмного забезпечення не можна дати точну відповідь для систем, що розробляються, просто тому, що необхідні дані недоступні.

Переваги:

- Комплексність: Враховує технічні, організаційні та фізичні аспекти ризиків.
- Інструментальна підтримка: Є спеціалізовані програмні засоби для реалізації CRAMM.

- Деталізованість: Включає кількісні та якісні методи оцінки.
- Підходить для державного сектору: Відповідає багатьом стандартам безпеки, включаючи ISO 27001.

Недоліки:

- Складність впровадження: Вимагає багато часу та ресурсів.
- Застарілість: Деякі підходи CRAMM можуть бути неактуальними для сучасних кіберзагроз.
- Фокус на документацію: Багато часу витрачається на заповнення шаблонів і форм.

1.2 NIST

У 2002 році Конгрес США прийняв закон, відомий як Федеральний закон про управління інформаційною безпекою (FISMA). Частина закону доручає Національному інституту стандартів і технологій розробити керівні принципи управління ризиками та інцидентами для всіх федеральних агентств. Результатом стала структура управління ризиками NIST[4], яка охоплює кібербезпеку, конфіденційність і методи реагування на інциденти. Його основна мета — забезпечити стандартизований, але гнучкий і настроюваний підхід до управління ризиками. Перша версія з’явилася в 2014 році, а NIST Incident Response 2 було випущено 8 серпня 2023 року. Також були розроблені менші та більш конкретні посібники з управління ризиками NIST, як-от NIST AI Risk Management Framework, який також був випущений у 2023 році.

Ключові компоненти NIST Risk Management Framework[5]:

Ідентифікація: NIST RMF починається з визначення ризиків для організації, будь то безпека, правові чи стратегічні ризики.

Вимірювання та оцінка: цей компонент описує, як виміряти або оцінити ідентифіковані ризики.

Зменшення ризику: для ризиків, які вимагають прийняття заходів, NIST RMF рекомендує розробити відповідні плани.

Звітування та моніторинг: RMF NIST включає процеси звітування про ризики та моніторинг прогресу.

Управління: цей компонент забезпечує впровадження політик і процедур управління ризиками.

Ці компоненти гарантують, що організації розробляють, належним чином документують і впроваджують політику та процедури інформаційної безпеки. Незважаючи на те, що це розроблено для федеральних агентств, з цих загальних кроків легко зрозуміти, що вони можуть принести користь будь-якій організації, завдяки тому, що NIST RMF дотримується підходу, заснованого на оцінці ризиків, який допомагає керувати інцидентами інформаційної безпеки в будь-якій компанії.

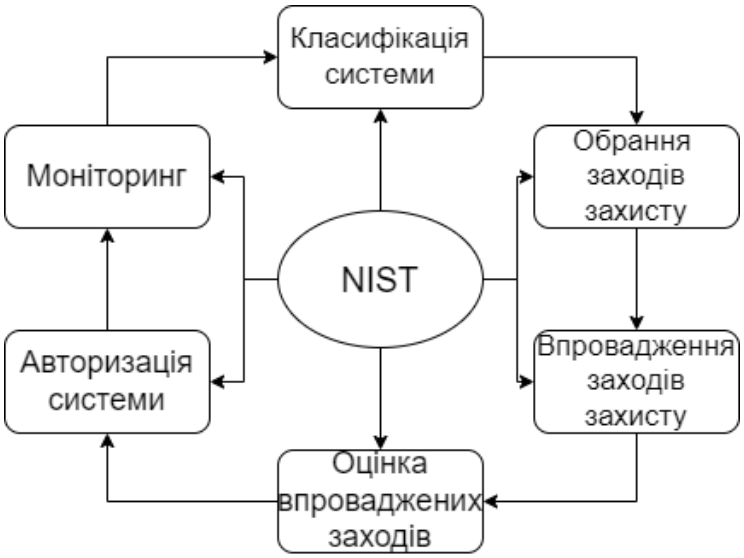

Рисунок 1.2 – Впровадження NIST RMF

Основні кроки впровадження NIST Risk Management Framework:

Крок 1: Класифікація системи

На цьому етапі відбувається класифікація інформаційних активів системи на основі їх чутливості та потенційного впливу на організацію. Це

передбачає аналіз конфіденційності даних, оцінку потенційного впливу на конфіденційність, цілісність і доступність і, зрештою, призначення категорій безпеки.

Крок 2. Обрання засобів/заходів захисту

Наступним кроком буде вибір і адаптація засобів та заходів захисту на основі її категоризації та конкретних потреб. Відповідні елементи описані в NIST SP 800-37, також присутня можливість налаштувати їх відповідно до унікальних характеристик системи та робочого середовища.

Крок 3: Запровадження засобів/заходів захисту

На етапі запровадження застосовуються вибрані засоби і заходи захисту. Це передбачає створення плану безпеки, який детально описує, як кожен елемент керування буде реалізовано та відстежено.

Крок 4: Оцінка впроваджених засобів та заходів

Щоб переконатися в ефективності запроваджених засобів, необхідно провести оцінку безпеки. Вона починається з розробки плану оцінки безпеки (SAP), який визначає цілі, методи та обсяг оцінювання. SAP служить посібником під час проведення оцінки безпеки, щоб оцінити ефективність елементів керування та відповідність вимогам безпеки.

Крок 5: Авторизація системи

Після етапу оцінки приймається рішення, чи слід застосовувати політику. На цьому етапі можна налаштувати будь-які аспекти, які не відповідають конкретним вимогам.

Крок 6: Моніторинг

Розроблюється план постійного моніторингу, який включає регулярні оцінки безпеки, сканування вразливостей і процедури реагування на інциденти. Забезпечується оперативне звітування про інциденти безпеки, уразливості та вживаються коригувальні дії, якщо це необхідно для підтримки безпеки системи.

Переваги:

- Гнучкість: Модель NIST підходить для організацій різного розміру та галузей.
- Докладна документація: Пропонує покроковий підхід до оцінки ризиків (NIST SP 800-30).
- Інтеграція з іншими стандартами: Легко адаптується до ISO 27001 та інших стандартів.
- Фокус на практичності: Орієнтований на впровадження конкретних заходів.

Недоліки:

- Складність реалізації: Документація може бути надто технічною та складною для початківців.
- Американський контекст: Зосереджений на регуляціях США, що може бути проблемою для міжнародних компаній.
- Відсутність глибокої кількісної оцінки: Основний акцент робиться на якісній оцінці.

1.3 ISO 27005

ISO 27005[6] є важливим міжнародним стандартом у сфері управління ризиками інформаційних технологій, опублікований Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC). Він допомагає організаціям раціоналізувати захист конфіденційних даних і передбачити наслідки кібератак і кіберзлочинів. ISO 27005 також базується на вказівках, викладених у стандартах ISO/IEC 27001 та ISO/IEC 27002. Спочатку опублікований у червні 2008 року під абревіатурою ISO/IEC 27005:2008, він був перевиданий у 2011 році та знову у 2018 році.

Міжнародна організація стандартизації рекомендує стандарт ISO 27005[7] компаніям, а також державним установам. На практиці цей стандарт

інформаційної безпеки використовується для забезпечення конфіденційності даних, доступності та цілісності ключових інформаційних активів організації.

Він призначений для підтримки впровадження інформаційної безпеки на основі підходу до управління ризиками. Навчання працівників, як правило, потрібне, щоб допомогти їм розвинути навички виконання процесів управління ризиками інформаційної безпеки. Люди, навчені ISO 27005, теоретично здатні ідентифікувати, аналізувати, оцінювати та управляти ризиками.

Цей стандарт також має на меті допомогти компаніям налаштувати СУІБ (Систему управління інформаційною безпекою). СУІБ передбачає встановлення процесів і політик кібербезпеки, водночас постійно вдосконалюючи управління ризиками та враховуючи людські та технічні фактори під час процесу.

Стандарт ISO 27005 дотримується логіки, яка нагадує методологію постійного вдосконалення PDCA (Plan, Do, Check, Act):

Plan: визначення та оцінка кіберризиків, та пошук необхідних заходів для управління ними;

Do: Запровадження цих заходів;

Check: перевірка результативності впроваджених заходів;

Act: Забезпечення моніторингу і вдосконалення стратегії управління ризиками.

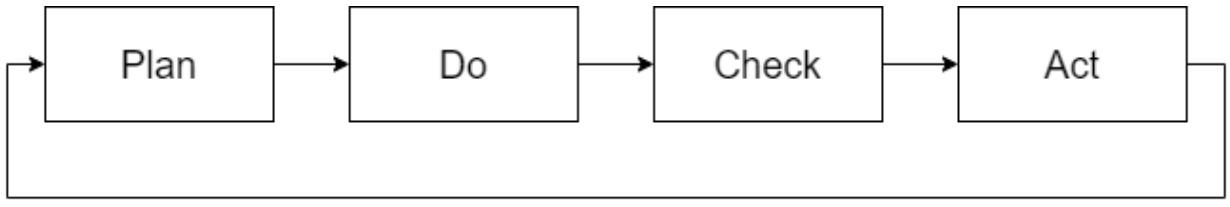

Рисунок 1.3 – Методика PDCA

Як працює ISO 27005?

1. Контекст управління ризиками

На цьому етапі визначаються межі управління ризиками та встановлюються критерії:

- Критерії оцінювання – ідентифікують активи, які можуть бути під загрозою, та порогові значення, за яких ризики потрібно усувати.
- Критерії впливу – визначають мінімальний рівень наслідків, після якого ризик вважається значним.
- Критерії прийнятності ризику – встановлюють, які ризики є допустимими.

2. Оцінка ризиків

Цей етап передбачає визначення елементів, які можуть бути під загрозою: організація, інформаційні системи, сервіси, дані. Потім ідентифікуються загрози та вразливості, що їх стосуються.

ISO 27005 вимагає співставлення цих загроз із безпековими потребами організації. Пріоритети встановлюються за критеріями оцінювання, визначеними на першому етапі.

Однак стандарт не передбачає конкретної шкали оцінювання ризиків. Команда повинна створити власну систему оцінки – якісну або кількісну. На практиці частіше застосовують якісний підхід.

3. Стратегія обробки ризиків

Організація визначає цілі з безпеки на основі оцінки ризиків. Далі розробляються заходи для їх усунення. В ISO 27005 передбачено чотири підходи:

- Уникнення: ризик вважається занадто серйозним, тому діяльність, що його викликає, припиняється.
- Передача: ризик передається третій стороні (наприклад, страхова компанія чи підрядник).

- Пом'якшення: розробляються заходи для зниження впливу чи ймовірності виникнення ризику.
- Збереження: ризик визнається допустимим, і організація вирішує його не усувати.

Усі варіанти залишають певний залишковий ризик, який необхідно оцінити.

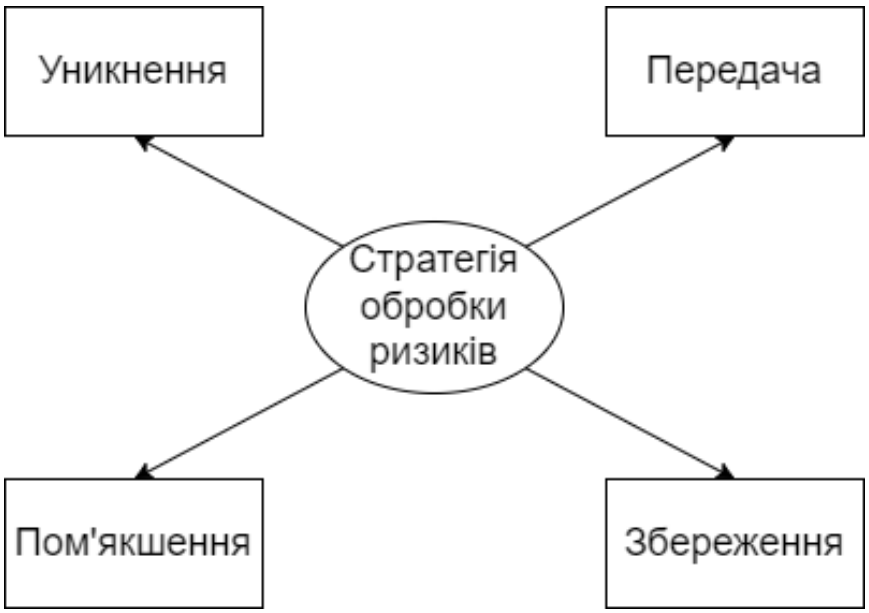

Рисунок 1.4 – Обробка ризиків за ISO 27005

4. Ухвалення стратегії

Стратегія обробки ризиків та залишкові ризики проходять стадію «прийняття», де керівництво організації ухвалює остаточне рішення. На цьому етапі можуть бути обґрунтовані винятки або скорочення витрат.

Хоча теоретично методологія ISO 27005 завершується на цьому, організація має повторювати процес у разі змін у загрозах чи вразливостях.

Переваги:

- Відповідність ISO 27001: Легко інтегрується в систему управління інформаційною безпекою (ISMS).
- Універсальність: Придатний для будь-якої галузі та типу організації.
- Орієнтованість на ризики: Пропонує структуру для ідентифікації, аналізу та обробки ризиків.

Недоліки:

- Відсутність конкретних інструментів: Стандарт лише визначає підхід, але не надає конкретних методик.
- Залежність від інших стандартів: Потребує інтеграції з іншими ISO стандартами для повної ефективності.
- Не деталізує кількісні оцінки: Орієнтований на якісні підходи.

1.4 FAIR

Модель FAIR[8] (Factor Analysis of Information Risk) – це система кількісного аналізу ризиків, яка допомагає організаціям оцінювати кіберризики в грошовому еквіваленті. Модель FAIR оцінює потенційні збитки шляхом аналізу конкретних сценаріїв ризику, що дозволяє підприємствам зрозуміти, де вони найбільш вразливі до кібератак. Визнана як міжнародний стандарт, FAIR допомагає організаціям приймати обґрунтовані рішення щодо управління ризиками та стратегій їх пом’якшення.

Методологія FAIR[9] забезпечує структурований спосіб кількісної оцінки кіберризиків шляхом аналізу впливу та ймовірності потенційних загроз. На відміну від детермінованих моделей, FAIR використовує ймовірнісний підхід, визнаючи випадковість даних для більш точного аналізу ризиків. Він зосереджений на критично важливих активах і ймовірних сценаріях ризику, що дозволяє організаціям оцінювати фінансові наслідки та визначати пріоритети заходів захисту. Ця модель підтримує прийняття обґрунтованих рішень, переводячи складні ризики в чіткі фінансові умови.

Методика FAIR прив’язує частоту та величину потенційних втрат до конкретних активів в організації. Ідентифікація та оцінка цих активів має вирішальне значення для визначення та оцінки ризику. Активом може бути будь-який пристрій, дані або компонент із внутрішньою вартістю, які можуть бути втрачені. FAIR розглядає різні види збитків, зокрема:

- ***Продуктивність:*** зниження через неможливість надати важливі продукти чи послуги.
- ***Реагування:*** ресурси, витрачені на реагування на ризик або загрозу одразу після її виникнення.
- ***Заміна:*** витрати на заміну скомпрометованих активів.
- ***Репутація:*** втрачені можливості або продажі через зниження сприйняття бренду або акціонерів.
- ***Конкурентна перевага:*** втрати від інтелектуальної власності або частки ринку, послаблення конкурентної переваги.
- ***Судові рішення та штрафи:*** судові витрати або штрафи, спричинені загрозою.

Для кількісної оцінки ризику FAIR ділить його на два основні компоненти: частота втрат (LEF) і величина втрат (LM).

Частота втрат(LEF) вимірює, як часто може відбуватися збиткова подія, враховуючи:

- Частота загрози (TEF): Як часто може виникнути загроза.
- Вразливості (Vul): ймовірність загрози, що призведе до втрати.
- Частота контактів (CF): Як часто актив стикається з загрозою.
- Імовірність дії (PoA): ймовірність дії загрози на актив.
- Спроможність загрози (TCap): сила та ресурси, які має загроза, щоб скомпрометувати актив.
- Сила опору (RS): здатність активу протистояти загрозі.

Величина втрат (LM) фіксує вплив загрози, розділений на:

- Основний збиток (PL): прямі збитки для основного акціонера.
- Вторинний збиток (SL): збитки в результаті реакції вторинних зацікавлених сторін.

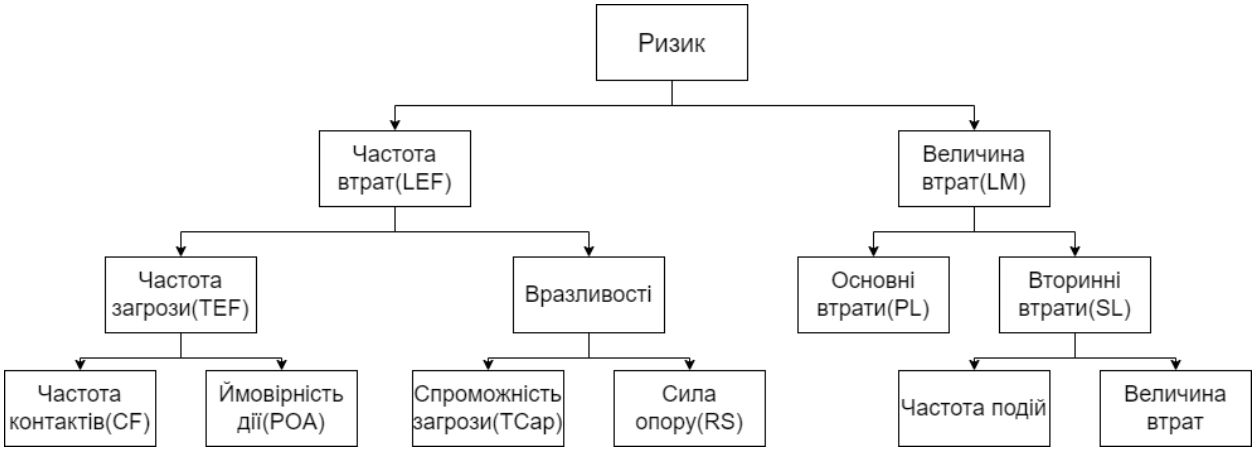

Рисунок 1.5 – Методика FAIR

Зрештою, модель FAIR допомагає організаціям мінімізувати ризик шляхом виявлення сприяючих факторів. Вона пропонує дві основні стратегії: зменшення частоти збитків або пом’якшення фінансового впливу, коли вони трапляються.

Чотири етапи оцінки ризиків за допомогою FAIR

Етап 1. Визначення сценаріїв ризику

Ідентифікуються активи (дані, інфраструктура), загрози (кіберзлочинці, інсайдери) та створюється контекст для аналізу ризиків, зосереджений на найважливіших загрозах.

Етап 2. Оцінка частоти втрат

Розраховується ймовірність втрат, враховуючи:

- Частоту загрози (TEF)
- Спроможність загрози (TCap)
- Сила опору (RS)
- Вразливості (Vul)

Етап 3. Оцінка величини втрати

Визначається фінансовий вплив ризиків:

- Основні збитки: прямі витрати (пошкодження, реагування).
- Вторинні збитки: непрямі втрати (репутація, юридичні санкції).

Етап 4. Формулювання ризику

Синтезується аналіз із використанням даних і моделювання, наприклад Монте-Карло. Це дозволяє оцінити ймовірність і вплив ризиків, формувати пріоритети та обґрунтовано розподіляти ресурси.

Переваги:

- Кількісний підхід: Основа методу – точні метрики, що дозволяють вимірювати ризики в фінансових термінах.
- Ефективність для бізнесу: Допомагає пов'язати ризики з фінансовими показниками, що полегшує комунікацію з керівництвом.
- Модульність: Може бути інтегрована з іншими методологіями.

Недоліки:

- Складність моделювання: Вимагає глибокого розуміння математики та статистики.
- Вузька спрямованість: Більше підходить для фінансових і бізнес-ризиків, ніж для технічних аспектів.
- Потреба у великих обсягах даних: Ефективність залежить від доступності точної інформації.

1.5 OCTAVE

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)[10] є основою для виявлення та управління ризиками інформаційної безпеки. Ця методика визначає комплексний метод оцінки, який дозволяє організації ідентифікувати інформаційні активи, важливі для неї, загрози для цих активів і вразливі місця, які можуть сприяти реалізації загроз.

OCTAVE[11] був розроблений у 2001 році в Університеті Карнегі-Меллона (CMU) для Міністерства оборони США. З того часу структура пройшла кілька етапів еволюції, але основні принципи та цілі залишилися незмінними. Існує дві версії: OCTAVE-S, спрощена методологія для невеликих організацій, які мають плоску ієрархічну структуру, і OCTAVE

Allegro, більш комплексна версія для великих організацій або організацій з багаторівневими структурами.

OCTAVE — це гнучка та самостійна методологія оцінки ризиків. Невелика команда людей з операційних (або бізнес-підрозділів) та IT-відділу працюють разом, щоб задовольнити потреби безпеки організації. Команда спирається на знання багатьох співробітників, щоб визначити поточний стан безпеки, визначити ризики для критичних активів і встановити стратегію безпеки. OCTAVE можна налаштувати для більшості організацій.

На відміну від більшості інших методів оцінки ризиків, підхід OCTAVE ґрунтується на операційних ризиках і методах безпеки, а не на технології. Він розроблений, щоб дозволити організації:

- Керувати оцінкою ризиків інформаційної безпеки самостійно
- Приймати найкращі рішення на основі їх унікальних ризиків
- Зосередитися на захисті ключових інформаційних ресурсів
- Ефективно передавати ключову безпекову інформацію

Основні етапи роботи OCTAVE:

Етап 1: Створення профілів загроз на основі активів. Команда аналізу визначає, що є важливим для організації (активи, пов’язані з інформацією), і що зараз робиться для захисту цих активів. Потім команда вибирає ті активи, які є найбільш важливими для організації (критичні активи), і описує вимоги безпеки для кожного критичного активу. Нарешті, визначаються загрози для кожного критичного активу, створюючи профіль загроз для цього активу.

Етап 2: Визначення вразливостей інфраструктури. Команда аналізу перевіряє шляхи доступу до мережі, визначаючи класи компонентів інформаційних технологій, пов’язані з кожним критичним активом. Потім команда визначає, наскільки кожен клас компонентів стійкий до мережевих атак.

Етап 3: розробка стратегії та планів безпеки. Під час цієї частини оцінки аналітична група визначає ризики для критично важливих активів

організації та вирішує, що з ними робити. На основі аналізу зібраної інформації команда створює стратегію захисту для організації та плани зменшення ризиків для критичних активів.

Рисунок 1.6 – Основні етапи OCTAVE

Методології OCTAVE:

OCTAVE Method

Перший варіант, орієнтований на великі організації (300+ співробітників). Передбачає проведення серії воркшопів за участю міждисциплінарної команди. Підходить для організацій із власною інфраструктурою та здатністю виконувати оцінку вразливостей. Складається з трьох фаз.

OCTAVE-S

Спрощений підхід для малих організацій (до 100 співробітників). Використовує структуровані інструменти (анкети, шаблони), що полегшує оцінку ризиків менш досвідченим командам. Не потребує детального аналізу інфраструктури та проведення воркшопів, адже команда аналітиків вже володіє ключовою інформацією.

OCTAVE Allegro

Сфокусований на інформаційних активах і тому, як вони використовуються, зберігаються, транспортуються та піддаються ризикам. Складається з восьми кроків, організованих у чотири фази:

- Розробка критеріїв оцінки ризику.
- Профілювання критичних інформаційних активів.
- Ідентифікація загроз у контексті використання активів.
- Аналіз ризиків та розробка заходів для їхньої мінімізації.

Allegro підходить як для командної роботи, так і для індивідуального виконання без значної участі організації.

Переваги:

- Фокус на організацію: Враховує специфіку бізнес-процесів і структури організації.
- Простота: Менш технічно складний порівняно з іншими методами.
- Підходить для малих і середніх компаній: Можна використовувати без наявності великих ресурсів.

Недоліки:

- Обмеженість для технічних ризиків: Гірше підходить для оцінки кіберзагроз порівняно з іншими методами.
- Застарілий підхід: Не враховує нові типи загроз, такі як хмарні технології та IoT.
- Суб'єктивність: Значна частина аналізу базується на судженнях учасників.

1.6 COBIT

COBIT[12] (Control Objectives for Information and Related Technologies) – це набір передових практик і процедур, які допомагають організаціям досягати стратегічних цілей шляхом ефективного використання наявних ресурсів і мінімізації IT-ризиків. COBIT поєднує корпоративне управління та IT-

управління. Цей зв'язок реалізується шляхом об'єднання цілей бізнесу та IT, визначення показників і моделей зрілості для вимірювання досягнення цілей, а також визначення відповідальності власників бізнес-процесів та IT-процесів.

Перша версія COBIT[13] була випущена організацією ISACA в 1996 році. Перше видання складалося з основи, а друге було розширено, щоб включити керівні принципи аудиту, набір інструментів впровадження та цілі контролю. Третє видання додало керівні принципи управління. Третє видання COBIT випущено Інститутом ITG (IT Governance Institute). Поточне видання є п'ятим (COBIT 5), а п'ята версія доступна з квітня 2012 року. COBIT 5 консолідує та інтегрує COBIT 4.1, Val IT 2.0 і Risk IT Framework, а також суттєво спирається на бізнес-моделі інформаційної безпеки.

Остання версія, COBIT 2019, була випущена в 2018 році. Нові висновки експертів з IT та управління були включені в нову версію.

Компоненти COBIT:

- ***Структура***: організовує цілі управління IT і передові практики та пов'язує їх із вимогами бізнесу.
- ***Описи процесів***: еталонна модель процесу та спільна мова для всіх в організації. Процеси відображаються на сферах відповідальності планування, архітектури, експлуатації та моніторингу.
- ***Цілі контролю***: надає повний набір вимог високого рівня, які повинні враховуватися керівництвом для ефективного контролю кожного IT-процесу.
- ***Інструкції з управління***: допомагають розподілити відповідальність, узгодити цілі, виміряти ефективність і проілюструвати взаємозв'язок з іншими процесами.
- ***Моделі ефективності***: оцінка ефективності і усунення можливих прогалин.

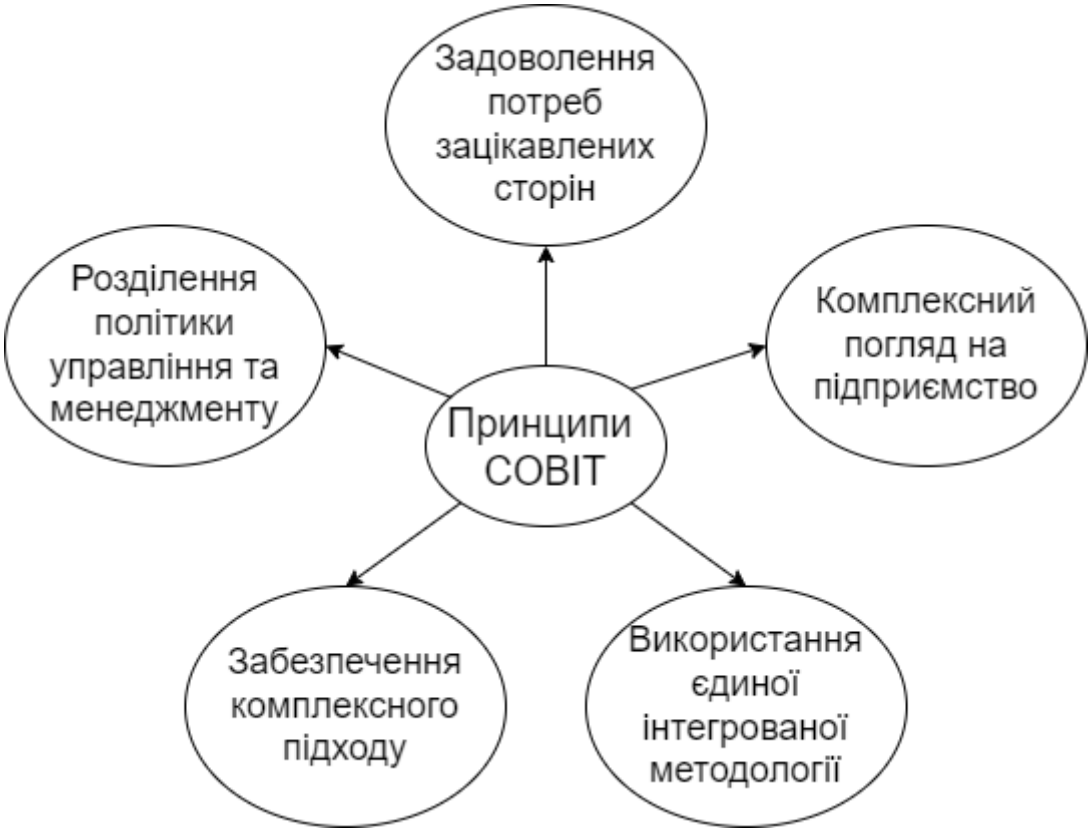

Рисунок 1.7 – Основні принципи COBIT

Переваги:

- Гармонізація з бізнес-процесами: Дозволяє пов'язати IT-цілі з бізнес-цілями, забезпечуючи інтеграцію IT у бізнес-процеси.
- Комплексність: Охоплює всі аспекти управління IT, включаючи аудит, ризики, контроль і оцінку ефективності.
- Гнучкість: Легко інтегрується з іншими фреймворками та стандартами (ISO 27001, ITIL, NIST).

Недоліки:

- Складність впровадження: Вимагає значних ресурсів і часу для інтеграції в організацію.
- Трудомісткість та вартість: Реалізація повного фреймворка може бути надто складною та дороговартісною для малих і середніх компаній.
- Висока залежність від експертів: Потребує кваліфікованих фахівців для правильної реалізації та підтримки.

1.7 Група стандартів ISO 31010

ISO 31000[14] – це набір міжнародних стандартів з управління ризиками. Він був розроблений у листопаді 2009 року Міжнародною організацією стандартизації(ISO). Метою цих стандартів є надання узгодженої методології для оцінки та управління ризиками, вирішення історичних неоднозначностей та відмінностей у способах опису ризиків. Стандарти були розроблені, щоб увійти в інтегровану систему управління.

Мета ISO 31000[15] полягає в тому, щоб бути застосовним і адаптованим для будь-якого державного, приватного чи громадського підприємства, асоціації, групи чи окремої особи. Відповідно, загальна сфера застосування ISO 31000 – як набір стандартів управління ризиками – розроблена не для певної галузевої групи, системи управління чи предметної галузі, а радше для забезпечення всіх операцій, пов’язаних з управлінням ризиками.

Згідно ISO 31000, процес управління ризиками складається з розділів:

- обмін інформацією та консультування;
- сфера застосування, контекст та критерії;
- оцінка ризику;
- вплив на ризик;
- моніторинг та перегляд;
- документування та звітність.

ISO 31010 є міжнародним стандартом, що визначає методи оцінювання ризиків у рамках системи управління ризиками. Він доповнює ISO 31000 і надає широкий набір інструментів для аналізу ризиків у різних галузях.

ISO 31010:2009

ISO 31010:2009 "Risk management – Risk assessment techniques" був першим виданням цього стандарту, розробленим спільно Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною

комісією (IEC). Він містить опис різних методів оцінки ризиків, зокрема: метод Дельфі, SWOT-аналіз, аналіз сценаріїв, дерева рішень, FMEA, FTA та багато інших.

Переваги:

- Включає широкий спектр методів оцінки ризиків.
- Може бути застосований у різних сферах діяльності.
- Сприяє підвищенню ефективності прийняття рішень.

Недоліки:

- Деякі методи описані загально, без детальної інструкції щодо їх застосування.
- Відсутність чітких рекомендацій щодо вибору конкретного методу залежно від ситуації.

IEC 31010:2019

У 2019 році стандарт ISO 31010:2009 було оновлено, і він отримав нову назву – IEC 31010:2019. В оновленій версії уточнено й розширено методи оцінювання ризиків, а також додано нові підходи до їх застосування.

Основні відмінності від ISO 31010:2009:

- Оновлено та уточнено опис методів оцінки ризиків.
- Включено більше прикладів використання методів у різних контекстах.
- Додано рекомендації щодо комбінованого застосування різних методів.

ISO 31000:2018

ISO 31000:2018 "Risk management – Guidelines" є основним стандартом, що встановлює принципи та загальні підходи до управління ризиками. Він не містить конкретних методів оцінки ризиків, але ISO 31010 є його доповненням у цьому аспекті.

Переваги:

- Гнучкий та адаптивний підхід до управління ризиками.
- Орієнтований на інтеграцію ризик-менеджменту в процеси організації.
- Забезпечує системний підхід до ухвалення рішень.

Недоліки:

- Відсутність конкретних методів оцінки ризиків (потребує доповнення ISO 31010).
- Вимагає адаптації під конкретні умови кожної організації.

ДСТУ IEC/ISO 31010:2013

Державний стандарт України ДСТУ IEC/ISO 31010:2013 є офіційним перекладом міжнародного стандарту ISO 31010:2009, який затверджений для застосування в Україні. Він містить аналогічні методи оцінки ризиків і використовується в українських організаціях для забезпечення управління ризиками відповідно до міжнародних практик.

1.8 Порівняння

Ознайомившись із особливостями різних методологій оцінки ризиків у кіберсистемах, можна помітити, що кожна з них пропонує унікальний підхід до вирішення завдань кібербезпеки. Від універсальних стандартів, які підходять для будь-яких організацій, до спеціалізованих інструментів, орієнтованих на конкретні потреби, ці методи формують широкий спектр можливостей для управління ризиками. Однак, щоб обрати найбільш ефективний підхід, необхідно врахувати контекст організації, її ресурси та пріоритети – чи то технічна безпека, чи бізнес-цілі.

Наступне порівняння методологій допоможе систематизувати їхні сильні та слабкі сторони, висвітлюючи ключові аспекти, такі як сфера застосування, складність впровадження, гнучкість і актуальність у сучасних

умовах. Це дозволить краще зрозуміти, який метод або комбінація методів буде оптимальним для конкретної організації, забезпечуючи баланс між практичністю, адаптивністю та ефективністю в управлінні кіберризиками.

1) CRAMM

Сфера застосування: Найкраще для великих систем, що вже діють, особливо в державному секторі.

Тип оцінки: Поєднання якісного (інтерв'ю) та кількісного (оцінка активів, загроз, вразливостей).

Складність впровадження: Висока – потребує багато часу, ресурсів і спеціалізованого ПЗ.

Гнучкість: Обмежена – складно адаптувати до систем у розробці чи нових загроз.

Інтеграція: Відповідає ISO 27001, але менш сумісний з іншими.

Актуальність: Застарілий – не враховує сучасні загрози (IoT, хмари).

Практичність: Висока – деталізований набір контрзаходів (понад 3000).

2) NIST RMF

Сфера застосування: Розроблено для федеральних агентств США, але підходить організаціям будь-якого розміру.

Тип оцінки: Переважно якісний, з елементами кількісного.

Складність впровадження: Середня до високої – потребує детальної документації та технічних знань.

Гнучкість: Висока – адаптується до різних галузей і потреб.

Інтеграція: Легко поєднується з ISO 27001, ITIL тощо.

Актуальність: Висока – оновлюється (наприклад, NIST AI RMF 2023).

Практичність: Висока – покроковий підхід із конкретними заходами.

3) ISO 27005

Сфера застосування: Універсальний – для будь-яких організацій і галузей.

Тип оцінки: Переважно якісний, кількісний підхід визначається організацією.

Складність впровадження: Середня – залежить від інтеграції з ISO 27001.

Гнучкість: Висока – легко адаптується до різних контекстів.

Інтеграція: Тісно пов’язаний з ISO 27001/27002.

Актуальність: Середня – оновлений у 2018, але не деталізує нові загрози.

Практичність: Середня – бракує конкретних інструментів, потрібна додаткова адаптація.

4) FAIR

Сфера застосування: Великі організації з фокусом на бізнес-ризики та фінансові оцінки.

Тип оцінки: Кількісний – вимірює ризики у грошовому еквіваленті.

Складність впровадження: Висока – потребує математичних знань і великих обсягів даних.

Гнучкість: Середня – адаптується до бізнес-контексту, але менш гнучкий технічно.

Інтеграція: Може поєднуватися з іншими методами (NIST, ISO).

Актуальність: Висока – ймовірнісний підхід підходить для сучасних загроз.

Практичність: Середня – дає чіткі фінансові оцінки, але складна в реалізації.

5) OCTAVE

Сфера застосування: Гнучкий – для малих (OCTAVE-S) і великих (OCTAVE Allegro) організацій.

Тип оцінки: Якісний – базується на судженнях учасників.

Складність впровадження: Низька до середньої – не потребує великих ресурсів.

Гнучкість: Висока – налаштовується під організацію.

Інтеграція: Обмежена – менш сумісний з іншими стандартами.

Актуальність: Низька – не враховує хмарні технології чи IoT.

Практичність: Висока – проста і орієнтована на організаційні потреби.

6) COBIT

Сфера застосування: Великі організації з розвиненою IT-інфраструктурою.

Тип оцінки: Якісний – фокус на управлінні та контролі.

Складність впровадження: Висока – трудомісткий і дорогий.

Гнучкість: Висока – інтегрується з бізнес-процесами.

Інтеграція: Відмінна – сумісний з ISO 27001, ITIL, NIST.

Актуальність: Висока – COBIT 2019 враховує сучасні тенденції.

Практичність: Середня – комплексний, але потребує експертів.

7) ISO 31000/31010

Сфера застосування: Універсальний – для будь-яких організацій і галузей.

Тип оцінки: Змішаний – широкий спектр методів (SWOT, FMEA тощо).

Складність впровадження: Середня – залежить від обраного методу.

Гнучкість: Дуже висока – адаптується до будь-якого контексту.

Інтеграція: Висока – сумісний з іншими ISO-стандартами.

Актуальність: Середня – оновлений у 2019, але не спеціалізований на кіберзагрозах.

Практичність: Середня – багато методів, але бракує деталізації.

Таблиця 1.1 – Порівняння методологій оцінювання ризиків

Методологія	Переваги	Недоліки	Застосування
CRAMM	Деталізація, відповідність ISO 27001	Застарілість, складність	Державний сектор
NIST RMF	Гнучкість, актуальність	Складна документація	Державні та комерційні організації
ISO 27005	Універсальність, інтеграція	Відсутність інструментів	Організації з ISO 27001
FAIR	Фінансові метрики, модульність	Складність, потреба в даних	Великі корпорації
OCTAVE	Простота, фокус на бізнес	Обмежена технічна деталізація	Малі організації
COBIT	Комплексність, актуальність	Висока складність	Великі корпорації
ISO 31000/31010	Гнучкість, універсальність	Відсутність спеціалізації	Універсальні проекти

Висновки до розділу 1

Порівняння методів оцінки ризиків у кіберсистемах показало, що кожен із них має унікальні характеристики, які визначають їхню застосовність у різних сценаріях. NIST RMF вирізняється високою актуальністю та практичністю, що робить його ідеальним для організацій із сильним фокусом на кібербезпеку, особливо в державному секторі. CRAMM пропонує деталізовані контрзаходи, але його застарілість обмежує використання в умовах сучасних загроз. ISO 27005 та ISO 31000/31010 відзначаються універсальністю і гнучкістю, однак потребують додаткової адаптації для конкретних потреб. FAIR є потужним інструментом для фінансової оцінки ризиків, але вимагає значних ресурсів і даних. OCTAVE підходить для малих організацій завдяки простоті, хоча поступається в технічній деталізації. COBIT забезпечує комплексне IT-управління, але його складність може бути перешкодою для невеликих компаній. Але жоден з цих методів не пропонує

можлиаості врахування взаємозв’язків між інцидентами, тобто ймовірність того, що один інцидент викличе за собою виникнення інших. Таким чином, вибір методу залежить від розміру організації, її пріоритетів (технічний захист чи бізнес-цілі), доступних ресурсів і рівня готовності до впровадження. Оптимальний підхід може включати комбінацію кількох методів для досягнення максимальної ефективності в управлінні кіберризиками.

2 РОЗРОБКА МЕТОДУ ОЦІНКИ РИЗИКІВ

У сучасному цифровому середовищі кіберзагрози стають дедалі складнішими, а їх наслідки можуть призвести до значних фінансових та репутаційних втрат для компаній[16]. Саме тому ефективне управління ризиками є критично важливим завданням для організацій будь-якого масштабу. Для оцінки рівня кіберризику необхідно враховувати не лише ймовірність реалізації загрози, але й потенційний вплив інциденту та вартість активів, які можуть постраждати.

2.1 Загальний вигляд та компоненти формули

Представлена методика оцінки ризиків базується на універсальній формулі:

$$\mathrm{R} = P * I * V$$

де P - імовірність реалізації загрози, I – оцінка впливу інциденту, V – цінність активу[17].

Ця формула є основою для обрахунку ризику, але при цьому вимагає вдосконалення та уточнення, оскільки для точного підрахунку необхідний більш формальний опис імовірності реалізації загрози, оцінки впливу інциденту та цінності активу, який буде базуватися на чітких математичних формулах та статистичних даних.

Кожен з компонентів формули можна обрахувати таким чином:

Імовірність реалізації загрози(P):

Імовірність реалізації загрози визначає, наскільки часто певний тип загрози може бути реалізований на практиці. Без розуміння цієї ймовірності неможливо адекватно оцінити рівень ризику та розробити ефективні заходи захисту.

Оцінка ймовірності базується на статистичних даних про кількість кіберінцидентів, що сталися за певний період, а також на аналізі тенденцій у сфері кібербезпеки. Використання середньорічної кількості інцидентів (ANI)

дозволяє оцінити поширеність конкретних загроз і порівняти їх між собою. Чим частіше відбувається той чи інший тип атак, тим вищою є його ймовірність у майбутньому.

Для отримання достовірних значень використовуються звіти міжнародних організацій з кібербезпеки, таких як Verizon DBIR[18] та ENISA Threat Landscape[19], які містять детальні аналітичні дані про сучасні загрози, їх частоту та методи атакуючих.

Розрахунок ймовірності реалізації загрози дозволяє компаніям прогнозувати можливі інциденти та оптимізувати свої заходи захисту відповідно до реального рівня загрози.

Середньорічна кількість інцидентів (ANI):

Значення від 0 до 1, де 0 – інциденти такого типу відсутні, 1 – найбільша кількість інцидентів(в порівнянні з іншими типами). Ці значення можна визначити на основі даних, представлених у згаданих вище звітах(Рисунок 2.1, 2.2, 2.3)

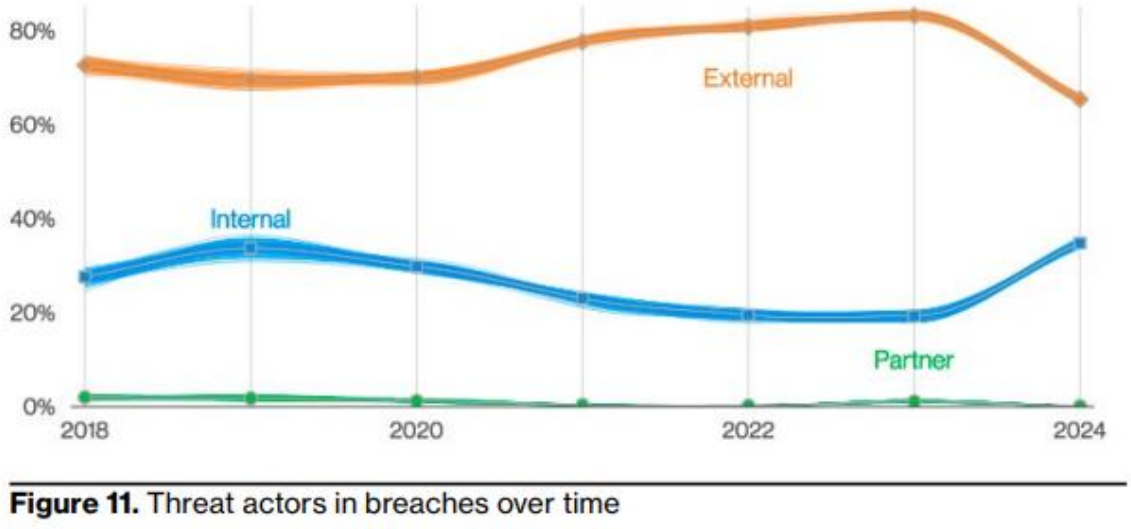

Figure 11. Threat actors in breaches over time

Рисунок 2.1 – Співвідношення внутрішніх і зовнішніх порушників за останні 7 років[18]

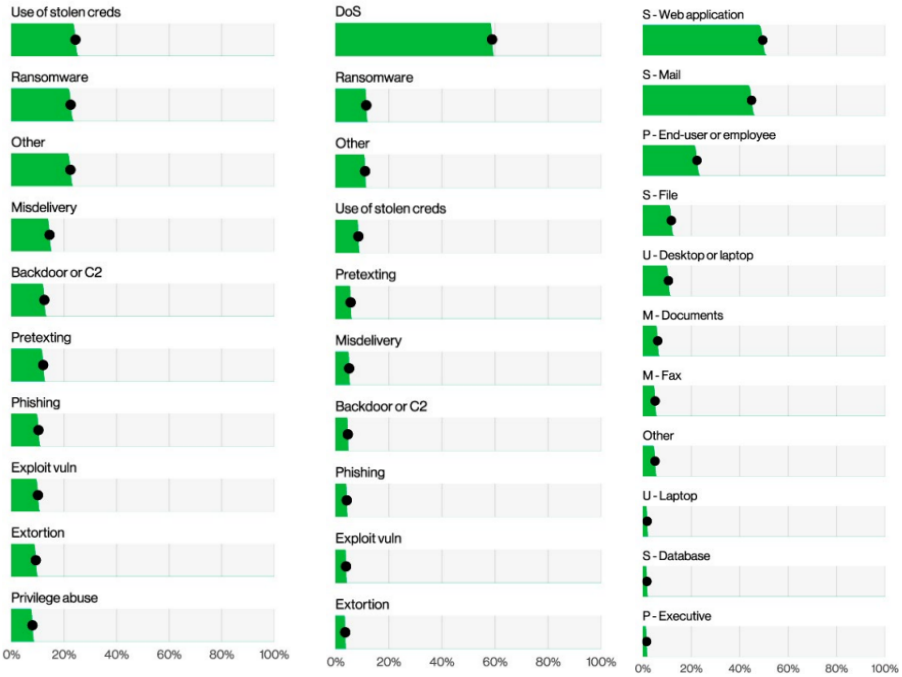

Figure 15. Top Action varieties in breaches (n=9,982)

Figure 16. Top Action varieties in incidents (n=28,625)

Figure 22. Top Asset varieties in incidents (n=6,606)

Рисунок 2.2 – Розподілення атак за їх типами, причинами, та задіяними активами[18]

Figure 2: Breakdown of analysed incidents by threat type (July 2023 till June 2024)

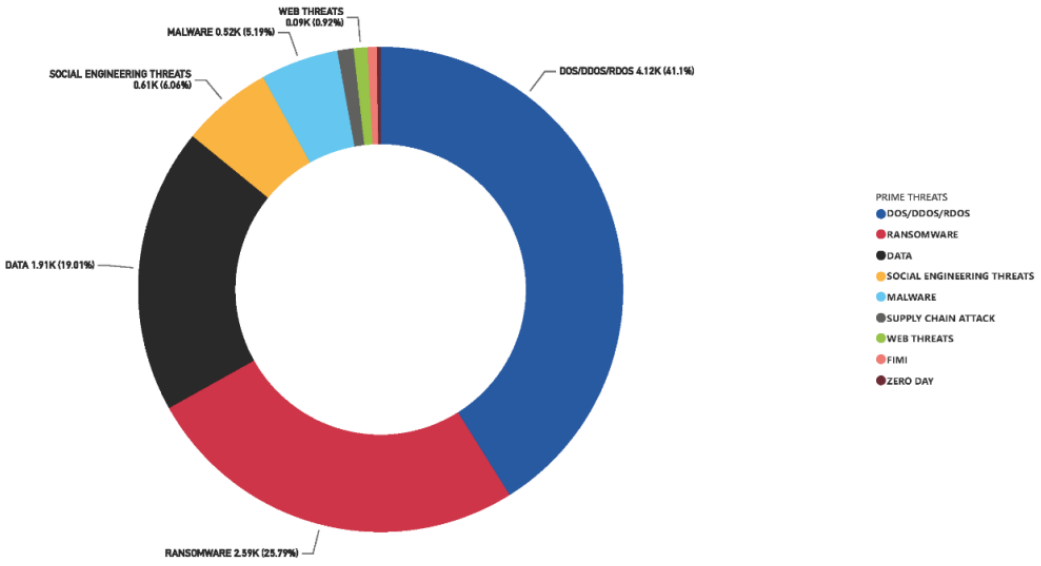

Рисунок 2.3 – Кількість атак та їх процентне співвідношення за 2023-2024 роки[19]

Оцінка впливу(I): оцінює вплив інциденту на діяльність компанії.

Оцінка впливу є ключовим показником, що дозволяє визначити масштаб негативних наслідків кіберінциденту для організації. Вона допомагає зрозуміти, які ресурси та процеси можуть бути порушені, які репутаційні, фінансові та операційні ризики виникають, а також як це вплине на діяльність компанії в цілому[20].

Цей показник є багатовимірним і враховує різні аспекти впливу, включаючи безпеку даних, репутаційні втрати, доступність послуг, ймовірність атак та ефективність існуючого захисту. Комплексний підхід до оцінки впливу дозволяє уникнути ситуацій, коли окремі аспекти ризиків залишаються поза увагою, що може призвести до недооцінки загроз.

Важливість оцінки впливу полягає також у її ролі для прийняття управлінських рішень. На основі цього показника визначаються заходи з нейтралізації або мінімізації наслідків інциденту, виділяються ресурси на відновлення, а також формуються довгострокові стратегії посилення безпеки.

Оцінка впливу складається з кількох індексів, кожен з яких відображає певний аспект впливу кіберінциденту.

Індекс впливу на конфіденційність (PCI):

Індекс PCI враховує три ключові аспекти: чутливість даних, обсяг можливого витоку та репутаційний ризик. Кожен з цих елементів має важливе значення для оцінки впливу інциденту на конфіденційність організації. Чутливість даних визначає, наскільки важливою є інформація, що може бути зловмисно витягнута або знищена. Цей фактор включає різні категорії даних, від публічних до критичних, що дає уявлення про те, наскільки значним буде збиток від їхнього розголошення. Обсяг витоку вказує на масштаб інциденту, від поодиноких записів до повного витоку всієї інформації. Ризик репутаційних втрат оцінює, як сильно інцидент може вплинути на довіру до компанії та її імідж. Цей індекс необхідний для оцінки того, наскільки серйозними можуть бути наслідки витоку або знищення даних і як це

позначиться на юридичних, фінансових та репутаційних аспектах діяльності організації. Без цього індексу компанія не зможе точно оцінити реальні збитки від інциденту, що може призвести до неефективного управління ризиками.

$$PCI = \frac{S_{data}+L_{data}+R_{data}-3}{12} \quad (2.1)$$

S_{data}: Чутливість даних (1 – нечутливі, 2 – публічні, 3 – конфіденційні, 4 – персональні, 5 – критичні)

L_{data}: Можливий об'єм витоку/знищення (1 – одиничні записи, 2 – обмежений витік, 3 – частковий витік, 4 – значний витік, 5 – повний витік)

R_{data}: Ризик репутаційних втрат (1 – дуже низький, 2 – низький, 3 – середній, 4 – високий, 5 – дуже високий)

Індекс впливу на доступність (IAA):

Індекс IAA складається з двох основних компонентів: часу відновлення та впливу на функціональність компанії. Час відновлення визначає, скільки часу знадобиться для відновлення нормальної роботи після інциденту. Цей аспект має важливе значення для оцінки того, як швидко компанія зможе повернутися до своєї діяльності після порушення доступності даних. Вплив на функціональність оцінює, наскільки серйозно інцидент порушить операційні процеси компанії. Якщо збої в системах суттєво впливають на роботу ключових бізнес-процесів, це може призвести до великих фінансових втрат і зниження ефективності роботи. Цей індекс дозволяє оцінити, як швидко можна відновити критичні системи і скільки часу буде потрібно для повернення до нормального рівня функціонування. Без цього індексу неможливо точно визначити, як інцидент позначиться на операційному стані компанії та якими будуть економічні та організаційні наслідки. Індекс важливий для планування заходів відновлення і для оцінки потенційних втрат у разі тривалих перерв.

$$IAA = \frac{A_r+A_i-2}{8} \quad (2.2)$$

A_r: Час відновлення (1 – миттєво, 2 – хвилини, 3 – години, 4 – дні, 5 –тижні)

A_i: Вплив на функціональність компанії (1 – дуже низький, 2 – низький, 3 – середній, 4 – високий, 5 – дуже високий)

Репутаційний вплив (RII):

Індекс RII оцінює три основні аспекти репутаційного впливу: цінність бренду, довіру клієнтів і позиції на ринку. Цінність бренду визначає, наскільки сильно компанія буде страждати від погіршення свого іміджу після інциденту. Втрата довіри клієнтів може призвести до відтоку споживачів, а отже, зниження доходів. Вплив на ринкові позиції вказує, наскільки інцидент може вплинути на конкурентоспроможність компанії на ринку. Якщо репутація бренду серйозно постраждає, це може призвести до значних довгострокових фінансових втрат. Цей індекс необхідний для розуміння довгострокових наслідків інциденту для іміджу організації, оскільки часто репутаційні втрати мають більш серйозні наслідки, ніж безпосередні фінансові збитки. Без цього індексу компанія може не оцінити реальний масштаб репутаційного шкоди, що може призвести до помилок в стратегії управління кризовими ситуаціями.

$$RII = \frac{B_v + C_t + M_p - 3}{27} \quad (2.3)$$

B_v: вплив на цінність бренду (від 1 до 10, 1 – дуже низький, 10 – дуже високий)

C_t: вплив на довіру клієнтів (від 1 до 10, 1 – дуже низький, 10 – дуже високий)

M_p: вплив на позиції на ринку (від 1 до 10, 1 – дуже низький, 10 – дуже високий)

Індекс наміру атаки (AII):

Індекс AII оцінює три основні фактори, які визначають наміри атакуючого: мотивацію, рівень навичок і можливість здійснити атаку. Мотивація атакуючого вказує на рівень зацікавленості хакера в атаці, що визначає, наскільки він готовий докласти зусиль для здійснення інциденту. Рівень навичок атакуючого визначає, наскільки складну атаку може здійснити зловмисник, а можливість здійснити атаку оцінює, чи є у нього доступ до необхідних ресурсів і інструментів для її проведення. Цей індекс важливий для

оцінки потенційних загроз і розуміння того, скільки ресурсів може бути витрачено на боротьбу з певною атакою. Без нього компанія може недооцінити можливість серйозної атаки від висококваліфікованого або мотивованого атакуючого, що знижує ефективність заходів безпеки.

$$AII = \frac{(2*A_m+5*A_s+3*A_o - 10)}{40} \quad (2.4)$$

A_m: Мотивація атакуючого (1 – дуже низька, 2 – низька, 3 – середня, 4 – висока, 5 – дуже висока)

A_s: Рівень навичок атакуючого (1 – дуже низький, 2 – низький, 3 – середній, 4 – високий, 5 – дуже високий)

A_o: Можливість здійснити атаку (1 – дуже низька, 2 – низька, 3 – середня, 4 – висока, 5 – дуже висока)

Індекс експлуатаційної доступності (EAI):

Індекс EAI оцінює, наскільки легко атака може бути здійснена з точки зору доступності інструментів для експлуатації вразливості та складності атаки. Він бере до уваги середній час, необхідний для здійснення атаки, наявність інструментів для її реалізації та складність експлуатації вразливості. Якщо для здійснення атаки є доступні готові інструменти або експлуатація вразливості є відносно простою, ймовірність атаки зростає. Цей індекс необхідний для оцінки, скільки часу та ресурсів можуть бути витрачені на успішну атаку. Без цього індексу організація може не помітити уразливих місць, де хакери можуть використовувати доступні інструменти для здійснення атаки, що може призвести до високих ризиків. Це дозволяє більш точно оцінити реальний рівень захисту компанії та визначити пріоритети для закриття вразливостей.

$$EAI = \frac{1}{T_e} \times R_t \times C_c \quad (2.5)$$

T_e - середній час, необхідний для здійснення атаки (години).

R_t - наявність готових інструментів для експлуатації (1 – відсутні, 2 – важкодоступні, 3 – частково доступні, 4 – в цілому доступні, 5 – доступні відкрито).

C_c — складність експлуатації вразливості (1 – дуже висока, 2 – висока, 3 – середня, 4 – низька, 5 – дуже низька)

Після обрахунку індексу для кожного типу загрози, EAI необхідно нормалізувати наступним чином:

$$EAI_{\text{норм}} = \frac{EAI - EAI_{min}}{EAI_{max} - EAI_{min}} \quad (2.6)$$

Індекс складності захисту (DCI):

Індекс DCI оцінює складність виправлення вразливостей, моніторингу загроз та впровадження заходів пом'якшення. Він важливий для того, щоб зрозуміти, як важко буде компанії захиститися від атак, якщо вони виникнуть. Вразливості з високою складністю усунення потребують значних ресурсів і часу для виправлення, а також можуть вимагати комплексного моніторингу та заходів пом'якшення. Цей індекс важливий для визначення, наскільки компанія здатна впоратися з вразливістю і захиститися від потенційних загроз. Без нього організація може зневіритися у своїх можливостях захисту та витратити надто багато ресурсів на захист від малозначущих загроз, одночасно ігноруючи більш серйозні.

$$DCI = \frac{C_p + C_m + C_i - 3}{12} \quad (2.7)$$

C_p: складність виправлення вразливості (1 – дуже легко, 2 – легко, 3 – середньо, 4 – складно, 5 – дуже складно).

C_m: складність моніторингу загроз, пов'язаних із вразливістю (1 – дуже легко, 2 – легко, 3 – середньо, 4 – складно, 5 – дуже складно).

C_i: складність впровадження заходів пом'якшення (1 – дуже легко, 2 – легко, 3 – середньо, 4 – складно, 5 – дуже складно).

Індекс поточного рівня захисту (CDI):

Індекс CDI оцінює загальний рівень захисту організації від потенційних загроз. Він враховує чотири важливі аспекти: превентивний захист, детекцію атак, пом'якшення наслідків і ефективність реагування. Цей індекс дозволяє визначити, наскільки готова компанія до потенційних атак, і чи є у неї необхідні інструменти для виявлення та мінімізації наслідків кіберінцидентів. Якщо рівень захисту низький, то організація може зіткнутися з великими втратами від атак. Без цього індексу компанія не зможе точно оцінити рівень своїх захисних механізмів і своєчасно вжити необхідних заходів для захисту від кіберзагроз.

$$CDI = \frac{1}{\left(\frac{2\times D_p+3\times D_d+3\times D_m+5\times D_r-13}{117}\right)^2} \quad (2.8)$$

D_p – рівень превентивного захисту (наприклад, фаєрволи, антивірус, політики доступу) (1-10, де 1 – дуже низький, 10 – дуже високий)

D_d – рівень детекції атак (SIEM, IDS/IPS, логування) (1-10, де 1 – дуже низький, 10 – дуже високий)

D_m – рівень пом’якшення наслідків (резервні копії, ізоляція атакованих вузлів) (1-10, де 1 – дуже низький, 10 – дуже високий)

D_r – рівень реагування (ефективність процедур реагування на інциденти) (1-10, де 1 – дуже низький, 10 – дуже високий)

Загальна формула для розрахунку **I**:

$$I = \frac{\left(\frac{PCI\cdot 3+IAA+RII\cdot 2}{6}+2\cdot\frac{AII\cdot 5+EAI_{\text{норм}}\cdot 3+DCI\cdot 2}{10}\right)}{3}\cdot CDI \quad (2.9)$$

Цінність активу(V): Враховує вагомість активу для організації.

Цінність активу визначає, наскільки важливий той чи інший ресурс для організації. Втрата або порушення роботи критично важливого активу може мати значно серйозніші наслідки, ніж інцидент із менш значущим ресурсом. Саме тому правильна оцінка вартості активів дозволяє компанії розставити

пріоритети у захисті та ефективно розподілити ресурси для забезпечення кібербезпеки.

Для кількісного визначення цінності активу використовується індекс максимальної вартості інциденту (AAVI), який обчислюється на основі вартості активу (Vd) та рівня критичності інциденту (Ia). Чим важливіший актив і чим серйозніше його пошкодження або втрата впливає на бізнес, тим вищим буде показник AAVI.

Завдяки цьому підходу можна не лише оцінити потенційні збитки, але й визначити, які активи потребують найбільшого захисту та які заходи слід вжити для мінімізації ризиків.

Індекс максимальної вартості інциденту (AAVI):

$$AAVI = V_d \times I_a/10 \quad (2.11)$$

V_d: вартість активу.

I_a: рівень критичності інциденту (від 1 до 10, 1 – дуже низький, 10 – дуже високий)

Загальна формула для обрахунку ризику:

$$R=P*I*V \quad (2.12)$$

2.2 Матриця поширення

Після обрахунку **R** для кожного типу інциденту необхідно створити **матрицю поширення,** яка буде відображати можливість виникнення різних типів інцидентів унаслідок виникнення певного інцидента. Матриця складається наступним чином: по вертикалі розташовуються типи інцидентів, які можуть статися, а по горизонталі – типи інцидентів, які можуть виникнути внаслідок інцидента, який розташований по вертикалі. В кожну клітинку вписується число від 0 до 1, де 0 – такий інцидент неможливий, 1 – такий інцидент відбудеться з вірогідністю 100%.

Нехай:

$R = (R_1, R_2, \dots, R_n)$ – вектор ризиків кожного типу інцидентів (стовпець розрахованих значень ризику).

$P = [p_{ij}]$ – матриця поширення інцидентів розмірності $n \times n$, де p_{ij} – ймовірність того, що інцидент i і спричинить інцидент j.

$R' = (R'_1, R'_2, \dots, R'_n)$ – новий вектор ризиків, що враховує поширення інцидентів.

Тоді значення ризиків з урахуванням поширення інцидентів можна обрахувати так:

$$R'_j = \sum_{i=1}^{n} R_i \cdot p_{ij} \cdot \mathrm{n}/5, \quad \forall j \in \{1, \dots, n\} \tag{2.13}$$

Побудова матриці поширення інцидентів є важливим етапом у комплексній оцінці ризиків, оскільки вона дозволяє враховувати каскадний ефект атак та інцидентів. У реальних умовах кіберзагрози рідко існують у ізоляції – часто один інцидент може спричинити інші, створюючи ланцюгову реакцію, яка значно посилює загальний рівень ризику для компанії.

Матриця поширення інцидентів дозволяє враховувати взаємозв'язки між ними, відображаючи ймовірність того, що один інцидент може спричинити інший. Завдяки цьому підходу можна оцінити, як окремі інциденти можуть масштабуватися або впливати на різні аспекти діяльності компанії.

Перевагами представленого методу можна вважати:

1. Комплексний підхід. Формула враховує три основні складові ризику, що дозволяє отримати збалансовану та реалістичну оцінку загроз.

2. Гнучкість. Метод може бути адаптований для різних галузей, організаційних структур та видів активів, що робить його універсальним.

3. Обґрунтованість. Всі індекси та коефіцієнти в методиці мають чітке математичне підґрунтя, що забезпечує точність та простоту обчислень.

4. Прогнозування ризиків. Оскільки оцінка базується на статистичних даних та аналізі загроз, компанії можуть не лише реагувати на атаки, а й завчасно виявляти слабкі місця свого захисту.

2.3 Рекомендації щодо застосування метода

Представлений метод оцінки ризиків у кіберсистемах допомагає організаціям виявляти, аналізувати та зменшувати загрози для інформаційних систем. Нижче викладено спрощені рекомендації та покрокові дії для ефективного застосування цього методу.

Оцінка ризиків починається з розуміння того, які активи є ключовими для організації. Це можуть бути дані, програми, обладнання, сервери, мережева інфраструктура чи хмарні сервіси. Важливо оцінити, наскільки вони цінні для бізнесу, враховуючи як фінансові, так і операційні аспекти, наприклад, як їх втрата чи пошкодження вплине на роботу. Залучення різних команд – IT, фінансів, операційного відділу – допоможе отримати повну картину й уникнути пропусків.

Наступний крок – визначення можливих загроз для кожного типу активів, наприклад, кібератак, збоїв чи людських помилок. Потрібно зрозуміти, наскільки ймовірно, що ці загрози реалізуються, спираючись на галузеві звіти, історію інцидентів або консультації з експертами. Наприклад, атаки на дані можуть бути частішими, ніж фізичне пошкодження обладнання. Важливо також врахувати, як одна загроза може спровокувати інші, створюючи ланцюг проблем. Цей аспект враховує матриця поширення, яка є частиною метода.

Розуміння того, хто може становити загрозу, є критично важливим. Зловмисники бувають різними: від внутрішніх працівників із особистими мотивами до професійних хакерів. Для кожного типу зловмисника потрібно оцінити їхні можливості, мотивацію та доступні інструменти. Це допоможе передбачити, які атаки є найімовірнішими та як із ними боротися. Регулярне оновлення цих даних допоможе забезпечити актуальність оцінки.

Оцінка впливу загрози враховує, як інцидент може зашкодити організації. Це не лише прямі фінансові втрати, а й репутаційні, операційні чи юридичні наслідки. Наприклад, витік даних може підірвати довіру клієнтів, а

збій у роботі сервера – зупинити бізнес-процеси. Також треба враховувати легкість реалізації атаки, складність захисту та поточний рівень безпеки організації. Поєднання ймовірності, впливу та цінності активу дає повну картину ризику, допомагаючи визначити, на чому слід зосередити ресурси та зусилля.

Зменшення ризиків потребує комплексного підходу. На основі проведеної оцінки ризиків треба впроваджувати заходи для їх для запобігання (наприклад, захист мережі), виявлення (моніторинг загроз) і реагування (план відновлення). Наприклад, для захисту від атак на дані допоможуть навчання працівників і сучасні системи безпеки, а для зменшення впливу збоїв – резервні копії. Важливо регулярно перевіряти працездатність механізмів захисту через тести чи симуляції, щоб переконатися в їхній ефективності та працездатності.

Оцінка ризиків – це не одноразовий процес. Її потрібно повторювати регулярно, особливо після впровадження змін у системі. Що частіше проводиться така оцінка – то більш підготовленою буде організація до можливих інцидентів.

2.4 Етапи застосування методу

Крок 1: Визначення та оцінка активів

Перший етап – скласти повний перелік активів організації, які можуть бути вразливими до кіберзагроз. Наприклад, це можуть бути цифрові дані (бази клієнтів, фінансова інформація), програмне забезпечення (операційні системи, додатки), апаратне забезпечення (комп’ютери, мобільні пристрої), сервери (веб-, поштові), мережева інфраструктура (маршрутизатори, комутатори) та хмарні сервіси (сховища даних, обчислювальні ресурси). Кожна організація самостійно визначає такі активи та складає перелік.

Для кожного активу треба оцінити його цінність для компанії, враховуючи фінансові витрати від втрати активу чи його пошкодження, а

також операційну значущість. Наприклад, зупинка веб-сервера може призвести до простою онлайн-магазину, а витік клієнтських даних – до репутаційних втрат. Також бажано залучити представників різних відділів – IT, фінансів, операційного управління – щоб врахувати всі аспекти.

Крок 2: Виявлення загроз

На цьому етапі визначаються потенційні загрози для кожного типу активів. Наприклад, цифрові дані можуть бути вразливими до витоку, атак програм-вимагачів чи фішингу, а сервери – до DDoS-атак чи спроб зламу. На даному етапі компанія може спиратися як на загальнодоступні звіти про кіберзагрози, так і на внутрішню історію інцидентів або консультації з галузевими експертами.

Далі необхідно оцінити ймовірність кожної загрози. Знову ж таки, ці дані можуть бути взяті з представленого методу, загальнодоступних джерел, або компанія може самостійно визначити ймовірність, враховуючи певні особливості своїх активів.

Крок 3: Моделювання потенційних зловмисників

Розуміння того, хто може становити загрозу, допомагає краще підготуватися до атак. Треба створити профілі різних типів зловмисників, які можуть атакувати організацію. Наприклад, це можуть бути внутрішні працівники, які діють через особисті мотиви (наприклад, незадоволення), інсайдери, які співпрацюють із конкурентами, професійні хакерські угруповування, окремі хакери, що шукають вигоду чи визнання, або початківці, які використовують прості інструменти. Кожна компанія самостійно визначає актуальні для неї типи зловмисників.

Для кожного типу зловмисника проводиться оцінка їхньої мотивації, рівня навичок і доступних ресурсів. Наприклад, внутрішній працівник може мати доступ до даних, але обмежені технічні знання, тоді як хакерська група може використовувати складні методи. Створені профілі допоможуть передбачити найімовірніші сценарії атак.

Крок 4: Оцінка впливу загроз

На цьому кроці треба оцінити, як кожна загроза може вплинути на організацію, враховуючи не лише прямі фінансові втрати, а й репутаційні, операційні та юридичні наслідки. Наприклад, витік даних може призвести до штрафів і втрати клієнтів, а збій сервера – до зупинки бізнес-процесів. Необхідно враховувати кілька аспектів:

Конфіденційність: необхідно визначити, наскільки серйозними будуть наслідки втрати чи розголошення даних. Наприклад, витік персональних даних клієнтів матиме більший вплив, ніж втрата публічної інформації.

Доступність: необхідно визначити, як довго триватиме відновлення після інциденту, і як це вплине на роботу компанії.

Репутація: необхідно визначити, чи постраждає довіра клієнтів і партнерів.

Легкість атаки: необхідно визначити, наскільки просто зловмиснику реалізувати атаку, враховуючи доступність інструментів і складність.

Рівень захисту: необхідно визначити, чи є в організації достатні заходи безпеки для протидії.

Крок 5: Розрахунок ризиків

Необхідно використати отримані оцінки ймовірності, впливу та цінності активів, щоб визначити рівень ризику для кожної загрози. Наприклад, загроза з високою ймовірністю, значним впливом і критичним активом матиме найвищий ризик, тоді як малоймовірна загроза з низьким впливом на некритичний актив буде менш пріоритетною.

Далі ризики сортуються за значущістю, щоб зрозуміти, на чому зосередити зусилля. Наприклад, атаки на клієнтські дані чи ключові сервери можуть бути пріоритетними через їхній потенційний вплив. Також не слід ігнорувати малоімовірні загрози з катастрофічними наслідками, такі як складні кібератаки, які можуть завдати значної шкоди.

Крок 6: Аналіз поширення інцидентів

Матриця поширення допоможе зрозуміти, як один інцидент може вплинути на інші активи. Наприклад, збій сервера може зупинити хмарні сервіси, а витік даних – спровокувати репутаційну кризу. Заповнення матриці може відбуватися як по прикладу, наведеному в описаному методі, так і кожною компанією самостійно, або за допомогою окремих аналітиків. Створена матриця допоможе зрозуміти ширші наслідки інцидентів і визначити, які активи потребують додаткової уваги.

Крок 7: Впровадження заходів зниження ризиків

Необхідно розробити та впровадити заходи для зниження ризиків, приділяючи особливу увагу загрозам із найвищим пріоритетом. Можна використовувати три основні типи заходів:

- Превентивні: Рекомендується встановлювати системи захисту, такі як антивірусне програмне забезпечення, брандмауери чи шифрування, щоб зменшити ймовірність успішних атак.
- Виявлення: Слід налаштувати системи моніторингу, наприклад, інструменти виявлення вторгнень, для швидкого реагування на інциденти.
- Реагування: Потрібно підготувати плани відновлення, такі як створення резервних копій або розробка процедур реагування, щоб мінімізувати наслідки інцидентів.

Наприклад, для захисту від фішингу доцільно навчати працівників розпізнавати підозрілі електронні листи та застосовувати фільтри електронної пошти. Для зменшення впливу збоїв серверів можна створювати резервні системи. Важливо переконатися, що обрані заходи відповідають рівню ризиків, а ресурси розподіляються раціонально.

Крок 8: Тестування та перевірка заходів

Слід регулярно перевіряти ефективність заходів захисту за допомогою симуляцій кібератак, тестування на проникнення або внутрішніх аудитів.

Наприклад, можна провести фішингову кампанію для працівників, щоб оцінити їхню готовність до реальної атаки, або перевірити працездатність резервних копій, щоб упевнитися в їхній надійності.

За результатами тестувань необхідно оновлювати заходи, усуваючи виявлені слабкі місця. Наприклад, якщо працівники часто стають жертвами фішингу, варто покращити програми навчання. Рекомендується документувати результати тестувань, щоб використовувати їх для подальшого вдосконалення системи захисту.

Крок 9: Моніторинг і оновлення оцінки

Оцінка ризиків є безперервним процесом. Потрібно налаштувати постійний моніторинг загроз за допомогою інструментів, таких як системи управління подіями безпеки, для виявлення підозрілих дій у реальному часі.

Слід прводити оцінку ризиків якомога частіше, а також після значних змін, наприклад, впровадження нових компонентів системи, реорганізації чи появи нових типів загроз. Рекомендується стежити за галузевими звітами та новинами про кіберзагрози, щоб залишатися в курсі актуальних тенденцій. Необхідно аналізувати будь які інциденти чи спроби атак, щоб удосконалювати підхід до оцінки та захисту.

Крок 10: Звітність і комунікація

Потрібно регулярно інформувати керівництво та зацікавлені сторони про результати оцінки ризиків і впроваджені заходи. Слід виділити ключові ризики, запропоновані дії та їхній вплив у зрозумілій формі, наприклад, через короткі звіти чи презентації.

Рекомендується пояснювати, як заходи захисту сприяють роботі компанії, наприклад, зменшують простої чи допомагають уникнути штрафів. Це сприятиме отриманню підтримки для фінансування та впровадження ініціатив із кібербезпеки. Також доцільно інформувати працівників про їхню роль у захисті, зокрема про важливість дотримання правил безпеки.

Висновки до розділу 2

Запропонований метод оцінки кіберризиків є комплексним підходом, який враховує ключові фактори для визначення рівня загроз. Імовірність реалізації загрози (P) визначається на основі статистичних даних щодо частоти виникнення інцидентів. Оцінка впливу (I) відображає наслідки інциденту для конфіденційності, доступності та репутації організації. Цінність активу (V) характеризує його вагомість і потенційний економічний ефект від атаки. Матриця поширення інцидентів враховує каскадні ефекти атак, що дозволяє уточнити рівень ризиків.

Цей метод забезпечує точну та деталізовану оцінку кіберризиків, сприяючи обґрунтованому прийняттю рішень щодо заходів кіберзахисту. Він дає змогу не лише оцінювати ризики для окремих активів, а й прогнозувати потенційні загрози, спричинені ланцюговими атаками. Метод вирізняється глибшим аналізом ризиків завдяки врахуванню каскадних ефектів, гнучкістю та адаптивністю до потреб різних організацій і секторів економіки, а також об’єктивністю, що базується на математичних розрахунках. У відповідному розділі наведено загальні рекомендації та покрокові дії для практичного застосування методу, що полегшує його впровадження організаціями.

3 ПРАКТИЧНЕ ВИКОРИСТАННЯ МЕТОДУ ОЦІНКИ РИЗИКУ

3.1 Визначення активів компанії та типів атак

Першим етапом є визначення основних активів компанії, їх вартості та важливості, а також попередня оцінка типів можливих атак для кожного з активів.

Наприклад, активи компанії можуть бути розділені на такі категорії:

1. Цифрова інформація та дані: (файли, бази даних).

2. Програмне забезпечення: (операційні системи, прикладні програми, інструменти розробки, ліцензії, внутрішні та сторонні сервіси).

3. Апаратне забезпечення: (комп’ютери, ноутбуки, мобільні пристрої).

4. Сервери: (веб-сервери, поштові сервери, DNS-сервери).

5. Мережева інфраструктура: (маршрутизатори, комутатори).

6. Хмарні сервіси та ресурси: (сховища даних, обчислювальні потужності).

На основі отриманих категорій можна визначити основні типи атак для кожної з них:

Цифрова інформація та дані: Витік даних, Ransomware, DDoS, Фішинг, SQL Injection

Програмне забезпечення: Malware Injection, Man-in-the-Middle, Reverse Engineering, Zero-Day Exploits

Апаратне забезпечення: Крадіжка, Підміна компонентів, Фізичне пошкодження

Сервери: DDoS, Brute Force, SQL Injection, XSS, CSRF, Man-in-the-Middle

Мережева інфраструктура: Man-in-the-Middle, спуфінг, Сніфінг, DDoS

Хмарні сервіси та ресурси: DDoS, Витік даних, Злам акаунтів, Man-in-the-Middle

3.2 Уточнення оцінки ризику на основі моделей порушника

Другим етапом є створення моделі порушника, визначення його мотивації, навичок та знань для здійснення конкретних атак

Наприклад, компанія може визначити для себе такі основні типи порушників:

1) Незадоволений працівник

Зазвичай це низько кваліфіковані працівники, які не мають спеціальних технічних знань, проте можуть завдати шкоди

2) Зловмисний інсайдер

Той, хто свідомо зливає інформацію або передає доступ конкурентам за винагороду, також може керуватися інструкціями досвідчених спеціалістів

3) Кіберзлочинні групи

Організовані групи висококваліфікованих хакерів, які атакують компанії з метою крадіжки даних, шантажу чи саботажу

4) Окремі хакери

Окремі особи, які прагнуть вкрасти дані чи завдати шкоди заради власної вигоди або репутації

3.3 Приклад розрахунку ризиків

Після цього можна приступити до розрахунку ризиків. Спочатку оцінюється ймовірність виникнення кожного типу інцидента на основі статистичних даних:

Таблиця 3.1 – Ймовірність виникнення інцидентів

		P
Цифрова інформація та дані	Витік даних	0,4
	Ransomware	0,5
	DDoS	1
	Фішинг	0,35
	SQL Injection	0,15
Програмне забезпечення	Malware Injection	0,2
	Man-in-the-Middle	0,1
	Reverse Engineering	0,1
	Zero-Day Exploits	0,05
Апаратне забезпечення	Крадіжка	0,3
	Підміна компонентів	0,05
	Фізичне пошкодження	0,2

Кінець таблиці 3.1

Сервери	DDoS	1
	Brute Force	0,2
	SQL Injection	0,15
	XSS	0,15
	CSRF	0,1
Мережева інфраструктура	DDoS	1
	Спуфінг	0,15
	Сніфінг	0,2
	Man-in-the-Middle	0,1
Хмарні сервіси та ресурси	DDoS	1
	Витік даних	0,4
	Злам акаунтів	0,35
	Man-in-the-Middle	0,1

Наступним кроком є оцінка впливу кожного типу інциденту. Створюється по одній таблиці для кожного типу порушника. При цьому індекси **PCI, IAA, RII, EAI, DCI, CDI** обраховуються один раз і є спільними для всіх таблиць, а індекс **AII** варіюється в залежності від типу порушника. Таблиці з розрахунками наведені в додатку А(Таблиці 4.1-4.5). На основі них можна вирахувати середнє значення впливу:

Таблиця 3.2 – Середнє значення впливу

I1	I2	I3	I4	Iсер
1,009	1,200	1,440	1,320	1,2422
0,787	1,003	1,597	1,327	1,1785
0,491	0,688	0,866	0,767	0,7029
1,313	1,608	2,963	2,374	2,0646
1,222	1,697	2,457	1,745	1,7802
0,854	1,070	1,826	1,421	1,2928
1,484	2,197	2,815	2,102	2,1495
1,910	2,009	3,099	2,604	2,4055
5,503	5,725	7,954	6,282	6,366
0,897	1,080	1,368	1,106	1,1128
2,637	2,857	3,251	2,593	2,8347
1,644	1,644	1,691	1,458	1,6094
0,339	0,565	0,791	0,530	0,5565
0,219	0,398	0,564	0,386	0,3917
1,051	1,428	2,069	1,692	1,5599
0,798	1,115	1,654	1,178	1,1864
1,420	1,983	2,941	2,096	2,11
0,280	0,435	0,620	0,388	0,4308
0,936	1,251	1,539	1,277	1,2507
1,026	1,241	1,792	1,333	1,3479
1,231	1,637	2,368	1,962	1,7991
0,153	0,288	0,490	0,288	0,3046
0,731	0,909	1,265	1,011	0,9791
0,584	0,854	1,313	1,043	0,9488
0,660	0,880	1,144	0,924	0,9017

Далі розраховується вартість активів та максимальна вартість кожного з можливих інцидентів

Таблиця 3.3 – Оцінка вартості активів

		V_d	I_a	AAVI	V
Цифрова інформація та дані	Витік даних	120 000,00 ₴	9	108 000,00 ₴	108 000 ₴
	Ransomware		7	84 000,00 ₴	84 000 ₴
	DDoS		3	36 000,00 ₴	36 000 ₴
	Фішинг		6	72 000,00 ₴	72 000 ₴
	SQL Injection		5	60 000,00 ₴	60 000 ₴
Програмне забезпечення	Malware Injection	100 000,00 ₴	8	80 000,00 ₴	80 000 ₴
	Man-in-the-Middle		6	60 000,00 ₴	60 000 ₴
	Reverse Engineering		8	80 000,00 ₴	80 000 ₴
	Zero-Day Exploits		9	90 000,00 ₴	90 000 ₴
Апаратне забезпечення	Крадіжка	105 000,00 ₴	5	52 500,00 ₴	52 500 ₴
	Підміна компонентів		6	63 000,00 ₴	63 000 ₴
	Фізичне пошкодження		8	84 000,00 ₴	84 000 ₴
Сервери	DDoS	95 000,00 ₴	2	19 000,00 ₴	19 000 ₴
	Brute Force		3	28 500,00 ₴	28 500 ₴
	SQL Injection		6	57 000,00 ₴	57 000 ₴
	XSS		5	47 500,00 ₴	47 500 ₴
	CSRF		6	57 000,00 ₴	57 000 ₴
Мережева інфраструктура	DDoS	60 000,00 ₴	4	24 000,00 ₴	24 000 ₴
	Спуфінг		5	30 000,00 ₴	30 000 ₴
	Сніфінг		5	30 000,00 ₴	30 000 ₴
	Man-in-the-Middle		7	42 000,00 ₴	42 000 ₴
Хмарні сервіси та ресурси	DDoS	30 000,00 ₴	2	6 000,00 ₴	6 000 ₴
	Витік даних		8	24 000,00 ₴	24 000 ₴
	Злам акаунтів		8	24 000,00 ₴	24 000 ₴
	Man-in-the-Middle		5	15 000,00 ₴	15 000 ₴

Тепер можна підрахувати значення ризику для окремих інцидентів **(P*I*V)**

Таблиця 3.4 – Значення ризиків

		P	I	V	R
Цифрова інформація та дані	Витік даних	0,4	1,242	108 000,00 ₴	53 662,13 ₴
	Ransomware	0,5	1,179	84 000,00 ₴	49 497,96 ₴
	DDoS	1	0,703	36 000,00 ₴	25 303,88 ₴
	Фішинг	0,35	2,065	72 000,00 ₴	52 027,13 ₴
	SQL Injection	0,15	1,780	60 000,00 ₴	16 022,11 ₴
Програмне забезпечення	Malware Injection	0,2	1,293	80 000,00 ₴	20 684,08 ₴
	Man-in-the-Middle	0,1	2,150	60 000,00 ₴	12 897,07 ₴
	Reverse Engineering	0,1	2,405	80 000,00 ₴	19 243,79 ₴
	Zero-Day Exploits	0,05	6,366	90 000,00 ₴	28 647,17 ₴
Апаратне забезпечення	Крадіжка	0,3	1,113	52 500,00 ₴	17 526,92 ₴
	Підміна компонентів	0,05	2,835	63 000,00 ₴	8 929,17 ₴
	Фізичне пошкодження	0,2	1,609	84 000,00 ₴	27 037,59 ₴
Сервери	DDoS	1	0,556	19 000,00 ₴	10 573,22 ₴
	Brute Force	0,2	0,392	28 500,00 ₴	2 232,75 ₴
	SQL Injection	0,15	1,560	57 000,00 ₴	13 337,15 ₴
	XSS	0,15	1,186	47 500,00 ₴	8 452,76 ₴
	CSRF	0,1	2,110	57 000,00 ₴	12 026,78 ₴
Мережева інфраструктура	DDoS	1	0,431	24 000,00 ₴	10 338,84 ₴
	Спуфінг	0,15	1,251	30 000,00 ₴	5 628,04 ₴
	Сніфінг	0,2	1,348	30 000,00 ₴	8 087,37 ₴
	Man-in-the-Middle	0,1	1,799	42 000,00 ₴	7 556,41 ₴
Хмарні сервіси та ресурси	DDoS	1	0,305	6 000,00 ₴	1 827,78 ₴
	Витік даних	0,4	0,979	24 000,00 ₴	9 399,25 ₴
	Злам акаунтів	0,35	0,949	24 000,00 ₴	7 969,57 ₴
	Man-in-the-Middle	0,1	0,902	15 000,00 ₴	1 352,53 ₴

Після цього створюється матриця поширення та розраховується R’(значення ризиків з урахуванням можливого поширення інцидентів)

Таблиця 3.5 – Матриця поширення

		Цифрова інформація та дані					Програмне забезпечення				Апаратне забезпечення			Сервери					Мережева інфраструктура				Хмарні сервіси та ресурси			
		Витік даних	Ransomware	DDoS	Фішинг	SQL Injection	Malware Injection	Man-in-the-Middle	Reverse Engineering	Zero-Day Exploits	Крадіжка	Підміна компонентів	Фізичне пошкодження	DDoS	Brute Force	SQL Injection	XSS	CSRF	DDoS	Спуфінг	Сніфінг	Man-in-the-Middle	DDoS	Витік даних	Злам акаунтів	Man-in-the-Middle
Цифрова інформація та дані	Витік даних	0	0,3	0,2	0,1	0,4	0,2	0,3	0,1	0,2	0	0	0	0,2	0,1	0,3	0,3	0,1	0,2	0,2	0,3	0,3	0,2	0,5	0,4	0,3
	Ransomware	0,4	0	0,3	0,1	0,2	0,3	0,2	0,1	0,2	0	0	0	0,2	0,1	0,2	0,2	0,1	0,2	0,1	0,2	0,2	0,2	0,4	0,3	0,2
	DDoS	0,2	0,2	0	0,1	0,1	0,2	0,3	0,1	0,2	0	0	0	0,4	0,1	0,1	0,1	0	0,5	0,2	0,3	0,3	0,3	0,2	0,2	0,3
	Фішинг	0,5	0,4	0,2	0	0,3	0,4	0,3	0,1	0,3	0	0	0	0,2	0,2	0,3	0,2	0,1	0,2	0,2	0,3	0,3	0,2	0,5	0,5	0,3
	SQL Injection	0,6	0,2	0,1	0,1	0	0,3	0,2	0,1	0,3	0	0	0	0,1	0,1	0,5	0,5	0,2	0,1	0,1	0,2	0,2	0,1	0,4	0,3	0,2
Програмне забезпечення	Malware Injection	0,4	0,3	0,2	0,2	0,3	0	0,4	0,3	0,5	0	0	0	0,2	0,2	0,3	0,3	0,1	0,2	0,2	0,3	0,4	0,2	0,4	0,4	0,3
	Man-in-the-Middle	0,5	0,2	0,3	0,2	0,2	0,3	0	0,2	0,3	0	0	0	0,3	0,2	0,2	0,2	0,1	0,4	0,4	0,5	0	0,3	0,3	0,3	0,5
	Reverse Engineering	0,2	0,1	0,1	0,1	0,2	0,4	0,2	0	0,6	0	0	0	0,1	0,1	0,1	0,1	0	0,1	0,1	0,2	0,2	0,1	0,2	0,2	0,2
	Zero-Day Exploits	0,3	0,2	0,2	0,2	0,4	0,5	0,3	0,5	0	0	0	0	0,2	0,2	0,4	0,3	0,1	0,2	0,2	0,3	0,3	0,2	0,4	0,4	0,3
Апаратне забезпечення	Крадіжка	0,5	0	0	0	0	0	0	0	0	0	0,2	0,3	0	0	0	0	0	0	0	0	0	0	0,3	0,2	0
	Підміна компонентів	0,3	0,1	0	0,1	0	0,3	0	0,2	0	0,3	0	0,2	0	0	0,1	0,1	0,1	0	0,5	0,5	0,7	0	0,1	0	0,1
	Фізичне пошкодження	0,1	0	0	0	0	0	0	0	0	0,2	0,2	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Сервери	DDoS	0,2	0,2	0,4	0,1	0,1	0,2	0,3	0,1	0,2	0	0	0	0	0,2	0,1	0,1	0	0,5	0,2	0,3	0,3	0,4	0,2	0,2	0,3
	Brute Force	0,3	0,2	0,2	0,2	0,3	0,3	0,3	0,1	0,2	0	0	0	0,2	0	0,3	0,2	0,1	0,2	0,2	0,3	0,3	0,2	0,4	0,4	0,3
	SQL Injection	0,6	0,2	0,1	0,1	0,5	0,3	0,2	0,1	0,3	0	0	0	0,1	0,1	0	0,5	0,2	0,1	0,1	0,2	0,2	0,1	0,4	0,3	0,2
	XSS	0,4	0,1	0,1	0,1	0,5	0,2	0,2	0,1	0,2	0	0	0	0,1	0,1	0,5	0	0,3	0,1	0,1	0,2	0,2	0,1	0,2	0,2	0,2
	CSRF	0,2	0,1	0	0,1	0,2	0,1	0,1	0	0,1	0	0	0	0	0,1	0,4	0,4	0	0	0,1	0,1	0,1	0	0,1	0,2	0,1
Мережева інфраструктура	DDoS	0,2	0,2	0,5	0,1	0,1	0,2	0,4	0,1	0,2	0	0	0	0,5	0,2	0,1	0,1	0	0	0,2	0,4	0,4	0,5	0,2	0,2	0,4
	Спуфінг	0,3	0,1	0,2	0,2	0,2	0,2	0,4	0,1	0,2	0	0	0	0,2	0,2	0,2	0,1	0,1	0,2	0	0,4	0,4	0,2	0,3	0,3	0,4
	Сніфінг	0,4	0,2	0,3	0,2	0,3	0,3	0,5	0,1	0,3	0	0	0	0,3	0,3	0,3	0,2	0,1	0,4	0,4	0	0,5	0,3	0,4	0,4	0,5
	Man-in-the-Middle	0,5	0,2	0,3	0,2	0,2	0,3	0	0,2	0,3	0	0	0	0,3	0,2	0,2	0,2	0,1	0,4	0,4	0,5	0	0,3	0,3	0,3	0,5
Хмарні сервіси та ресурси	DDoS	0,2	0,2	0,3	0,1	0,1	0,2	0,3	0,1	0,2	0	0	0	0,4	0,1	0,1	0,1	0	0,5	0,2	0,3	0,3	0	0,3	0,2	0,3
	Витік даних	0,5	0,4	0,2	0,1	0,4	0,2	0,3	0,1	0,2	0	0	0	0,2	0,1	0,3	0,3	0,1	0,2	0,2	0,3	0,3	0,3	0	0,5	0,3
	Злам акаунтів	0,5	0,3	0,2	0,3	0,4	0,4	0,3	0,2	0,3	0	0	0	0,2	0,3	0,4	0,2	0,1	0,2	0,3	0,4	0,3	0,2	0,5	0	0,4
	Man-in-the-Middle	0,3	0,2	0,3	0,2	0,2	0,3	0,5	0,2	0,3	0	0	0	0,3	0,2	0,2	0,2	0,1	0,4	0,4	0,5	0,5	0,3	0,3	0,3	0

Таблиця 3.6 – Кінцеві значення ризиків

		P	I	V	R	R'
Цифрова інформація та дані	Витік даних	0,4	1,242	108 000,00 ₴	53 662,13 ₴	68 423,00 ₴
	Ransomware	0,5	1,179	84 000,00 ₴	49 497,96 ₴	64 367,19 ₴
	DDoS	1	0,703	36 000,00 ₴	25 303,88 ₴	38 332,73 ₴
	Фішинг	0,35	2,065	72 000,00 ₴	52 027,13 ₴	73 218,48 ₴
	SQL Injection	0,15	1,780	60 000,00 ₴	16 022,11 ₴	35 030,78 ₴
Програмне забезпечення	Malware Injection	0,2	1,293	80 000,00 ₴	20 684,08 ₴	42 384,97 ₴
	Man-in-the-Middle	0,1	2,150	60 000,00 ₴	12 897,07 ₴	33 422,00 ₴
	Reverse Engineering	0,1	2,405	80 000,00 ₴	19 243,79 ₴	32 598,42 ₴
	Zero-Day Exploits	0,05	6,366	90 000,00 ₴	28 647,17 ₴	48 436,42 ₴
Апаратне забезпечення	Крадіжка	0,3	1,113	52 500,00 ₴	17 526,92 ₴	25 755,30 ₴
	Підміна компонентів	0,05	2,835	63 000,00 ₴	8 929,17 ₴	21 644,12 ₴
	Фізичне пошкодження	0,2	1,609	84 000,00 ₴	27 037,59 ₴	29 169,07 ₴
Сервери	DDoS	1	0,556	19 000,00 ₴	10 573,22 ₴	24 861,73 ₴
	Brute Force	0,2	0,392	28 500,00 ₴	2 232,75 ₴	19 955,47 ₴
	SQL Injection	0,15	1,560	57 000,00 ₴	13 337,15 ₴	32 614,32 ₴
	XSS	0,15	1,186	47 500,00 ₴	8 452,76 ₴	23 800,47 ₴
	CSRF	0,1	2,110	57 000,00 ₴	12 026,78 ₴	20 836,32 ₴
Мережева інфраструктура	DDoS	1	0,431	24 000,00 ₴	10 338,84 ₴	25 791,29 ₴
	Спуфінг	0,15	1,251	30 000,00 ₴	5 628,04 ₴	21 305,55 ₴
	Сніфінг	0,2	1,348	30 000,00 ₴	8 087,37 ₴	29 370,01 ₴
	Man-in-the-Middle	0,1	1,799	42 000,00 ₴	7 556,41 ₴	28 081,34 ₴
Хмарні сервіси та ресурси	DDoS	1	0,305	6 000,00 ₴	1 827,78 ₴	16 453,18 ₴
	Витік даних	0,4	0,979	24 000,00 ₴	9 399,25 ₴	29 772,30 ₴
	Злам акаунтів	0,35	0,949	24 000,00 ₴	7 969,57 ₴	31 813,70 ₴
	Man-in-the-Middle	0,1	0,902	15 000,00 ₴	1 352,53 ₴	21 641,07 ₴

Аналіз отриманих даних демонструє результати оцінки ризиків для кіберсистем на основі розробленого методу, який враховує поширення інцидентів та їхній вплив на різні типи активів. Проведений розрахунок дозволяє кількісно оцінити ймовірність виникнення кіберзагроз, їхній потенційний вплив та фінансові наслідки, що забезпечує можливість ідентифікації критичних точок у системі.

Результати таблиці свідчать, що найвищий рівень ризику характерний для інцидентів, пов’язаних з фішингом, витоком даних та ransomware. Це обумовлюється поширеністю таких типів атак, а також складністю забезпечення ефективного захисту від них.

На наступній діаграмі представлена візуалізація значень ризику без урахування поширення інцидентів та з його врахуванням(R та R' відповідно). Вона показує зміну рівня ризику після створення матриці поширення.

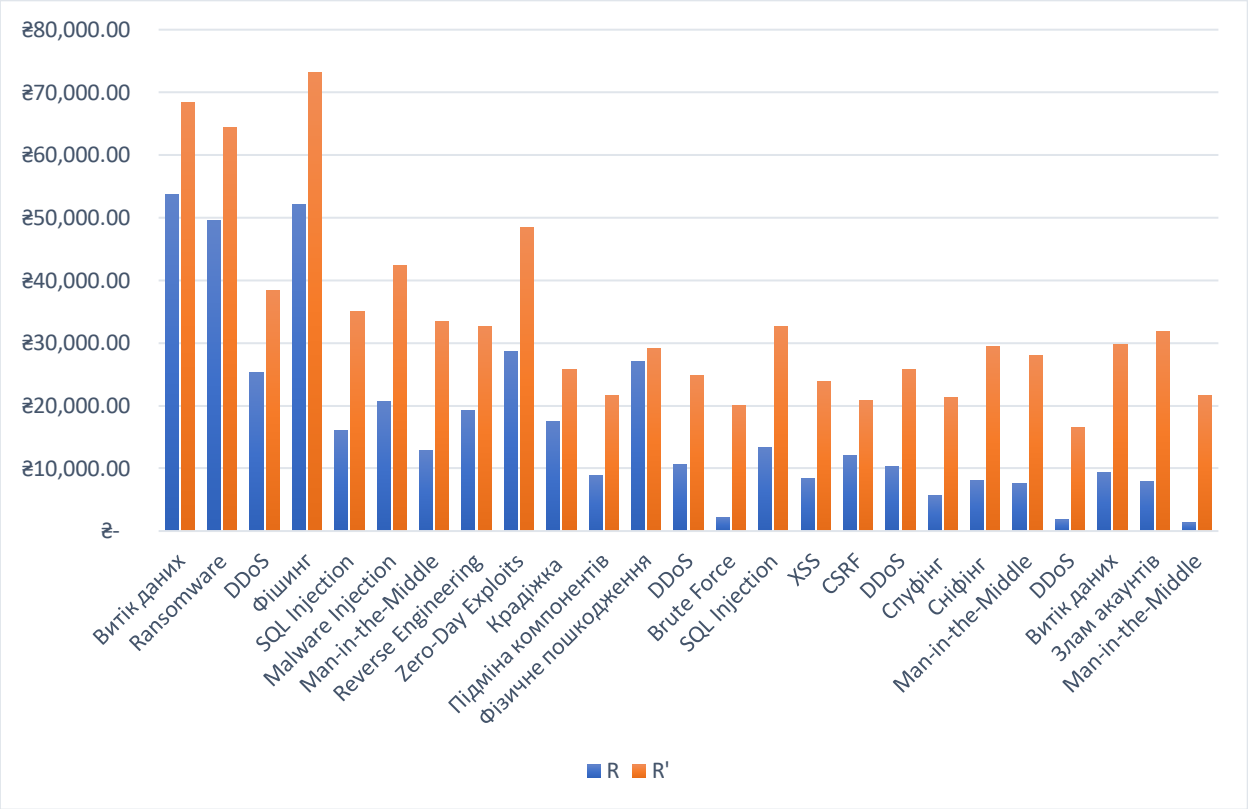

Рисунок 3.1 – Діаграма значень ризику без урахування поширення інцидентів та з його врахуванням

Висновки до розділу 3

У третьому розділі представлено приклад практичного застосування розробленого методу оцінки ризиків у кіберсистемах на основі аналізу інцидентів та їх поширення. Метод включає кількісну оцінку ризиків з урахуванням ймовірності виникнення інцидентів, їх впливу та поширення в системі. Було проведено аналіз ризиків для різних типів активів (цифрова інформація, програмне забезпечення, апаратне забезпечення, сервери, мережева інфраструктура, хмарні сервіси) з урахуванням типових кіберзагроз, таких як витік даних, ransomware, DDoS-атаки, фішинг, SQL-ін’єкції тощо.

Розроблений алгоритм передбачає побудову матриці поширення інцидентів, яка дозволяє врахувати взаємозв’язки між різними активами та загрозами, а також розрахунок ризиків у фінансовому еквіваленті (R та R').

Результати моделювання показали, що найвищі ризики пов’язані з інцидентами, такими як фішинг, витік даних та ransomware для цифрової інформації, а також із zero-day exploits для програмного забезпечення. Це свідчить про необхідність пріоритетного захисту відповідних активів.

Експериментальне підтвердження ефективності методу продемонструвало його здатність ідентифікувати критичні точки в кіберсистемах та прогнозувати потенційні збитки. Отримані результати дозволяють організаціям оптимізувати розподіл ресурсів для захисту інформаційних систем, зосереджуючи увагу на найбільш уразливих активах і загрозах. Практична цінність методу полягає в його універсальності та можливості адаптації до різних типів кіберсистем, що робить його корисним інструментом для вдосконалення систем управління кіберрисками.

ВИСНОВКИ

У результаті виконання дипломної роботи було розроблено метод оцінки ризиків у кіберсистемах на основі аналізу інцидентів та їх поширення, що є актуальним внеском у сферу кібербезпеки. Основні наукові та практичні результати роботи полягають у наступному:

Проведено аналіз сучасних методологій оцінки ризиків (CRAMM, NIST, ISO 27005, FAIR, OCTAVE, COBIT, ISO 31010), що дозволило виявити їхні сильні та слабкі сторони. На основі цього розроблено власний метод, який поєднує кількісний підхід із урахуванням поширення інцидентів у кіберсистемах. Метод враховує ймовірність виникнення загроз, їхній вплив та взаємозв'язки між активами, що відповідає сучасним вимогам до оцінки кіберризиків. Використання матриці поширення інцидентів та фінансового еквіваленту ризиків забезпечує точність і практичну застосовність методу, що узгоджується з передовими підходами, такими як FAIR, але адаптовано до ширшого спектру кіберсистем.

Розроблений метод було апробовано на прикладі моделювання кіберзагроз для різних типів активів (цифрова інформація, програмне забезпечення, апаратне забезпечення, сервери, мережева інфраструктура, хмарні сервіси). Результати показали здатність методу ідентифікувати критичні точки та прогнозувати потенційні збитки, що підтверджує його практичну цінність. Метод може бути впроваджений у діяльність організацій, які керують інформаційними системами, зокрема у фінансовому секторі, державних установах, IT-компаніях та промислових підприємствах. Його універсальність дозволяє адаптувати метод до кіберсистем різного масштабу та складності.

Наукова значущість роботи полягає у створенні нового методу оцінки ризиків, який враховує можливість поширення інцидентів у кіберсистемах, що є новим підходом у порівнянні з традиційними методологіями. Науково-технічна значущість проявляється у можливості використання методу для

вдосконалення систем управління кіберрисками, що сприяє підвищенню безпеки інформаційних систем. Соціально-економічна значущість роботи полягає у потенційному зниженні фінансових втрат організацій від кібератак, а також у підвищенні рівня кібербезпеки, що має важливе значення для суспільства в умовах зростання кіберзагроз. Результати роботи були представлені на XXIII Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених і опубліковані у збірнику матеріалів, що підтверджує їх визнання науковою спільнотою.

Таким чином, розроблений метод оцінки ризиків є важливим кроком у підвищенні безпеки кіберсистем, має значний потенціал для практичного застосування та відкриває перспективи для подальших досліджень у сфері кібербезпеки.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Теоретичні і прикладні проблеми фізики, математики та інформатики: матеріалиXXIII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених (14 – 17 травня 2025 р., м. Київ, Україна) / Уклад.: Пономаренко С. М., Бех С. В., Степаненко В. М., Козленко О. В., Мирошникова І. Ю., Мікава П. В., Деркач О. Г. – Київ : КПІ ім. Ігоря Сікорського, Видавництво «Політехніка», 2025. – 474 с. ISBN 978-966-990-053-1.

2. Denning D. E. CRAMM: A Risk Analysis Method for Information Systems [Текст] / D. E. Denning // Computers & Security. – 1989. – Vol. 8, Iss. 3. – с. 233–240.

3. Yazar Z. A Qualitative Risk Analysis and Management Tool – CRAMM [Електронний ресурс] / Z. Yazar. – SANS Institute InfoSec Reading Room, 2002. – 15 с. – Режим доступу: https://www.sans.org/reading-room/whitepapers/auditing/qualitative-risk-analysis-management-tool-cramm-82.

4. Ross R. S. Managing Information Security Risk: Organization, Mission, and Information System View (NIST SP 800-39) [Текст] / R. S. Ross. – Gaithersburg: National Institute of Standards and Technology, 2011. – 88 с. – Режим доступу: https://csrc.nist.gov/publications/sp800.

5. NIST Risk Management Framework [Електронний ресурс] / National Institute of Standards and Technology. – 2025. – Режим доступу: https://csrc.nist.gov/projects/risk-management.

6. Бойко А. О. Управління ризиками інформаційної безпеки відповідно до стандарту ISO/IEC 27005 [Текст] / А. О. Бойко // Наукові записки НаУКМА. Комп’ютерні науки. – 2019. – Т. 2. – С. 45–52.

7. ISO 27005: Everything You Need to Know if You Are Considering Implementing It [Електронний ресурс] / C-Risk. – 2023. – Режим доступу: https://www.c-risk.com/en/blog/iso-27005-everything-you-need-to-know-if-you-are-considering-implementing-it.

8. Freund J. Measuring and Managing Information Risk: A FAIR Approach [Текст] / J. Freund, J. Jones. – Oxford: Butterworth-Heinemann, 2014. – 408 с.

9. Standards Groups and Regulators Recognize FAIR [Електронний ресурс] / FAIR Institute. – 2017. – Режим доступу: https://www.fairinstitute.org/blog/standards-groups-and-regulators-recognize-fair.

10. Alberts C. Managing Information Security Risks: The OCTAVE Approach [Текст] / C. Alberts, A. Dorofee. – Boston: Addison-Wesley, 2002. – 512 с.

11. Woody C. Considering Operational Security Risks with OCTAVE Allegro [Електронний ресурс] / C. Woody, C. Alberts. – Pittsburgh: Software Engineering Institute, Carnegie Mellon University, 2008. – 28 с. – Режим доступу: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8765.

12. Гнатів Н. І. Застосування COBIT для управління IT-процесами в організаціях [Текст] / Н. І. Гнатів // Вісник Національного університету «Львівська політехніка». Інформаційні системи та мережі. – 2020. – № 917. – С. 123–130.

13. COBIT 2019 Framework: Governance and Management Objectives [Електронний ресурс] / ISACA. – Schaumburg: ISACA, 2018. – 300 с. – Режим доступу: https://www.isaca.org/resources/cobit

14. Кравець П. О. Використання стандарту ISO 31010 для оцінки ризиків у кібербезпеці [Текст] / П. О. Кравець // Південноукраїнський правничий часопис. – 2023. – № 1. – С. 89–95.

15. Purdy G. ISO 31010: Risk Assessment Techniques [Текст] / G. Purdy // Risk Management Journal. – 2010. – Vol. 12, Iss. 4. – С. 15–24.

16. Rising Cyber Threats Pose Serious Concerns for Financial Stability [Електронний ресурс] / International Monetary Fund. – 2024. – Режим доступу: https://www.imf.org/en/Blogs/Articles/2024/04/09/Rising-Cyber-Threats-Pose-Serious-Concerns-for-Financial-Stability.

17. Risk Management [Електронний ресурс] / Plymouth University // Security and Risk Management Articles. – 2023. – 8 с. – Режим доступу: https://pearl.plymouth.ac.uk/cgi/viewcontent.cgi?params=/context/secam-research/article/1450/&path_info=encyclopedia_01_00050_v2.pdf.

18. 2024 Data Breach Investigations Report [Електронний ресурс] / Verizon. – 2024. – 104 с. – Режим доступу: https://www.verizon.com/business/resources/Tc94/reports/2024-dbir-data-breach-investigations-report.pdf.

19. ENISA Threat Landscape 2024 [Електронний ресурс] / European Union Agency for Cybersecurity (ENISA). – 2024. – 132 с. – Режим доступу: https://www.enisa.europa.eu/sites/default/files/202411/ENISA%20Threat%20Landscape%202024_0.pdf.

20. Cybersecurity Statistics of 2024 [Електронний ресурс] / NordLayer. – 2024. – Режим доступу: https://nordlayer.com/blog/cybersecurity-statistics-of-2024/.

ДОДАТОК А

Таблиця А.1 – Розрахунок впливу для незадоволеного працівника

		S_{data}	L_{data}	R_{data}	PCI	A_v	A_i	IAA	B_v	C_i	M_p	RII	A_m	A_s	A_o	AII	T_e	R_i	C_e	EAI	EAінорм	C_p	C_m	C_i	DCI	Dp	Dd	Dm	Dr	CDI	I
Цифрова інформація та дані	Витік даних	4	3	5	0,750	2	2	0,250	5	7	6	0,556	5	1	2	0,275	10	2	2	0,400	0,015	3	2	3	0,417	6	7	3	8	2,875	1,009
	Ransomware	3	2	2	0,333	3	2	0,375	2	3	8	0,370	3	1	1	0,100	5	4	4	3,200	0,127	4	2	3	0,500	8	6	3	7	3,240	0,787
	DDoS	1	1	2	0,083	3	1	0,250	1	2	2	0,074	5	1	2	0,275	3	3	3	3,000	0,119	2	4	2	0,417	7	9	6	6	2,370	0,491
	Фішинг	2	2	1	0,167	1	2	0,125	3	1	3	0,148	3	1	2	0,175	5	5	4	4,000	0,159	2	2	3	0,333	5	4	5	4	7,071	1,313
	SQL Injection	4	3	3	0,583	2	3	0,375	4	2	4	0,259	1	1	1	0,000	15	2	1	0,133	0,004	3	3	3	0,500	6	6	4	4	5,701	1,222
Програмне забезпечення	Malware Injection	3	3	2	0,417	3	4	0,625	6	4	5	0,444	3	1	1	0,100	7	3	3	1,286	0,050	4	2	3	0,500	8	7	2	7	3,240	0,854
	Man-in-the-Middle	4	3	2	0,500	4	2	0,500	3	4	5	0,333	2	1	1	0,050	4	3	3	2,250	0,089	3	4	3	0,583	6	5	5	4	5,701	1,484
	Reverse Engineering	4	4	4	0,750	4	4	0,750	6	5	8	0,593	1	1	1	0,000	20	1	1	0,050	0,001	4	3	4	0,667	5	6	6	3	5,941	1,910
	Zero-Day Exploits	5	4	5	0,917	5	5	1,000	8	3	9	0,630	1	1	1	0,000	30	1	1	0,033	0,000	5	5	5	1,000	4	5	4	2	13,368	5,503
Апаратне забезпечення	Крадіжка	3	2	2	0,333	4	2	0,500	4	1	3	0,185	2	2	3	0,325	2	5	2	5,000	0,199	3	2	1	0,250	4	6	6	7	3,143	0,897
	Підміна компонентів	4	3	3	0,583	3	2	0,375	5	2	4	0,296	3	3	3	0,500	1	4	4	16,000	0,640	2	3	3	0,417	6	4	5	5	5,263	2,637
	Фізичне пошкодження	3	2	1	0,250	4	2	0,500	5	1	3	0,222	4	4	4	0,750	1	5	5	25,000	1,000	4	2	1	0,333	2	6	7	8	2,794	1,644
Сервери	DDoS	2	1	2	0,167	3	1	0,250	2	1	2	0,074	3	1	1	0,100	4	3	4	3,000	0,119	2	4	2	0,417	6	7	7	8	2,086	0,339
	Brute Force	3	2	1	0,250	2	2	0,250	3	2	2	0,148	2	1	1	0,050	20	5	5	1,250	0,049	3	2	3	0,417	9	8	8	9	1,425	0,219
	SQL Injection	4	3	3	0,583	3	3	0,500	4	3	3	0,259	1	1	1	0,000	18	2	1	0,111	0,003	4	3	3	0,583	5	6	5	5	4,525	1,051
	XSS	4	4	2	0,583	3	2	0,375	4	2	3	0,222	1	1	1	0,000	21	2	1	0,095	0,002	3	3	3	0,500	5	7	4	6	3,803	0,798
	CSRF	3	4	2	0,500	3	3	0,500	2	2	4	0,185	1	1	1	0,000	19	2	1	0,105	0,003	4	3	3	0,583	4	6	4	4	6,760	1,420
Мережева інфраструктура	DDoS	2	1	1	0,083	3	1	0,250	2	1	3	0,111	2	1	2	0,125	5	3	3	1,800	0,071	3	2	3	0,417	7	8	7	8	1,851	0,280
	Спуфінг	4	3	3	0,583	4	3	0,625	4	3	5	0,333	2	1	2	0,125	3	4	3	4,000	0,159	3	2	3	0,417	8	5	6	6	3,143	0,936
	Сніфінг	3	2	2	0,333	5	2	0,625	2	2	3	0,148	2	1	2	0,125	2	4	4	8,000	0,319	3	3	3	0,500	8	6	5	5	3,679	1,026
	Man-in-the-Middle	4	3	2	0,500	4	3	0,625	5	2	4	0,296	1	1	1	0,000	4	4	3	3,000	0,119	4	4	2	0,583	7	4	5	5	4,873	1,231
Хмарні сервіси та ресурси	DDoS	1	2	1	0,083	3	1	0,250	2	1	2	0,074	1	1	1	0,000	5	3	3	1,800	0,071	2	3	2	0,333	7	9	8	8	1,617	0,153
	Витік даних	4	2	4	0,583	2	3	0,375	5	6	4	0,444	1	1	2	0,075	10	2	2	0,400	0,015	2	2	3	0,333	9	7	2	7	3,049	0,731
	Злам акаунтів	3	2	3	0,417	2	2	0,250	4	7	4	0,444	1	1	1	0,000	14	2	3	0,429	0,016	2	2	3	0,333	9	5	5	6	3,240	0,584
	Man-in-the-Middle	3	3	4	0,583	4	3	0,625	3	5	4	0,333	1	1	1	0,000	5	3	3	1,800	0,071	3	3	3	0,500	8	8	5	6	2,641	0,660

Таблиця А.2 – Розрахунок впливу для зловмисного інсайдера

		S_{data}	L_{data}	R_{data}	PCI	A_v	A_i	IAA	B_v	C_i	M_p	RII	A_m	A_s	A_o	AII	T_e	R_i	C_e	EAI	EAінорм	C_p	C_m	C_i	DCI	Dp	Dd	Dm	Dr	CDI	I
Цифрова інформація та дані	Витік даних	4	3	5	0,750	2	2	0,250	5	7	6	0,556	5	2	3	0,475	10	2	2	0,400	0,015	3	2	3	0,417	6	7	3	8	2,875	1,200
	Ransomware	3	2	2	0,333	3	2	0,375	2	3	8	0,370	3	2	2	0,300	5	4	4	3,200	0,127	4	2	3	0,500	8	6	3	7	3,240	1,003
	DDoS	1	1	2	0,083	3	1	0,250	1	2	2	0,074	5	3	2	0,525	3	3	3	3,000	0,119	2	4	2	0,417	7	9	6	6	2,370	0,688
	Фішинг	2	2	1	0,167	1	2	0,125	3	1	3	0,148	3	2	2	0,300	5	5	4	4,000	0,159	2	2	3	0,333	5	4	5	4	7,071	1,608
	SQL Injection	4	3	3	0,583	2	3	0,375	4	2	4	0,259	2	2	2	0,250	15	2	1	0,133	0,004	3	3	3	0,500	6	6	4	4	5,701	1,697
Програмне забезпечення	Malware Injection	3	3	2	0,417	3	4	0,625	6	4	5	0,444	3	2	2	0,300	7	3	3	1,286	0,050	4	2	3	0,500	8	7	2	7	3,240	1,070
	Man-in-the-Middle	4	3	2	0,500	4	2	0,500	3	4	5	0,333	3	3	2	0,425	4	3	3	2,250	0,089	3	4	3	0,583	6	5	5	4	5,701	2,197
	Reverse Engineering	4	4	4	0,750	4	4	0,750	6	5	8	0,593	2	1	1	0,050	20	1	1	0,050	0,001	4	3	4	0,667	5	6	6	3	5,941	2,009
	Zero-Day Exploits	5	4	5	0,917	5	5	1,000	8	3	9	0,630	2	1	1	0,050	30	1	1	0,033	0,000	5	5	5	1,000	4	5	4	2	13,368	5,725
Апаратне забезпечення	Крадіжка	3	2	2	0,333	4	2	0,500	4	1	3	0,185	3	3	3	0,500	2	5	2	5,000	0,199	3	2	1	0,250	4	6	6	7	3,143	1,080
	Підміна компонентів	4	3	3	0,583	3	2	0,375	5	2	4	0,296	3	4	3	0,625	1	4	4	16,000	0,640	2	3	3	0,417	6	4	5	5	5,263	2,857
	Фізичне пошкодження	3	2	1	0,250	4	2	0,500	5	1	3	0,222	4	4	4	0,750	1	5	5	25,000	1,000	4	2	1	0,333	2	6	7	8	2,794	1,644
Сервери	DDoS	2	1	2	0,167	3	1	0,250	2	1	2	0,074	3	3	2	0,425	4	3	4	3,000	0,119	2	4	2	0,417	6	7	7	8	2,086	0,565
	Brute Force	3	2	1	0,250	2	2	0,250	3	2	2	0,148	3	3	2	0,425	20	5	5	1,250	0,049	3	2	3	0,417	9	8	8	9	1,425	0,398
	SQL Injection	4	3	3	0,583	3	3	0,500	4	3	3	0,259	2	2	2	0,250	18	2	1	0,111	0,003	4	3	3	0,583	5	6	5	5	4,525	1,428
	XSS	4	4	2	0,583	3	2	0,375	4	2	3	0,222	2	2	2	0,250	21	2	1	0,095	0,002	3	3	3	0,500	5	7	4	6	3,803	1,115
	CSRF	3	4	2	0,500	3	3	0,500	2	2	4	0,185	2	2	2	0,250	19	2	1	0,105	0,003	4	3	3	0,583	4	6	4	4	6,760	1,983
Мережева інфраструктура	DDoS	2	1	1	0,083	3	1	0,250	2	1	3	0,111	3	2	3	0,375	5	3	3	1,800	0,071	3	2	3	0,417	7	8	7	8	1,851	0,435
	Спуфінг	4	3	3	0,583	4	3	0,625	4	3	5	0,333	3	3	2	0,425	3	4	3	4,000	0,159	3	2	3	0,417	8	5	6	6	3,143	1,251
	Сніфінг	3	2	2	0,333	5	2	0,625	2	2	3	0,148	3	2	2	0,300	2	4	4	8,000	0,319	3	3	3	0,500	8	6	5	5	3,679	1,241
	Man-in-the-Middle	4	3	2	0,500	4	3	0,625	5	2	4	0,296	2	2	2	0,250	4	4	3	3,000	0,119	4	4	2	0,583	7	4	5	5	4,873	1,637
Хмарні сервіси та ресурси	DDoS	1	2	1	0,083	3	1	0,250	2	1	2	0,074	2	2	2	0,250	5	3	3	1,800	0,071	2	3	2	0,333	7	9	8	8	1,617	0,288
	Витік даних	4	2	4	0,583	2	3	0,375	5	6	4	0,444	2	2	2	0,250	10	2	2	0,400	0,015	2	2	3	0,333	9	7	2	7	3,049	0,909
	Злам акаунтів	3	2	3	0,417	2	2	0,250	4	7	4	0,444	2	2	2	0,250	14	2	3	0,429	0,016	2	2	3	0,333	9	5	5	6	3,240	0,854
	Man-in-the-Middle	3	3	4	0,583	4	3	0,625	3	5	4	0,333	2	2	2	0,250	5	3	3	1,800	0,071	3	3	3	0,500	8	8	5	6	2,641	0,880

Таблиця А.3 – Розрахунок впливу для кіберзлочинних груп

		S_{data}	L_{data}	R_{data}	PCI	A_v	A_i	IAA	B_v	C_i	M_p	RII	A_m	A_s	A_o	AII	T_e	R_i	C_e	EAI	EAінорм	C_p	C_m	C_i	DCI	Dp	Dd	Dm	Dr	CDI	I
Цифрова інформація та дані	Витік даних	4	3	5	0,750	2	2	0,250	5	7	6	0,556	4	5	2	0,725	10	2	2	0,400	0,015	3	2	3	0,417	6	7	3	8	2,875	1,440
	Ransomware	3	2	2	0,333	3	2	0,375	2	3	8	0,370	5	5	3	0,850	5	4	4	3,200	0,127	4	2	3	0,500	8	6	3	7	3,240	1,597
	DDoS	1	1	2	0,083	3	1	0,250	1	2	2	0,074	3	5	3	0,750	3	3	3	3,000	0,119	2	4	2	0,417	7	9	6	6	2,370	0,866
	Фішинг	2	2	1	0,167	1	2	0,125	3	1	3	0,148	4	5	4	0,875	5	5	4	4,000	0,159	2	2	3	0,333	5	4	5	4	7,071	2,963
	SQL Injection	4	3	3	0,583	2	3	0,375	4	2	4	0,259	4	5	1	0,650	15	2	1	0,133	0,004	3	3	3	0,500	6	6	4	4	5,701	2,457
Програмне забезпечення	Malware Injection	3	3	2	0,417	3	4	0,625	6	4	5	0,444	5	5	5	1,000	7	3	3	1,286	0,050	4	2	3	0,500	8	7	2	7	3,240	1,826
	Man-in-the-Middle	4	3	2	0,500	4	2	0,500	3	4	5	0,333	3	5	3	0,750	4	3	3	2,250	0,089	3	4	3	0,583	6	5	5	4	5,701	2,815
	Reverse Engineering	4	4	4	0,750	4	4	0,750	6	5	8	0,593	3	5	1	0,600	20	1	1	0,050	0,001	4	3	4	0,667	5	6	6	3	5,941	3,099
	Zero-Day Exploits	5	4	5	0,917	5	5	1,000	8	3	9	0,630	2	5	1	0,550	30	1	1	0,033	0,000	5	5	5	1,000	4	5	4	2	13,368	7,954
Апаратне забезпечення	Крадіжка	3	2	2	0,333	4	2	0,500	4	1	3	0,185	2	5	4	0,775	2	5	2	5,000	0,199	3	2	1	0,250	4	6	6	7	3,143	1,368
	Підміна компонентів	4	3	3	0,583	3	2	0,375	5	2	4	0,296	2	5	5	0,850	1	4	4	16,000	0,640	2	3	3	0,417	6	4	5	5	5,263	3,251
	Фізичне пошкодження	3	2	1	0,250	4	2	0,500	5	1	3	0,222	1	5	5	0,800	1	5	5	25,000	1,000	4	2	1	0,333	2	6	7	8	2,794	1,691
Сервери	DDoS	2	1	2	0,167	3	1	0,250	2	1	2	0,074	3	5	3	0,750	4	3	4	3,000	0,119	2	4	2	0,417	6	7	7	8	2,086	0,791
	Brute Force	3	2	1	0,250	2	2	0,250	3	2	2	0,148	2	5	4	0,775	20	5	5	1,250	0,049	3	2	3	0,417	9	8	8	9	1,425	0,564
	SQL Injection	4	3	3	0,583	3	3	0,500	4	3	3	0,259	3	5	2	0,675	18	2	1	0,111	0,003	4	3	3	0,583	5	6	5	5	4,525	2,069
	XSS	4	4	2	0,583	3	2	0,375	4	2	3	0,222	3	5	2	0,675	21	2	1	0,095	0,002	3	3	3	0,500	5	7	4	6	3,803	1,654
	CSRF	3	4	2	0,500	3	3	0,500	2	2	4	0,185	3	5	2	0,675	19	2	1	0,105	0,003	4	3	3	0,583	4	6	4	4	6,760	2,941
Мережева інфраструктура	DDoS	2	1	1	0,083	3	1	0,250	2	1	3	0,111	3	5	2	0,675	5	3	3	1,800	0,071	3	2	3	0,417	7	8	7	8	1,851	0,620
	Спуфінг	4	3	3	0,583	4	3	0,625	4	3	5	0,333	2	5	3	0,700	3	4	3	4,000	0,159	3	2	3	0,417	8	5	6	6	3,143	1,539
	Сніфінг	3	2	2	0,333	5	2	0,625	2	2	3	0,148	3	5	3	0,750	2	4	4	8,000	0,319	3	3	3	0,500	8	6	5	5	3,679	1,792
	Man-in-the-Middle	4	3	2	0,500	4	3	0,625	5	2	4	0,296	2	5	3	0,700	4	4	3	3,000	0,119	4	4	2	0,583	7	4	5	5	4,873	2,368
Хмарні сервіси та ресурси	DDoS	1	2	1	0,083	3	1	0,250	2	1	2	0,074	2	5	2	0,625	5	3	3	1,800	0,071	2	3	2	0,333	7	9	8	8	1,617	0,490
	Витік даних	4	2	4	0,583	2	3	0,375	5	6	4	0,444	3	5	1	0,600	10	2	2	0,400	0,015	2	2	3	0,333	9	7	2	7	3,049	1,265
	Злам акаунтів	3	2	3	0,417	2	2	0,250	4	7	4	0,444	3	5	2	0,675	14	2	3	0,429	0,016	2	2	3	0,333	9	5	5	6	3,240	1,313
	Man-in-the-Middle	3	3	4	0,583	4	3	0,625	3	5	4	0,333	2	5	1	0,550	5	3	3	1,800	0,071	3	3	3	0,500	8	8	5	6	2,641	1,144

Таблиця А.4 – Розрахунок впливу для окремих хакерів

		S_{data}	L_{data}	R_{data}	PCI	A_c	A_i	IAA	B_v	C_i	M_p	RII	A_m	A_k	A_n	AII	T_e	R_i	C_e	EAI	ЕАІнорм	C_p	C_m	C_i	DCI	Dp	Dd	Dm	Dr	CDI	I
Цифрова інформація та дані	Витік даних	4	3	5	0,750	2	2	0,250	5	7	6	0,556	4	4	2	0,600	10	2	2	0,400	0,015	3	2	3	0,417	6	7	3	8	2,875	1,320
	Ransomware	3	2	2	0,333	3	2	0,375	2	3	8	0,370	5	3	3	0,600	5	4	4	3,200	0,127	4	2	3	0,500	8	6	3	7	3,240	1,327
	DDoS	1	1	2	0,083	3	1	0,250	1	2	2	0,074	3	4	3	0,625	3	3	3	3,000	0,119	2	4	2	0,417	7	9	6	6	2,370	0,767
	Фішинг	2	2	1	0,167	1	2	0,125	3	1	3	0,148	4	3	4	0,625	5	5	4	4,000	0,159	2	2	3	0,333	5	4	5	4	7,071	2,374
	SQL Injection	4	3	3	0,583	2	3	0,375	4	2	4	0,259	4	2	1	0,275	15	2	1	0,133	0,004	3	3	3	0,500	6	6	4	4	5,701	1,745
Програмне забезпечення	Malware Injection	3	3	2	0,417	3	4	0,625	6	4	5	0,444	5	2	5	0,625	7	3	3	1,286	0,050	4	2	3	0,500	8	7	2	7	3,240	1,421
	Man-in-the-Middle	4	3	2	0,500	4	2	0,500	3	4	5	0,333	3	2	3	0,375	4	3	3	2,250	0,089	3	4	3	0,583	6	5	5	4	5,701	2,102
	Reverse Engineering	4	4	4	0,750	4	4	0,750	6	5	8	0,593	3	3	1	0,350	20	1	1	0,050	0,001	4	3	4	0,667	5	6	6	3	5,941	2,604
	Zero-Day Exploits	5	4	5	0,917	5	5	1,000	8	3	9	0,630	2	2	1	0,175	30	1	1	0,033	0,000	5	5	5	1,000	4	5	4	2	13,368	6,282
Апаратне забезпечення	Крадіжка	3	2	2	0,333	4	2	0,500	4	1	3	0,185	2	3	4	0,525	2	5	2	5,000	0,199	3	2	1	0,250	4	6	6	7	3,143	1,106
	Підмна компонентів	4	3	3	0,583	3	2	0,375	5	2	4	0,296	2	2	5	0,475	1	4	4	16,000	0,640	2	3	3	0,417	6	4	5	5	5,263	2,593
	Фізичне пошкодження	3	2	1	0,250	4	2	0,500	5	1	3	0,222	1	3	5	0,550	1	5	5	25,000	1,000	4	2	1	0,333	2	6	7	8	2,794	1,458
Сервери	DDoS	2	1	2	0,167	3	1	0,250	2	1	2	0,074	3	2	3	0,375	4	3	4	3,000	0,119	2	4	2	0,417	6	7	7	8	2,086	0,530
	Brute Force	3	2	1	0,250	2	2	0,250	3	2	2	0,148	2	2	4	0,400	20	5	5	1,250	0,049	3	2	3	0,417	9	8	8	9	1,425	0,386
	SQL Injection	4	3	3	0,583	3	3	0,500	4	3	3	0,259	3	3	2	0,425	18	2	1	0,111	0,003	4	3	3	0,583	5	6	5	5	4,525	1,692
	XSS	4	4	2	0,583	3	2	0,375	4	2	3	0,222	3	2	2	0,300	21	2	1	0,095	0,002	3	3	3	0,500	5	7	4	6	3,803	1,178
	CSRF	3	4	2	0,500	3	3	0,500	2	2	4	0,185	3	2	2	0,300	19	2	1	0,105	0,003	4	3	3	0,583	4	6	4	4	6,760	2,096
Мережева інфраструктура	DDoS	2	1	1	0,083	3	1	0,250	2	1	3	0,111	3	2	2	0,300	5	3	3	1,800	0,071	3	2	3	0,417	7	8	7	8	1,851	0,388
	Спуфінг	4	3	3	0,583	4	3	0,625	4	3	5	0,333	2	3	3	0,450	3	4	3	4,000	0,159	3	2	3	0,417	8	5	6	6	3,143	1,277
	Сніфінг	3	2	2	0,333	5	2	0,625	2	2	3	0,148	3	2	3	0,375	2	4	4	8,000	0,319	3	3	3	0,500	8	6	5	5	3,679	1,333
	Man-in-the-Middle	4	3	2	0,500	4	3	0,625	5	2	4	0,296	2	3	3	0,450	4	4	3	3,000	0,119	4	4	2	0,583	7	4	5	5	4,873	1,962
Хмарні сервіси та ресурси	DDoS	1	2	1	0,083	3	1	0,250	2	1	2	0,074	2	2	2	0,250	5	3	3	1,800	0,071	2	3	2	0,333	7	9	8	8	1,617	0,288
	Витік даних	4	2	4	0,583	2	3	0,375	5	6	4	0,444	3	3	1	0,350	10	2	2	0,400	0,015	2	2	3	0,333	9	7	2	7	3,049	1,011
	Злам акаунтів	3	2	3	0,417	2	2	0,250	4	7	4	0,444	3	3	2	0,425	14	2	3	0,429	0,016	2	2	3	0,333	9	5	5	6	3,240	1,043
	Man-in-the-Middle	3	3	4	0,583	4	3	0,625	3	5	4	0,333	2	3	1	0,300	5	3	3	1,800	0,071	3	3	3	0,500	8	8	5	6	2,641	0,924