МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

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

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “СИСТЕМА ОЦІНКИ ТА МІНІМІЗАЦІЇ ЗАГРОЗ ПРИ УПРАВЛІННІ КІБЕРРИЗИКАМИ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

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

_____ Вадим РЯБЦУН
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав(ла): здобувач(ка) вищої освіти гр. УБД-41

Вадим РЯБЦУН
Ім’я, ПРІЗВИЩЕ

Керівник: Юрій Щавінський
к.т.н., доцент Ім’я, ПРІЗВИЩЕ

Рецензент: Юрій ПЕПА
к.т.н., доцент Ім’я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Рябцуну Вадиму Павловичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Система оцінки та мінімізації загроз при управлінні кіберризиками”,
керівник кваліфікаційної роботи ЩАВІНСЬКИЙ Юрій, *к.т.н., доцент*,
(ПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “24“ лютого 2025 р. №56.

2. Строк подання кваліфікаційної роботи “12” травня 2025р.

3. Вихідні дані до кваліфікаційної роботи: *сучасні методи оцінки кіберризиків, аналіз механізмів мінімізації загроз в організаціях, застосування підходів до управління кіберризиками.*

4. Перелік питань, які мають бути розроблені:
4.1. Провести аналіз наукових та нормативних джерел щодо методів оцінки кіберризиків, вразливостей та загроз в інформаційних системах.
4.2. Проаналізувати сучасні стандарти та підходи до управління ризиками (ISO/IEC 27005, NIST SP 800-30, FAIR, OCTAVE).
4.3. Розробити методику оцінки кіберризиків на основі аналізу загроз та побудови матриці ризиків.
4.4. Запропонувати технічні та організаційні заходи для мінімізації кіберризиків, включаючи використання SIEM-систем, політик безпеки та засобів контролю доступу.
4.5. Розробити та протестувати модель управління кіберризиками на тестовому середовищі (віртуальні машини або SOC-лабораторію).

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “5“ березня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкта, предмета, мети та завдань дослідження.	18.03.2025	Виконано
2.	Збір та аналіз літератури.	29.03.2025	Виконано
3.	Аналіз особливостей управління інформаційною безпекою підприємства	08.04.2025	Виконано
4.	Дослідження основних характеристик технологій формування обізнаності й навчання персоналу.	15.04.2025	Виконано
5.	Вивчення інструментів та методів формування обізнаності й навчання персоналу з інформаційної безпеки	22.04.2025	Виконано
6.	Формулювання висновків за результатами проведеного дослідження.	29.04.2025	Виконано
7.	Оформлення роботи.	06.05.2025	Виконано
8.	Оформлення презентації.	09.05.2025	Виконано
9.	Отримання рецензії на роботу.	12.06.2025	Виконано
10.	Захист в ДЕК.	__.06.2025	

Здобувач вищої освіти _____ Вадим РЯБЦУН
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

ПОДАННЯ ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувач Рябцун В.П. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Система оцінки та мінімізації загроз при управлінні кіберризиками"
Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач вищої освіти РЯБЦУН Вадим у кваліфікаційній роботі успішно дослідив сучасні методи оцінки кіберризиків, проаналізував ключові міжнародні стандарти (ISO/IEC 27005, NIST SP 800-30, FAIR, OCTAVE), розглянув класифікацію загроз і вразливостей в інформаційних системах, вивчив програмні інструменти для оцінки та управління ризиками (Nessus, RiskLens, Archer GRC, SIEM-системи). Також у роботі були запропоновані обґрунтовані заходи щодо мінімізації ризиків як технічного, так і організаційного характеру.

РЯБЦУН Вадим продемонстрував глибоке розуміння теоретичних засад теми дослідження, практичну обізнаність із сучасними підходами до управління кіберризиками та здатність до логічного, аналітичного мислення. Робота містить чітку структуру, науково обґрунтовані висновки та прикладну спрямованість.

Здобувач проявив себе як організований, відповідальний, ініціативний виконавець, що здатний самостійно вирішувати складні завдання у сфері інформаційної безпеки. Результати роботи були апробовані на Всеукраїнській науково-практичній конференції «Стратегії кіберстійкості: управління ризиками та безперервність бізнесу» (лютий 2025 року).

Все це дає підстави оцінити кваліфікаційну роботу Рябцуна Вадима на оцінку «відмінно» та рекомендувати його до присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою «Управління інформаційною та кібернетичною безпекою».

Керівник кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Рябцун В.П. допускається до захисту даної роботи в Екзаменаційній комісії.

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

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти Рябцуна Вадима
на тему “Система оцінки та мінімізації загроз при управлінні кіберризиками”

Актуальність. У сучасному цифровому середовищі, де кіберзагрози щоденно еволюціонують, захист інформаційних активів є критично важливим для організацій будь-якого рівня. Управління кіберризиками стало обов’язковою складовою стратегічного планування у сфері інформаційної безпеки. Високий рівень залежності бізнесу від IT-систем та інтернет-інфраструктури вимагає постійного аналізу ризиків, їх моніторингу та впровадження ефективних заходів захисту. У цьому контексті тема дипломної роботи Рябцуна В.П. є вкрай актуальною, оскільки охоплює аналіз методик, інструментів та засобів мінімізації загроз у межах процесів управління кіберризиками, що має велике прикладне значення для фахівців з кібербезпеки.

Позитивні сторони.

У роботі системно досліджено міжнародні підходи до оцінки кіберризиків, зокрема ISO/IEC 27005, NIST SP 800-30, FAIR, OCTAVE . Розглянуто особливості сучасних загроз, вразливостей та способи їх ідентифікації з використанням відповідного інструментарію (Nessus, OpenVAS, RiskLens тощо). Дипломна робота структурована, відповідає встановленим вимогам до оформлення, містить значну кількість рисунків, схем і таблиць, що ілюструють практичну частину. Автором опрацьовано великий обсяг джерел (58 найменувань), включно з актуальними міжнародними нормативами. Запропоновано практичні рекомендації з побудови моделей управління ризиками та мінімізації наслідків інцидентів у реальному середовищі.

Недоліки. До недоліків роботи можна віднести обмежене застосування статистичних методів кількісного аналізу ризиків. Також доцільним було б розширити розділ, присвячений автоматизованим GRC-рішенням, з прикладами їх впровадження на реальних кейсах. Водночас зазначені зауваження мають суто рекомендований характер і не знижують наукової та практичної цінності дослідження.

Висновок: Кваліфікаційна бакалаврська робота Рябцуна В.П. виконана на високому науково-методичному рівні, вирізняється актуальністю, практичною спрямованістю й чіткою логікою викладу матеріалу. Робота заслуговує оцінки «відмінно»**,** а здобувач Вадим Рябцун – присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою «Управління інформаційною та кібернетичною безпекою»**.**

Рецензент: _____ Юрій ПЕПА
к.т.н., доцент *підпис* Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню способів оцінки та мінімізації загроз при управлінні кіберризиками. Робота складається зі вступу, чотирьох розділів, що містять 2 рисунки і 7 таблиць, висновків і списку використаних джерел із 60 найменувань. Загальний обсяг роботи становить 68 аркушів, з яких 4 аркуші займають додатки та список використаних джерел.

Метою роботи є розробка та обґрунтування ефективних способів оцінки кіберризиків та мінімізації загроз в інформаційних системах організацій.

Об'єктом дослідження є процеси управління кіберризиками в інформаційних системах.

Предметом дослідження є методики, моделі та інструменти оцінки кіберризиків, а також заходи їхньої мінімізації.

Методи дослідження. У роботі використано методи системного аналізу, порівняння, моделювання загроз, експертної оцінки, аналізу нормативних стандартів та засоби візуалізації ризиків.

У результаті проаналізовано сучасні методи управління кіберризиками, розглянуто міжнародні стандарти (ISO/IEC 27005, NIST SP 800-30, FAIR), проведено моделювання загроз, оцінено рівень ризиків, запропоновано заходи з їх мінімізації.

Галузь застосування. Розроблені підходи можуть бути використані для впровадження систем управління інформаційною безпекою на підприємствах різних галузей.

Ключові слова: КІБЕРРИЗИКИ, ІНФОРМАЦІЙНА БЕЗПЕКА, ЗАГРОЗИ, ВРАЗЛИВОСТІ, ОЦІНКА РИЗИКІВ, МЕТОДИКИ УПРАВЛІННЯ.

ABSTRACT

The qualification thesis is devoted to the study of methods for assessing and minimizing threats in cyber risk management. The paper consists of an introduction, four chapters, which include 2 figures and 7 tables, conclusions, and a list of 60 references. The total volume of the thesis is 68 pages, including 4 pages of appendices and a list of references.

The aim of the work is to develop and justify effective methods for assessing cyber risks and minimizing threats in organizational information systems.

The object of the study is the processes of cyber risk management in information systems.

The subject of the study is the methodologies, models, and tools for cyber risk assessment, as well as measures for their minimization.

Research methods. The thesis uses methods of system analysis, comparison, threat modeling, expert evaluation, analysis of regulatory standards, and tools for risk visualization.

As a result, modern methods of cyber risk management were analyzed, international standards (ISO/IEC 27005, NIST SP 800-30, FAIR) were reviewed, threat modeling was conducted, risk levels were assessed, and measures for their mitigation were proposed.

Field of application. The proposed approaches can be used to implement information security management systems in enterprises across various industries.

Keywords: CYBER RISKS, INFORMATION SECURITY, THREATS, VULNERABILITIES, RISK ASSESSMENT, MANAGEMENT METHODOLOGIES.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ.....……..… 10

ВСТУП ……..... 12

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ УПРАВЛІННЯ КІБЕРРИЗИКАМИ …….. 14

1.1 Поняття кіберризиків та їх класифікація ……. 14

1.2 Системи та методи оцінки кіберризиків……...…..…….. 17

1.3 Вразливості та загрози в інформаційних системах……... 19

1.4 Огляд стандартів та регламентів щодо управління кіберризиками…… 22

Висновки до розділу 1…….. 24

РОЗДІЛ 2 АНАЛІЗ СИСТЕМ І МЕТОДІВ ОЦІНКИ КІБЕРРИЗИКІВ……. 26

2.1 Огляд сучасних підходів до аналізу кіберризиків…… 26

2.2 Побудова матриці ризиків та оцінка впливу загроз…… 28

2.3 Аналіз інструментів управління кіберризиками…… 31

2.4 Вибір оптимального підходу для оцінки ризиків на прикладі конкретної організації…… 33

Висновки до розділу 2…… 35

РОЗДІЛ 3 МЕТОДИ МІНІМІЗАЦІЇ КІБЕРРИЗИКІВ……..... 37

3.1 Технічні заходи зниження ризиків…… 37

3.2 Організаційні заходи мінімізації загроз…… 39

3.3 Автоматизація процесу управління кіберризиками…… 42

3.4 Оцінка ефективності запропонованих заходів…… 44

Висновки до розділу 3……. 46

РОЗДІЛ 4 ПРАКТИЧНА РЕАЛІЗАЦІЯ СИСТЕМИ ОЦІНКИ УПРАВЛІННЯ КІБЕРРИЗИКАМИ……..… 48

4.1 Впровадження системи оцінки кіберризиків у тестовому середовищі 48

4.2 Моделювання загроз та оцінка впливу атак…… 51

4.3 Використання програмних засобів для виявлення ризиків…… 55

4.4 Аналіз отриманих результатів та розробка рекомендацій…… 58

Висновки до розділу 4…….. 60

ВИСНОВКИ …… 62

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ …… 64

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ІС	Інформаційна система
КР	Кіберризик
ЗІ	Захист інформації
ІБ	Інформаційна безпека
УКР	Управління кіберризиками
ВЗ	Вразливість
З	Загроза
НА	Наслідки атаки
МЗ	Модель загроз
МОКР	Модель оцінки кіберризиків
CIA	Конфіденційність (Confidentiality), цілісність (Integrity), доступність (Availability)
FAIR	Factor Analysis of Information Risk (Факторний аналіз інформаційного ризику)
SIEM	Security Information and Event Management (система управління інформацією та подіями безпеки)
MFA	Multi-Factor Authentication (багатофакторна автентифікація)
GRC	Governance, Risk, and Compliance (управління, ризики та відповідність)
NIST	National Institute of Standards and Technology (Національний інститут стандартів і технологій, США)
ISO/IEC	Міжнародна організація зі стандартизації / Міжнародна електротехнічна комісія
SOC	Security Operations Center (центр реагування на інциденти безпеки)
XSS	Cross-Site Scripting (міжсайтове скриптування)
SQLi	SQL Injection (SQL-ін'єкція)

MITM	Man-in-the-Middle (атака "людина посередині")
CVSS	Common Vulnerability Scoring System (загальна система оцінювання вразливостей)
GDPR	General Data Protection Regulation (Загальний регламент захисту даних
DOS/DDOS	Denial of Service / Distributed Denial of Service (відмова в обслуговуванні / розподілена атака)
AV	Антивірусне програмне забезпечення
IDS/IPS	Intrusion Detection / Prevention System (система виявлення / запобігання вторгненням)
ZERO TRUST	Концепція повної недовіри до будь-яких елементів мережі
VAPT	Vulnerability Assessment and Penetration Testing (оцінювання вразливостей і тестування на проникнення)
CERT-UA	Комп’ютерна команда реагування на надзвичайні події України

ВСТУП

Актуальність теми. У сучасному цифровому середовищі інформаційні системи організацій стають ключовим елементом їхньої діяльності, а отже – об’єктом численних кіберзагроз. Кібератаки набувають дедалі складнішого характеру, змінюються їхні сценарії, масштаби й цілі. Порушення конфіденційності, цілісності або доступності даних може спричинити суттєві фінансові втрати, підрив репутації, правові наслідки та навіть зупинку критичних бізнес-процесів.

У зв’язку з цим зростає потреба у впровадженні ефективних систем управління кіберризиками, здатних виявляти, оцінювати та мінімізувати загрози в інформаційному просторі. Застосування сучасних методик аналізу ризиків, таких як побудова матриць ризиків, дерево атак, методологія FAIR, стандарти ISO/IEC 27005, NIST SP 800-30 тощо, дозволяє організаціям забезпечити проактивне управління безпекою на основі даних та обґрунтованих рішень.

Таким чином, дослідження методів оцінки кіберризиків та розробка заходів щодо їх мінімізації є актуальним науковим і практичним завданням у сфері інформаційної безпеки.

Метою дослідження є розробка та обґрунтування ефективних методів оцінки кіберризиків та мінімізації загроз у процесі управління інформаційною безпекою організації.

Для досягнення мети в роботі поставлено такі ***завдання***:

1. Проаналізувати сучасні підходи до управління кіберризиками на підприємстві.
2. Вивчити стандарти, моделі та методики оцінки ризиків, що застосовуються в сфері інформаційної безпеки.
3. Провести моделювання загроз для типових ІТ-систем з використанням практичних інструментів.

4. Оцінити рівень ризиків та розробити рекомендації щодо їхнього зниження.
5. Обґрунтувати вибір методів та засобів мінімізації ризиків для організації.

Об'єктом дослідження є процеси управління кіберризиками в інформаційних системах організацій.

Предметом дослідження є методики, моделі та інструменти оцінки кіберризиків, а також заходи їхньої мінімізації в системах управління інформаційною безпекою.

Методи дослідження. У роботі застосовано методи системного аналізу, порівняльного аналізу нормативних документів і стандартів, метод експертної оцінки, методи побудови моделей загроз та ризик-орієнтованого управління, а також програмні засоби для візуалізації й аналізу ризиків.

Практичне значення одержаних результатів. Результати роботи можуть бути використані для впровадження ефективної системи управління кіберризиками на підприємствах різних галузей. Запропоновані методи дозволяють обґрунтовано і системно оцінювати рівень загроз, вживати запобіжних заходів та знижувати ймовірність успішного здійснення кібератак.

Апробація результатів дипломної роботи були представлені на Всеукраїнській науково-практичній конференції «Стратегії кіберстійкості: управління ризиками та безперервність бізнесу», що відбулася 27 лютого 2025 року.

Розділ 1 ТЕОРЕТИЧНІ ОСНОВИ УПРАВЛІННЯ КІБЕРРИЗИКАМИ

1.1 Поняття кіберризиків та їх класифікація

В умовах глобальної цифровізації, коли інформація стала стратегічним ресурсом, питання кібербезпеки набуває критичного значення для діяльності будь-якої організації. Залежність від інформаційних систем і цифрової інфраструктури створює нові вектори атак і підвищує рівень вразливості до кіберзагроз. Саме в такому контексті виникає необхідність чіткого розуміння й обґрунтованого управління кіберризиками, які є центральним елементом сучасної парадигми інформаційної безпеки [2].

Кіберризик (англ. *cyber risk*) – це імовірність настання кіберінциденту, який здатен завдати шкоди інформаційним активам організації, спричинити порушення бізнес-процесів, призвести до фінансових, репутаційних або правових втрат. Згідно з ISO/IEC 27005:2022, кіберризик визначається як ефект невизначеності на інформаційні активи, що може вплинути на досягнення цілей організації у сфері безпеки. У практичному сенсі кіберризик є наслідком дії загроз, які реалізуються через вразливості у системах і процесах.

Сучасне розуміння кіберризику базується на інтеграції кількох ключових елементів: інформаційних активів, що потребують захисту; загроз**,** які потенційно можуть завдати шкоди; вразливостей**,** що створюють можливість реалізації загроз; ймовірності інциденту; та можливих наслідків. Формально це можна виразити такою формулою (1.1) [5]:

$$\textit{Кіберризик} = \textit{Загроза} \times \textit{Вразливість} \times \textit{Цінність активу} \times \textit{Ймовірність інциденту} \times \textit{Масштаб наслідків} \quad (1.1)$$

Загроза (threat) – це будь-який потенційний фактор, внутрішній чи зовнішній, здатний реалізувати небажаний вплив на інформаційну систему. Вразливість (vulnerability) – слабке місце в системі, яке може бути використане

для реалізації загрози. Інформаційні активи (інформація, бази даних, сервіси, інфраструктура) – об’єкти, що мають цінність для організації й повинні бути захищеними. Таким чином, ризик існує лише у випадку одночасної наявності загрози, вразливості та активу, що має цінність.

У системі управління ризиками класифікація кіберризиків має важливе значення, адже дозволяє структурувати об’єкти захисту, розподіляти ресурси, визначати пріоритети реагування й обирати релевантні контрзаходи.

Найпоширеніші критерії класифікації включають:

1. За джерелом загроз:
   - зовнішні загрози: включають атаки хакерів, зловмисні ПЗ (ransomware, spyware, трояни), DDoS-атаки, фішингові кампанії, втручання з боку конкурентів або державних акторів;
   - внутрішні загрози**:** пов’язані з працівниками або партнерами, які мають доступ до систем (інсайдерські атаки, службова недбалість, витік інформації через помилки користувачів).
2. За характером впливу [4]:
   - Фінансові ризики: безпосередні грошові збитки, витрати на усунення наслідків, штрафи за порушення законодавства.
   - Операційні ризики: вплив на працездатність інформаційних систем, порушення бізнес-процесів.
   - Юридичні ризики**:** пов’язані з невиконанням вимог нормативних документів (наприклад, GDPR, ISO/IEC 27001, Закон України «Про захист персональних даних»).
   - Репутаційні ризики**:** втрата довіри з боку клієнтів, партнерів, падіння ринкової вартості компанії.
3. За технічною природою:
   - Мережеві загрози: атаки типу MITM (man-in-the-middle), перехоплення трафіку, сканування портів, перехоплення DNS-запитів.

- Програмні вразливості**:** SQL-ін’єкції, XSS, вразливості у веб-додатках, переповнення буфера, нульові дні.
- Соціотехнічні атаки**:** фішинг, спуфінг, використання маніпулятивних технік для отримання конфіденційної інформації від співробітників.

4. За критичністю:

- Низький рівень ризику: незначний вплив, малоймовірна реалізація (наприклад, витік технічної інформації з обмеженим рівнем чутливості).
- Середній рівень ризику: помірна ймовірність інциденту, здатного частково вивести з ладу системи.
- Високий рівень ризику: висока ймовірність серйозного інциденту (наприклад, шифрування всієї бази клієнтів, втрата резервних копій, зупинка CRM або ERP-систем).

Відповідно до рекомендацій ISO/IEC 27005**,** управління ризиками повинно охоплювати такі етапи: встановлення контексту, ідентифікація активів і загроз, оцінка вразливостей, визначення рівня ризику, вибір та впровадження заходів управління ризиками, моніторинг та перегляд. Практика передбачає створення реєстру ризиків**,** матриці ризиків**,** формування профілів ризику для критичних активів, а також оцінку залишкового ризику після застосування заходів контролю.

Крім того, у межах корпоративного управління все більше застосовуються GRC-системи (Governance, Risk, Compliance)**,** які дозволяють автоматизувати процеси обліку ризиків, формування політик, аудитів і перевірок відповідності стандартам. У таких системах часто реалізовані модулі побудови heat maps**,** dashboard-аналітикита інтеграція з SIEM-сервісами для обробки подій у реальному часі.

У результаті слід підкреслити, що класифікація кіберризиків – це не лише формальність, а необхідна умова для побудови ефективної системи кіберзахисту. Вона дозволяє відстежувати динаміку ризиків, прогнозувати нові

загрози, планувати бюджети безпеки й оперативно приймати обґрунтовані рішення. Саме тому всебічне розуміння природи кіберризику є ключем до стійкості організації в умовах зростаючого тиску з боку кіберзагроз.

1.2 Системи та методи оцінки кіберризиків

Ефективне управління кіберризиками базується на здатності точно й обґрунтовано ідентифікувати, оцінювати та прогнозувати потенційні загрози, вразливості та їхній вплив на критичні активи. Зважаючи на складність інформаційного середовища, різноманітність архітектур систем і постійно змінюваний ландшафт загроз, процес оцінки кіберризиків потребує використання стандартизованих, адаптивних і, водночас, практично застосовних методик. У міжнародній практиці найбільш поширеними є: ISO/IEC 27005**,** NIST SP 800-30**,** FAIR (Factor Analysis of Information Risk) **та** OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)**.**

Міжнародний стандарт ISO/IEC 27005 є невід'ємною частиною серії стандартів ISO/IEC 27000, орієнтованих на створення, впровадження й підтримку системи управління інформаційною безпекою (СУІБ). ISO/IEC 27005 визначає загальний підхід до управління ризиками, включаючи: встановлення контексту, ідентифікацію активів, вразливостей, загроз, оцінку ймовірності інцидентів і їх наслідків, визначення рівня ризику та розробку відповідних заходів. Особливістю стандарту є його гнучкість – він не нав’язує конкретної математичної моделі, дозволяючи адаптувати методику до внутрішніх процесів організації. ISO/IEC 27005 підтримує як якісний (через шкали, експертні оцінки), так і кількісний (з використанням числових значень, розрахунків і моделювання) підхід до оцінювання. Це робить його придатним для широкого спектра організацій – від державного сектору до приватного бізнесу[3].

Методика NIST SP 800-30, розроблена Національним інститутом стандартів і технологій США (National Institute of Standards and Technology), є

частиною Risk Management Framework (RMF), що використовується в системах критичної інфраструктури, оборони, охорони здоров'я та фінансів. Методологія NIST побудована на чітко визначених етапах, зокрема: ідентифікація активів, виявлення загроз і вразливостей, оцінка ймовірності реалізації інцидентів, визначення впливу на бізнес-функції, побудова матриці ризиків (Risk Matrix), документування сценаріїв атак.

Метод рекомендує використовувати багаторівневі шкали оцінки впливу (низький, середній, високий) і ймовірності, що дає змогу проводити напівкількісний аналіз, зручний для візуалізації та пріоритизації заходів безпеки. NIST SP 800-30 також передбачає циклічність процесу, що дозволяє підтримувати актуальність ризикового профілю системи при кожній зміні конфігурації або архітектури.

Метод FAIR (Factor Analysis of Information Risk) вирізняється серед інших своєю кількісною природою та орієнтацією на фінансову оцінку ризику. Він базується на аналізі частоти загроз, ймовірності реалізації атаки, вартості впливу та можливих наслідків у грошовому еквіваленті. Наприклад, модель дозволяє оцінити: яку суму організація може втратити у випадку успішної фішингової атаки або скільки коштуватиме порушення конфіденційності персональних даних. FAIR активно використовується у великих корпораціях (наприклад, банках, страхових компаніях), де потрібні точні розрахунки для обґрунтування бюджету на інформаційну безпеку. Метод реалізований у таких ПЗ, як RiskLens, яке дозволяє будувати графіки ризику, оцінювати сценарії за допомогою діаграм Монте-Карло, обраховувати статистичні діапазони збитків, оцінювати запас ризику та ефективність впроваджених заходів[4].

Метод OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) був розроблений в університеті Карнегі-Меллон і націлений на стратегічну оцінку кіберризиків, з акцентом на участь внутрішніх користувачів, а не лише технічних фахівців. OCTAVE пропонує триетапну структуру: перший – створення профілю організації, визначення ключових активів і процесів; другий – виявлення інфраструктурних вразливостей і

потенційних загроз; третій – формування пріоритетів і стратегії реагування. Методика не вимагає використання складних технічних засобів і добре підходить для малих і середніх підприємств**,** які мають обмежені ресурси, але потребують розуміння своєї кіберстійкості. Крім того, OCTAVE може бути використана як частина внутрішнього аудиту безпеки, з акцентом на людський фактор, організаційну культуру та політики.

Порівняльний аналіз наведених методів показує, що ISO/IEC 27005 та NIST SP 800-30 найбільш ефективні у великих організаціях з розгалуженою IT-інфраструктурою, які мають відповідні ресурси для глибокої системної оцінки ризиків. FAIR є ідеальним вибором для організацій, що прагнуть визначити ризик у фінансових термінах для обґрунтування бюджетів безпеки та прийняття стратегічних рішень. OCTAVE забезпечує легкість впровадження і зручний підхід до самодіагностики в умовах обмежених ресурсів.

Вибір конкретної методики оцінки кіберризиків залежить від масштабів організації, галузі діяльності, рівня ризик-орієнтованого мислення персоналу, наявності внутрішніх ресурсів, регуляторних вимог і цілей безпеки. Найкращою практикою є поєднання кількох методів, що дозволяє забезпечити повноту аналізу та об’єктивність рішень у сфері інформаційної безпеки.

1.3 Вразливості та загрози в інформаційних системах

Інформаційні системи будь-якої сучасної організації постійно зазнають впливу як внутрішніх, так і зовнішніх факторів, що можуть поставити під загрозу їхню безперебійну роботу, конфіденційність даних, цілісність бізнес-процесів та довіру користувачів. В умовах цифрової трансформації саме поняття безпеки переходить у площину проактивного аналізу ризиків, серед яких ключову роль відіграють вразливості та загрози.

Вразливість в інформаційній безпеці – це слабке місце або недолік в архітектурі, налаштуваннях або процесах функціонування інформаційної

системи, що може бути використане зловмисником для реалізації атаки. Вразливості можуть виникати внаслідок технічних помилок, неправильного адміністрування, відсутності оновлень безпеки, відкритих мережевих портів, недосконалих алгоритмів автентифікації або через людський фактор. У багатьох випадках навіть найсучасніша IT-інфраструктура може бути скомпрометована через елементарне нехтування політиками безпеки, наприклад, використанням однакових паролів, відсутністю шифрування на робочих станціях або зберіганням конфіденційної інформації у відкритому доступі.

З метою систематизації відомих вразливостей у світі широко використовуються міжнародні стандарти класифікації, зокрема база даних CVE (Common Vulnerabilities and Exposures), яка надає унікальні ідентифікатори для кожної знайденої вразливості. Додатково до неї функціонує NVD (National Vulnerability Database), що розширює інформацію про CVE, включаючи технічні деталі, оцінку ризику та механізми захисту. Оцінювання критичності вразливостей зазвичай здійснюється за допомогою шкали CVSS (Common Vulnerability Scoring System), яка враховує рівень доступності, складність атаки, вплив на конфіденційність, цілісність і доступність системи. CVSS дозволяє класифікувати вразливості за балами від 0 до 10, де показник понад 7,0 вважається високим або критичним.

Загроза, у свою чергу, є потенційною подією або дією, яка може спричинити шкоду системі, скориставшись наявними вразливостями. Загрози можуть мати природне, техногенне або антропогенне походження. До природних загроз належать стихійні лиха (повені, пожежі, землетруси), що можуть пошкодити апаратні ресурси або порушити мережеву інфраструктуру. До техногенних загроз відносять збої в енергопостачанні, перегрів серверів, фізичне пошкодження обладнання. Найбільше занепокоєння, однак, викликають антропогенні – навмисні або ненавмисні дії людини: кібератаки, витоки даних, внутрішні порушення безпеки або фішингові кампанії.

Класифікація загроз у кіберсфері охоплює кілька основних груп. Перша – це шкідливе програмне забезпечення, включаючи комп'ютерні віруси, троянські програми, шпигунське ПЗ (spyware), програми-здирники (ransomware), хробаки (worms) і rootkits. Друга група – це атаки на мережеву інфраструктуру, зокрема DoS/DDoS-атаки, перехоплення трафіку, атаки типу Man-in-the-Middle (MITM), DNS-spoofing, підміна MAC-адрес, експлуатація відкритих портів або вразливих служб. До третьої групи належить експлуатація вразливостей веб-додатків, включаючи SQL-ін'єкції, XSS (Cross-Site Scripting), CSRF (Cross-Site Request Forgery), directory traversal та інші[27-29].

Окрему загрозу становить соціальна інженерія – набір технік, спрямованих на маніпуляцію людьми з метою отримання доступу до конфіденційної інформації. Фішинг, вішинг, смишинг, підробка листів від керівництва (business email compromise) – все це методи, що залежать не від технічної уразливості, а від психологічної вразливості персоналу.

Варто наголосити, що одним із найнебезпечніших видів загроз є внутрішні загрози – дії або бездіяльність працівників, які мають законний доступ до систем, але з певних причин стають джерелом ризику. Вони можуть діяти навмисно (шпигунство, саботаж, витік даних) або ненавмисно (випадкове видалення даних, запуск заражених програм).

Для виявлення вразливостей та оцінки рівня загроз використовуються спеціалізовані інструменти: сканери типу Nessus**,** OpenVAS**,** Qualys аналізують системи на предмет наявності відомих вразливостей. SIEM-системи (наприклад, IBM QRadar, Splunk, AlienVault OSSIM) здійснюють моніторинг подій у режимі реального часу, фіксують аномалії, корелюють події між собою та формують індикатори компрометації (IoC). Інтеграція цих інструментів у загальну стратегію управління ризиками дозволяє не лише виявляти, а й прогнозувати потенційні інциденти.

Узагальнюючи, можна зазначити, що вразливості та загрози є двома взаємопов'язаними компонентами моделі ризику. Виявлення, класифікація та усунення вразливостей, а також ідентифікація й нейтралізація загроз мають

бути системним процесом, інтегрованим у загальну політику інформаційної безпеки організації. Тільки за умови регулярного моніторингу та аналізу вразливостей, оцінки загроз і своєчасного реагування можна досягти ефективного контролю над ризиками в інформаційних системах.

1.4 Огляд стандартів та регламентів щодо управління кіберризиками

Ефективне управління кіберризиками передбачає дотримання відповідних міжнародних стандартів і регламентів, які встановлюють вимоги до захисту інформаційних активів, організаційних процесів і технічних засобів безпеки. Сучасна практика управління інформаційною безпекою базується на гармонізації підходів, які були розроблені міжнародними організаціями та регуляторами, зокрема ISO, NIST, Європейською Комісією та іншими. У цьому контексті особливу увагу слід приділити трьом ключовим документам: ISO/IEC 27001**,** NIST Cybersecurity Framework (CSF) **та** Регламенту ЄС про захист персональних даних (GDPR)**.**

ISO/IEC 27001 є міжнародним стандартом, який визначає вимоги до створення, впровадження, функціонування, моніторингу, перегляду, підтримання та покращення системи управління інформаційною безпекою (СУІБ). Цей стандарт орієнтований на ризик-орієнтований підхід і базується на циклі PDCA (Plan-Do-Check-Act). Основними компонентами ISO 27001 є: аналіз контексту організації, виявлення зацікавлених сторін, оцінка ризиків, визначення заходів контролю та політик безпеки, постійне покращення системи. У Додатку А ISO/IEC 27001 міститься перелік із 93 засобів контролю, згрупованих за тематиками, що охоплюють управління активами, контроль доступу, шифрування, захист від шкідливого ПЗ, реагування на інциденти тощо. Організації, які впровадили ISO 27001, демонструють високий рівень зрілості управління ризиками, що часто є передумовою для партнерських контрактів і аудиту.

NIST Cybersecurity Framework (CSF) був розроблений Національним інститутом стандартів і технологій США для критичної інфраструктури, але згодом отримав широке застосування в комерційному секторі. Він ґрунтується на п’яти функціональних доменах: Identify (Ідентифікація), Protect (Захист), Detect (Виявлення), Respond (Реагування), Recover (Відновлення)**.** Фреймворк не є сертифікаційним стандартом, а радше методологічним інструментом, що дозволяє організаціям оцінити рівень своєї кіберстійкості, виявити прогалини в захисті та сформувати дорожню карту розвитку системи безпеки. Особливо цінним у NIST CSF є поєднання технічних і організаційних вимог, акцент на безперервний моніторинг та адаптивне управління ризиками, що дозволяє враховувати динаміку змін у цифровому середовищі[23-26].

Регламент (ЄС) 2016/679 – Загальний регламент про захист даних (GDPR) встановлює правову основу захисту персональних даних громадян Європейського Союзу. Хоча GDPR не є стандартом інформаційної безпеки в традиційному сенсі, його виконання тісно пов’язане з процесом управління кіберризиками, особливо щодо захисту конфіденційності, прозорості обробки даних та реагування на витоки. Статті 32–34 Регламенту зобов’язують організації впроваджувати «відповідні технічні та організаційні заходи», включаючи шифрування, псевдонімізацію, регулярне тестування безпеки систем, а також забезпечувати інформування регуляторів та суб’єктів даних у разі інциденту. Невиконання вимог GDPR може призвести до значних штрафів – до 20 мільйонів євро або 4% річного обороту компанії.

Узгоджене застосування ISO 27001, NIST CSF та GDPR дозволяє побудувати комплексну систему управління кіберризиками, яка відповідає як технічним вимогам, так і правовим нормам. У практиці багатьох міжнародних компаній саме інтеграція цих документів є запорукою ефективного кіберзахисту, відповідності вимогам регуляторів та зниження рівня кіберризиків до прийнятного рівня.

Висновок до розділу 1

У першому розділі дипломної роботи було досліджено теоретичні засади управління кіберризиками, що є ключовим елементом сучасної системи інформаційної безпеки. Аналіз понять, класифікацій та методів оцінки кіберризиків дозволив сформувати цілісне розуміння їх природи, джерел походження та механізмів впливу на інформаційні системи організацій.

Зокрема, встановлено, що кіберризик є багатовимірним поняттям, що поєднує технічні, організаційні та людські чинники, а його реалізація можлива лише за наявності уразливості, загрози та значущого інформаційного активу. Наведена класифікація ризиків за джерелом, типом впливу, технічною природою та критичністю є основою для структурованого аналізу та прийняття управлінських рішень.

Огляд методик оцінювання кіберризиків (ISO/IEC 27005, NIST SP 800-30, FAIR, OCTAVE) продемонстрував, що ефективне управління ризиками вимагає адаптації підходу до особливостей організації. Залежно від рівня зрілості, наявних ресурсів і стратегічних цілей, організація може використовувати як якісні, так і кількісні методи для пріоритезації ризиків та вибору відповідних заходів реагування[11].

Особливу увагу було приділено аналізу вразливостей та загроз, які становлять основу будь-якої моделі ризику. Було показано, що ефективна ідентифікація, класифікація та усунення вразливостей, а також моніторинг загроз є ключовими умовами забезпечення кіберстійкості організації.

Нарешті, розгляд міжнародних стандартів і регламентів (ISO/IEC 27001, NIST CSF, GDPR) дозволив зрозуміти важливість нормативного підґрунтя для побудови системи управління кіберризиками. Їх дотримання не лише забезпечує відповідність вимогам регуляторів, а й підвищує довіру з боку клієнтів, партнерів та інвесторів.

Розділ створює теоретичну базу для подальшого практичного аналізу кіберризиків та розробки рекомендацій щодо їх ефективного управління в конкретному організаційному середовищі.

Розділ 2 АНАЛІЗ СИСТЕМ І МЕТОДІВ ОЦІНКИ КІБЕРРИЗИКІВ

2.1 Огляд сучасних підходів до аналізу кіберризиків

У контексті стрімкого розвитку цифрових технологій, зростання обсягу критичної інформації та підвищення складності інформаційних систем, завдання ефективного аналізу кіберризиків постає як ключове для забезпечення стабільної роботи будь-якої організації. У відповідь на ці виклики сформувалася низка сучасних підходів до аналізу ризиків, які базуються на міжнародних стандартах, нормативних моделях і практичних інструментах. Метою цих підходів є виявлення, вимірювання та пріоритизація ризиків, а також забезпечення управлінських рішень щодо їх зниження.

Сучасні методи аналізу кіберризиків умовно поділяються на якісні, кількісні та комбіновані**.** Якісні методи ґрунтуються на експертному оцінюванні рівня ризиків із використанням шкал і матриць, що дозволяє визначити пріоритетність загроз, не вдаючись до складних обчислень. Кількісні методи, навпаки, передбачають математичне моделювання, аналіз ймовірностей, використання статистичних даних та прогнозів збитків, що дає змогу обґрунтовано оцінити потенційний економічний вплив інцидентів. Комбіновані методи поєднують обидва підходи, зокрема у випадках, коли частина параметрів може бути визначена об'єктивно, а частина – лише експертно.

Серед найпоширеніших підходів слід виокремити ISO/IEC 27005**,** який підтримує реалізацію системи управління інформаційною безпекою згідно з ISO/IEC 27001. Він забезпечує детальну структуру процесу оцінки ризиків, включаючи ідентифікацію активів, загроз, вразливостей, визначення ймовірностей та наслідків. ISO 27005 не диктує конкретний алгоритм обчислення ризиків, залишаючи організації право самостійно обирати спосіб оцінювання – якісний чи кількісний[21-22].

Іншим впливовим підходом є NIST SP 800-30**,** який пропонує структуровану модель для виявлення загроз, оцінки вразливостей та аналізу

їхнього впливу на активи. Цей підхід широко використовується у державному секторі США, але завдяки своїй гнучкості він добре інтегрується і в приватних організаціях. NIST 800-30 підтримує формування сценаріїв ризиків, побудову матриць загроза–вразливість–наслідок та формування профілів ризиків для обґрунтування захисних заходів[10].

Особливої уваги заслуговує FAIR (Factor Analysis of Information Risk) – кількісний підхід, що дозволяє обрахувати ризик у грошовому еквіваленті. На відміну від традиційних шкал і кольорових матриць, FAIR розкладає ризик на фактори, що піддаються математичному аналізу: частота подій, ймовірність успішної атаки, потенційна шкода. Методика набуває популярності у великих компаніях, зокрема у фінансовому секторі, де необхідне обґрунтоване прийняття рішень на основі точних оцінок.

Ще один підхід – OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) – орієнтований на внутрішню самооцінку ризиків організацією. Він передбачає участь персоналу в ідентифікації критичних активів і загроз, визначення вразливих зон та пріоритизацію заходів. Метод особливо підходить для організацій, які не мають розвиненої технічної інфраструктури, але потребують систематизації знань і підвищення рівня обізнаності з питань безпеки.

З-поміж практичних інструментів для аналізу ризиків широко використовуються матриці ризиків**,** що поєднують ймовірність настання події з рівнем її впливу. Вони можуть бути побудовані як вручну в Excel, так і за допомогою спеціалізованого ПЗ. Також варто згадати використання аналізу CVSS-метрик**,** які дозволяють оцінити рівень загрози вразливості на основі загальновизнаних критеріїв.

Слід зазначити, що сучасні підходи до аналізу кіберризиків дозволяють адаптувати моделі оцінювання до специфіки організації, її розміру, галузі, технічної інфраструктури та культури безпеки. Ефективна реалізація аналізу ризиків потребує не лише вибору правильного методу, але й створення

організаційних передумов: призначення відповідальних осіб, створення політик безпеки, регулярного аудиту та залучення кваліфікованих фахівців.

2.2 Побудова матриці ризиків та оцінка впливу загроз

Процес оцінки кіберризиків є одним із фундаментальних етапів у системі управління інформаційною безпекою, адже саме він дозволяє визначити потенційні загрози, їх ймовірність та вплив на критичні активи організації. Одним із найбільш наочних і ефективних інструментів для цього є матриця ризиків – візуальна модель, яка поєднує два ключові параметри: ймовірність виникнення загрози та ступінь її впливу на діяльність організації.

Побудова матриці ризиків починається з ідентифікації активів, які мають критичне значення для організації. До таких активів належать як матеріальні ресурси (сервери, комп'ютери, мережеве обладнання), так і нематеріальні (інформація, програмне забезпечення, облікові записи доступу, репутація тощо). Після цього проводиться аналіз загроз**,** тобто подій або дій, які можуть негативно вплинути на зазначені активи. Загрози можуть бути як внутрішніми (недбалість співробітників, помилки адміністрування, внутрішній саботаж), так і зовнішніми(кібератаки, віруси, фішинг, DDoS-атаки, стихійні лиха тощо).

Наступним кроком є виявлення вразливостей – слабких місць у системі безпеки, які можуть бути використані для реалізації загроз. До прикладу, відсутність шифрування передавання даних, використання простих паролів, незахищені порти або недостатній рівень обізнаності персоналу з питань кібербезпеки. Взаємозв'язок між активами, загрозами і вразливостями дозволяє сформувати набір потенційних кіберризиків**,** які підлягають оцінюванню.

Оцінка ризику здійснюється шляхом аналізу двох основних характеристик:

1. Ймовірність реалізації загрози – визначає, наскільки часто або з якою вірогідністю може статися той чи інший інцидент (наприклад, 1 – рідко, 5 – дуже ймовірно).

2. Рівень впливу (наслідків) – відображає масштаб можливих збитків, що можуть бути спричинені реалізацією загрози (наприклад, 1 – незначний вплив, 5 – катастрофічний).

Рівень ризику розраховується за формулою:

$$Ризик = Ймовірність \times Вплив \quad (2.1)$$

На основі отриманих оцінок будується матриця ризиків**,** яка є двовимірною таблицею, де по горизонталі відкладається ймовірність, а по вертикалі – ступінь впливу, дивитись табл.2.1. Такий підхід дозволяє легко інтерпретувати результати та визначити, які ризики потребують негайного втручання, а які можна контролювати на базовому рівні.

Таблиця 2.1.

Двовимірна таблиця ймовірності та впливу

	Вплив: 1 (низький)	**2**	**3**	**4**	**5 (критичний)**
Ймовірність: 5 (висока)	середній	середній	високий	критичний	критичний
4	середній	середній	високий	високий	критичний
3	низький	середній	середній	високий	високий
2	низький	низький	середній	середній	високий
1 (низька)	низький	низький	низький	середній	середній

Матриця ризиків дає змогу ефективно пріоритизувати ресурси на захист тих активів, які мають найвищий ступінь загрози. Наприклад, якщо в результаті аналізу виявлено ризик втрати конфіденційних даних через фішинг (з ймовірністю 4 і впливом 5), такий ризик класифікується як критичний (рівень 20) і потребує негайного вжиття заходів: впровадження багатофакторної аутентифікації, навчання персоналу, налаштування спам-фільтрів.

Окрім загального підрахунку, у практиці оцінювання кіберризиків часто застосовують типові шкали оцінювання**,** що дозволяють стандартизувати процес:

1. Ймовірність**:**
    - 1 – малоймовірно (раз на 10 років)
    - 2 – маловірогідно (раз на 5 років)
    - 3 – можливо (раз на рік)
    - 4 – ймовірно (кілька разів на рік)
    - 5 – дуже ймовірно (щомісяця і частіше)
2. Вплив**:**
    - 1 – незначні збої без втрат
    - 2 – незначні фінансові або тимчасові втрати
    - 3 – помітні втрати або порушення процесів
    - 4 – значні втрати, потреба у відновленні
    - 5 – катастрофічні наслідки (втрата репутації, великі збитки, правові санкції)

Такий підхід є адаптивним і може змінюватися в залежності від галузі, масштабу організації, рівня цифрової зрілості та загрозового ландшафту.

Слід зазначити, що матриця ризиків – це не одноразовий документ, а динамічний інструмент, який має регулярно оновлюватися у відповідь на появу нових загроз, зміну IT-інфраструктури, запуск нових проєктів або зміну регуляторних вимог. Постійне оновлення забезпечує актуальність управлінських рішень та дозволяє зберігати високий рівень кіберстійкості організації.

Узагальнюючи, можна зробити висновок, що побудова матриці ризиків є критично важливим етапом процесу управління кібербезпекою. Вона забезпечує структурований, наочний та ефективний спосіб оцінки загроз, виявлення вразливостей та прийняття рішень щодо заходів захисту. У поєднанні з іншими методами, такими як CVSS, аналіз сценаріїв або фінансова

оцінка збитків, матриця ризиків виступає основою для формування цілісної системи кіберзахисту.

2.3 Аналіз інструментів управління кіберризиками

Сучасне управління кіберризиками передбачає застосування як методологічних підходів, так і програмних інструментів, що дозволяють здійснювати системну і послідовну оцінку ризиків, моніторинг уразливостей, аналіз інцидентів і підтримку прийняття обґрунтованих управлінських рішень. У цьому контексті особливої актуальності набули такі інструменти, як RiskLens, Archer GRC, Open FAIR, а також спеціалізовані засоби виявлення вразливостей – Nessus і OpenVAS.

RiskLens є однією з провідних платформ для кількісного аналізу кіберризиків, яка реалізує методологію Open FAIR (Factor Analysis of Information Risk). Цей інструмент дозволяє здійснювати грошову оцінку ризиків, що надає керівництву можливість приймати рішення на основі фінансових показників потенційних збитків. RiskLens розкладає ризик на окремі фактори – частоту подій, ймовірність реалізації загрози та очікувану шкоду – і на основі цих параметрів моделює сценарії розвитку подій. Платформа інтегрується з іншими корпоративними системами управління, зокрема з базами активів, журналами подій та системами контролю відповідності, що робить її ефективною для використання у великих організаціях, особливо у фінансовому та державному секторах.

Archer GRC (Governance, Risk and Compliance) – це комплексне рішення, яке забезпечує централізоване управління ризиками, політиками безпеки, аудитом та відповідністю до регуляторних вимог. Archer дозволяє організаціям створювати гнучкі моделі оцінки ризиків, поєднуючи якісні та кількісні методи, автоматизувати процеси оцінювання, документування та звітування. Система побудована за модульним принципом, що дає змогу налаштовувати її відповідно до потреб конкретної організації. Archer підтримує міжнародні

стандарти, зокрема ISO/IEC 27001, NIST, COBIT та GDPR, і є одним з найпопулярніших рішень у великих компаніях, які впроваджують стратегічний підхід до управління інформаційною безпекою[40-45].

Методологія Open FAIR, яка використовується у RiskLens і може бути впроваджена окремо, є єдиним міжнародно визнаним стандартом для кількісної оцінки інформаційних ризиків. Вона дозволяє аналізувати ризики за допомогою математичних моделей, оцінюючи частоту виникнення загроз, можливості їх реалізації та потенційні фінансові втрати. На відміну від традиційних якісних методів, які базуються на експертних оцінках і кольорових шкалах, Open FAIR надає інструменти для побудови обґрунтованих фінансових моделей ризику, що особливо важливо для компаній, які орієнтуються на ефективне планування бюджету безпеки.

У свою чергу, інструменти технічного рівня – Nessus і OpenVAS – використовуються для виявлення технічних вразливостей в інформаційних системах. Nessus, розроблений компанією Tenable, є одним із найпоширеніших сканерів вразливостей, який підтримує велику базу CVE-ідентифікаторів, регулярно оновлюється та здатен сканувати мережеві пристрої, сервери, операційні системи та веб-додатки на наявність відомих вразливостей. Nessus дозволяє оцінювати критичність уразливостей за шкалою CVSS, генерувати докладні звіти та допомагає оперативно реагувати на загрози[46-50].

OpenVAS (Open Vulnerability Assessment System) є відкритим аналогом Nessus, який також дозволяє здійснювати повноцінне сканування систем на наявність вразливостей. Він є частиною пакету Greenbone Vulnerability Management і надає можливість безкоштовно проводити тестування безпеки з високим рівнем налаштування. OpenVAS підтримує численні протоколи та сервіси, а його відкрита архітектура дозволяє адаптувати систему під специфіку будь-якого середовища. Завдяки своїй відкритості та гнучкості, OpenVAS широко застосовується в академічних установах, малих підприємствах і дослідницьких організаціях[13].

Загалом, ефективне управління кіберризиками вимагає використання як стратегічних інструментів – таких як RiskLens, Archer або методологія Open FAIR, – так і технічних рішень, як-от Nessus і OpenVAS, що забезпечують глибокий аналіз вразливостей. Поєднання цих підходів дозволяє створити багаторівневу систему захисту, яка охоплює як процеси прийняття управлінських рішень, так і безпосередній технічний контроль безпеки. Успішна реалізація таких інструментів сприяє не лише зниженню рівня ризиків, а й формуванню зрілої культури кібербезпеки в організації[51-52].

2.4 Вибір оптимального підходу для оцінки ризиків на прикладі конкретної організації

Для ефективного управління кіберризиками важливо не лише володіти знаннями про існуючі підходи до їх аналізу, але й вміти обрати найбільш доцільний метод з урахуванням специфіки конкретної організації. В якості прикладу розглянемо умовну компанію ТОВ "ІнфоСервіс", що надає послуги з розробки та підтримки програмного забезпечення для бізнес-клієнтів. Організація має розгалужену IT-інфраструктуру, зокрема внутрішні сервери, хмарні сервіси, системи резервного копіювання, а також зберігає чутливу клієнтську інформацію.

Зважаючи на обсяги інформаційних активів, підвищені вимоги до конфіденційності та потенційні фінансові втрати у разі інцидентів, компанії доцільно застосовувати комбінований підхід до оцінки ризиків, який включає елементи як якісного, так і кількісного аналізу. Зокрема, методологія ISO/IEC 27005 виступає базою для побудови процесу управління ризиками, а як інструмент кількісної оцінки доцільно впровадити Open FAIR, реалізований у платформі RiskLens.

На першому етапі, згідно з ISO/IEC 27005, було здійснено ідентифікацію активів: бази даних клієнтів, корпоративна пошта, вихідний код продуктів, віртуальні сервери, VPN-інфраструктура. Далі проведено виявлення загроз –

зловмисне ПЗ, фішингові атаки, витоки даних, внутрішні порушення політик доступу. Наступним кроком було визначення вразливостей, як-от недостатній контроль доступу, відсутність сегментації мережі, несвоєчасне оновлення ПЗ.

На основі цього було побудовано матрицю ризиків**,** що поєднує ймовірність загрози з потенційним впливом на бізнес. Наприклад, фішингова атака з високою ймовірністю (частота інцидентів раз на місяць) та середнім впливом (можливий доступ до акаунтів користувачів) класифікується як ризик середнього рівня. Водночас компрометація резервної копії, хоч і має меншу ймовірність, але через серйозний вплив класифікується як високий ризик.

Після побудови початкової матриці, з метою кращого обґрунтування інвестицій у заходи захисту, компанія застосувала кількісну оцінку ризиків через Open FAIR. Наприклад, розрахунок ризику витоку клієнтських даних передбачав моделювання частоти загроз (наприклад, 0.1 інцидентів на рік), ймовірності їх реалізації (20%) та потенційних втрат (300 000 грн), що дозволило оцінити очікувану річну шкоду (Annualized Loss Expectancy, ALE) у розмірі близько 6 000 грн. Такі показники допомогли обґрунтувати доцільність інвестування у системи багатофакторної аутентифікації та моніторингу доступів[14-15].

У ролі допоміжних технічних інструментів були використані Nessus та OpenVAS для виявлення технічних вразливостей, що дало змогу виявити низку критичних CVE-ідентифікаторів, пов’язаних з серверними ОС, які не оновлювалися понад 180 днів. Результати сканувань були включені до фінального звіту з оцінки ризиків і стали підставою для формування дорожньої карти покращення безпеки.

У підсумку, оптимальний підхід для ТОВ "ІнфоСервіс" базується на комбінації процесного підходу ISO/IEC 27005, кількісної моделі Open FAIR та технічного контролю через системи виявлення вразливостей. Такий багаторівневий підхід дозволяє не лише якісно описати поточні ризики, але й надати керівництву організації фінансово обґрунтовану картину для прийняття рішень, підвищуючи загальну кіберстійкість компанії.

Висновок до розділу 2

У другому розділі було проведено комплексний аналіз сучасних підходів до оцінки кіберризиків, розглянуто теоретичні засади побудови матриці ризиків, оцінено популярні інструменти управління ризиками та обґрунтовано вибір оптимального підходу для конкретної організації.

Встановлено, що на сьогоднішній день існує широкий спектр методів аналізу кіберризиків – від якісних до кількісних, а також комбінованих. До найвпливовіших стандартів і методик належать ISO/IEC 27005, NIST SP 800-30, FAIR, OCTAVE. Кожен із них має свої переваги залежно від специфіки організації, рівня цифрової зрілості, наявних ресурсів та цілей безпеки. Особливої уваги заслуговує методологія FAIR, яка дозволяє оцінити ризики у грошовому еквіваленті, що значно полегшує прийняття управлінських рішень у бізнес-середовищі.

Побудова матриці ризиків дозволила наочно поєднати ймовірність виникнення загроз та їх вплив на активи. Такий підхід сприяє пріоритизації ризиків і дозволяє сфокусувати ресурси на найкритичніших векторах загроз. Застосування методів експертного оцінювання, шкалювання ризиків та побудова матриці «імовірність – наслідки» довели свою ефективність у практиці.

Окрему увагу було приділено аналізу інструментів, які підтримують процес управління кіберризиками: RiskLens, Archer GRC, Open FAIR Framework – для стратегічного моделювання ризиків, а також сканери вразливостей Nessus та OpenVAS – для тактичного виявлення технічних слабких місць. Їх інтеграція дозволяє забезпечити наскрізний підхід до оцінки ризиків – від політики до технічного захисту[1].

У результаті аналізу визначено, що для обраної організації оптимальним є комбінований підхід із використанням методології FAIR та інструментів

автоматизованої оцінки вразливостей. Це дозволяє врахувати як стратегічні, так і операційні аспекти кібербезпеки, забезпечуючи точну, обґрунтовану й масштабовану оцінку ризиків.

Правильний вибір методів та інструментів аналізу кіберризиків є запорукою ефективної системи інформаційної безпеки. Застосування структурованих, стандартизованих та адаптованих до реалій організації підходів дозволяє своєчасно виявляти, оцінювати та мінімізувати вплив потенційних загроз.

Розділ 3 МЕТОДИ МІНІМІЗАЦІЇ КІБЕРРИЗИКІВ

3.1 Технічні заходи зниження ризиків

У сучасних умовах цифрової трансформації технічні заходи зниження кіберризиків виступають базисом захисту інформаційних ресурсів організацій. Оскільки більшість кібератак реалізується через вразливості в IT-інфраструктурі, недоліки автентифікації, помилки конфігурації або низький рівень моніторингу, критично важливо застосовувати технологічні рішення, які дозволяють виявляти, попереджати та оперативно реагувати на загрози. Одними з ключових інструментів у цій сфері є системи централізованого моніторингу подій безпеки (SIEM), багатофакторна автентифікація, концепція Zero Trust, засоби сегментації мережі, шифрування та контроль доступу.

Системи управління інформаційною безпекою та подіями (SIEM) є одним із найважливіших елементів сучасної кібербезпеки. SIEM-системи дозволяють збирати, зберігати та аналізувати журнали подій з усього середовища – серверів, мережевого обладнання, додатків, хмарних сервісів, антивірусного ПЗ тощо. Основна мета таких систем – виявити аномальну активність або кіберінцидент на ранній стадії. SIEM-платформи використовують кореляційні правила, аналітику поведінки користувачів (UEBA), машинне навчання для виявлення нетипових дій, що можуть вказувати на компрометацію[17-20].

Наприклад, IBM QRadar автоматизує процес виявлення загроз, забезпечує інтелектуальну кореляцію подій і здатен ідентифікувати складні, багатокрокові атаки, які не можуть бути виявлені ізольовано. Платформа Splunk Enterprise Security підтримує масштабовану інфраструктуру аналітики, інтегрує джерела даних із хмарних платформ, інтернету речей (IoT) та промислових систем. AlienVault USM (тепер – AT&T Cybersecurity) надає розширену функціональність за доступною вартістю, поєднуючи SIEM, IDS/IPS, аналіз вразливостей та виявлення активів в одному інтерфейсі. Всі ці рішення

дозволяють істотно знизити ризики, пов’язані з несвоєчасним виявленням атак, інсайдерською активністю або помилками в IT-середовищі.

Водночас, ефективність реагування на загрози прямо залежить від правильності політик контролю доступу до інформаційних ресурсів. Одним із найбільш дієвих інструментів у цій сфері є багатофакторна автентифікація (MFA)**.** Вона ґрунтується на використанні щонайменше двох з трьох факторів: знання (наприклад, пароль), володіння (смартфон, токен) та біометричні характеристики (відбиток пальця, розпізнавання обличчя). MFA істотно ускладнює реалізацію несанкціонованого доступу, навіть у разі компрометації одного з чинників, і особливо ефективна у хмарних середовищах, VPN-з'єднаннях, корпоративних системах CRM/ERP.

Ще одним потужним підходом є архітектура нульової довіри (Zero Trust Architecture)**.** Вона заперечує традиційний принцип "довіри за замовчуванням", який передбачає, що всі користувачі й пристрої всередині периметра мережі є безпечними. Zero Trust натомість вимагає перевірки кожного доступу незалежно від розташування користувача або пристрою. Це досягається шляхом використання динамічної автентифікації, політик мінімального привілею, мікросегментації мережі, постійного моніторингу поведінки та верифікації контексту доступу (час, місце, пристрій, рівень ризику сесії).

У межах Zero Trust, контроль над доступом реалізується не лише через автентифікацію, а й через динамічну авторизацію – перевірку дозволів в режимі реального часу на основі контексту. Такий підхід особливо ефективний у хмарних середовищах, де традиційний мережевий периметр розмитий, а користувачі можуть підключатися з різних пристроїв і географічних розташувань. Впровадження Zero Trust дозволяє значно знизити ризик lateral movement – горизонтального переміщення зловмисника після початкової компрометації[30-34].

Крім того, до технічних засобів мінімізації кіберризиків належать:

1. Мережна сегментація – розділення мережі на ізольовані зони з контролем трафіку між ними. Це зменшує ймовірність поширення атак і

унеможливлює доступ з однієї зони до критичних сервісів без явного дозволу.

2. Шифрування даних – забезпечення конфіденційності інформації під час зберігання (at rest) та передавання (in transit), що дозволяє знизити ризики витоку конфіденційної інформації навіть у разі перехоплення або фізичного доступу до носія[39].
3. Антивірусний та EDR-захист – засоби виявлення, блокування та ліквідації зловмисного ПЗ. Платформи класу EDR (Endpoint Detection and Response) дозволяють здійснювати глибокий аналіз поведінки процесів на кінцевих пристроях, швидко локалізувати та ізолювати заражені вузли.
4. Контроль привілеїв (PAM) – управління доступом адміністративних облікових записів, ведення аудиту їхньої активності, автоматизоване ротація паролів, що дозволяє запобігти ескалації прав з боку зловмисників.

Комплексне застосування цих технічних заходів значно підвищує рівень кіберзахисту організації, дозволяє не лише запобігати атакам, але й формувати проактивну модель безпеки – таку, що спирається на аналіз ризиків, автоматизоване виявлення загроз і гнучке реагування на інциденти. Водночас технічні засоби мають доповнюватися організаційними політиками, навчанням персоналу та регулярним аудитом для забезпечення сталого кіберзахисту.

3.2 Організаційні заходи мінімізації загроз

Організаційні заходи зниження кіберризиків є фундаментальною складовою системи інформаційної безпеки, оскільки саме людський фактор часто стає найслабшою ланкою в захисті інформаційних систем. Жодна технічна система не здатна повністю компенсувати відсутність внутрішньої культури безпеки, чітких регламентів поведінки користувачів та належної організації процесів. Організаційні заходи охоплюють створення нормативно-

регламентної бази, управління поведінкою персоналу, навчання та постійне вдосконалення практик реагування на інциденти.

Одним із ключових організаційних інструментів є **п**олітики інформаційної безпеки**,** що формалізують правила доступу до інформації, порядок обробки та зберігання даних, вимоги до автентифікації, захисту паролів, використання корпоративних ресурсів, роботи з віддаленими підключеннями тощо. Ретельно розроблена політика безпеки повинна бути затверджена керівництвом, охоплювати всі рівні організації – від ІТ-відділу до рядових користувачів – і містити механізми контролю за її дотриманням.

Крім загальної політики, доцільно впроваджувати спеціалізовані внутрішні документи: політику управління інцидентами, політику резервного копіювання, політику контролю змін, політику класифікації даних, політику управління вразливостями. Всі ці документи мають узгоджуватись із міжнародними стандартами (наприклад, ISO/IEC 27001) та регулярно переглядатися з урахуванням змін у технологічному середовищі або законодавчих вимог.

Другим ключовим елементом організаційного захисту є навчання персоналу**.** Більшість інцидентів інформаційної безпеки відбуваються через необережність або незнання співробітників – наприклад, відкриття фішингових листів, встановлення небезпечного ПЗ, слабкі паролі, нехтування процедурами автентифікації. Тому системне підвищення обізнаності співробітників щодо основних загроз, способів їх розпізнавання та правил безпечної поведінки є обов’язковою умовою кіберстійкості організації.

Навчання має охоплювати різні формати – від інструктажів при прийомі на роботу до регулярних семінарів, онлайн-курсів, інтерактивних тестів і тематичних вебінарів. Важливо адаптувати навчальні матеріали до рівня відповідальності працівників: наприклад, ІТ-адміністратори мають проходити поглиблену технічну підготовку, а рядові користувачі – засвоювати основи безпечної роботи в інформаційному середовищі. Доцільним є також

впровадження коротких нагадувань або внутрішніх розсилок із порадами з кібергігієни.

Особливе місце в організаційних заходах посідає проведення кібернавчань та тестів на проникнення (penetration testing)**.** Навчання у форматі симуляції інцидентів – наприклад, фішингових атак, шкідливого ПЗ чи DDoS-кампаній – дозволяє перевірити готовність персоналу до реальних загроз, виявити слабкі місця в поведінці користувачів та налагодити алгоритми реагування. Такі симуляції, відомі як tabletop-експерименти або red team/blue team exercises, є ефективним способом практичного вдосконалення безпекових процесів.

Тести на проникнення, своєю чергою, дозволяють імітувати дії зловмисника з метою перевірки ефективності систем захисту, виявлення вразливостей у мережі, системах автентифікації, вебзастосунках, серверах тощо. Penetration testing проводиться як внутрішніми фахівцями, так і сторонніми експертами (white hat hackers), які здійснюють контрольовану спробу атаки з дотриманням чітко визначених умов і меж. Звіт за результатами тестування дозволяє організації своєчасно усунути недоліки в інфраструктурі й уникнути серйозних наслідків у випадку реального інциденту.

До організаційних заходів також належить управління інцидентами безпеки, яке передбачає наявність чіткого плану дій на випадок атаки: визначення відповідальних осіб, каналів комунікації, сценаріїв реагування, процедур ізоляції уражених систем, відновлення роботи та звітування. Всі ці дії мають бути протестовані на практиці під час навчань та бути знайомими всім учасникам процесу.

Успішна реалізація організаційних заходів зниження ризиків вимагає не лише наявності документів та інструкцій, а й підтримки з боку керівництва, відповідного бюджету на навчання та інфраструктуру, а також системи внутрішнього контролю – зокрема, аудитів, аналізу інцидентів, звітності та постійного вдосконалення заходів безпеки. Такий підхід дозволяє побудувати

культуру безпеки, в якій кожен працівник усвідомлює свою відповідальність і діє відповідно до найкращих практик кіберзахисту.

3.3 Автоматизація процесу управління кіберризиками

У сучасному цифровому середовищі, де обсяги даних зростають експоненційно, а кіберзагрози стають дедалі складнішими й динамічнішими, ефективне управління кіберризиками неможливе без застосування автоматизованих рішень. Автоматизація процесу управління ризиками дозволяє значно підвищити точність, оперативність і масштабованість процедур виявлення, аналізу, моніторингу та реагування на кіберінциденти.

Насамперед, автоматизація дає змогу зменшити вплив людського фактору, мінімізувати ризик помилок під час обробки великої кількості даних, а також забезпечити безперервний моніторинг інформаційної інфраструктури в режимі реального часу. Класичні ручні методи аналізу загроз, заповнення таблиць Excel, виконання перевірок за чек-листами вже не здатні забезпечити належний рівень швидкості реагування та комплексного охоплення сучасних ризиків.

Одним із ключових напрямів автоматизації є використання платформ для управління ризиками (GRC – Governance, Risk and Compliance). Такі системи, як RSA Archer GRC, LogicManager, ServiceNow Risk Management чи MetricStream, дозволяють централізовано керувати ризиками, політиками, аудитами, контролями та інцидентами. Вони інтегрують усі компоненти системи безпеки в єдине середовище, забезпечують візуалізацію ризик-профілів, автоматичне формування звітів та моніторинг відповідності нормативним вимогам. Це значно спрощує взаємодію між департаментами безпеки, аудиту та управління.

Іншою важливою складовою є автоматизовані системи виявлення вразливостей, як-от Nessus, OpenVAS, Qualys або Rapid7 InsightVM. Вони дозволяють регулярно та автоматично сканувати IT-інфраструктуру на наявність вразливостей, класифікувати їх за рівнем критичності (часто з

урахуванням CVSS-балів), формувати рекомендації щодо усунення та інтегрувати результати у загальну систему оцінювання ризиків. Таким чином, автоматизація сканування дозволяє організаціям оперативно реагувати на нові загрози та уникати повторного виявлення одних і тих самих проблем.

Ще одним важливим напрямком є автоматизація обробки інцидентів за допомогою SIEM-систем (Security Information and Event Management), таких як IBM QRadar, Splunk, AlienVault OSSIM чи ArcSight. Вони збирають журнали подій з усіх компонентів мережі, аналізують їх у режимі реального часу та автоматично генерують попередження про підозрілу активність або потенційні інциденти. Поєднуючи SIEM із системами автоматизованого реагування (SOAR – Security Orchestration, Automation and Response), організація отримує можливість не лише виявляти загрози, а й миттєво вживати заходів: блокувати підозрілі IP-адреси, закривати доступи, ізолювати заражені пристрої тощо.

Важливим елементом автоматизації є також використання штучного інтелекту (AI) та машинного навчання (ML) для аналізу поведінки користувачів та виявлення аномалій. Такі системи, наприклад, як Darktrace, можуть вивчати нормальну поведінку працівників і пристроїв у мережі, і на цій основі автоматично виявляти підозрілі дії або порушення політик. Це дозволяє виявити загрози нового типу, які ще не мають відомих сигнатур або шаблонів.

Автоматизація також охоплює процес оцінки ризиків на основі моделей типу FAIR (Factor Analysis of Information Risk), реалізованих, зокрема, в платформі RiskLens. Ці системи дозволяють проводити кількісну оцінку ризиків у грошовому еквіваленті на основі об’єктивних і суб’єктивних факторів. Вони автоматизують збір даних, побудову моделей втрат, генерацію сценаріїв та аналіз впливу різних заходів контролю на ризиковий профіль компанії.

Крім того, автоматизація дозволяє реалізовувати циклічні процеси управління ризиками, у яких дії з ідентифікації, аналізу, реагування та перегляду ризиків постійно оновлюються за допомогою спеціалізованих інструментів. Це підтримує концепцію безперервного вдосконалення (continuous improvement) та підвищує загальний рівень кіберстійкості.

Впровадження автоматизованих рішень у сфері управління кіберризиками не лише підвищує ефективність та швидкість реагування, але й дозволяє керівництву отримувати вичерпну інформацію про поточний рівень ризиків, обґрунтовувати бюджет на кібербезпеку та приймати стратегічні рішення на основі об’єктивних даних.

3.4 Оцінка ефективності запропонованих заходів

Ефективність заходів з управління кіберризиками визначається не лише фактом їх впровадження, але й здатністю реально знижувати рівень ризику, підвищувати кіберстійкість організації та забезпечувати відповідність нормативним вимогам. Оцінка ефективності є критичним етапом у циклі управління ризиками, адже дозволяє виявити сильні й слабкі сторони обраних стратегій, оптимізувати ресурси та обґрунтовано приймати рішення щодо подальших кроків.

Насамперед, до оцінки варто підходити системно, використовуючи поєднання кількісних і якісних методів аналізу**.** Для цього застосовуються такі ключові показники:

1. Зниження залишкового ризику (residual risk) – порівняння рівня ризику до та після впровадження заходів. Це може бути реалізовано через повторне заповнення матриці ризиків або перегляд моделей, побудованих за методологією FAIR.
2. Кількість кіберінцидентів за певний період часу до і після застосування заходів – один з найочевидніших і об'єктивних індикаторів ефективності.
3. Час виявлення і реагування (MTTD/MTTR) – середній час, необхідний для виявлення (Mean Time to Detect) та усунення інциденту (Mean Time to Respond). Зменшення цих показників свідчить про підвищення ефективності як технічних, так і організаційних заходів.

4. Оцінка ефективності навчань персоналу – проводиться за допомогою тестування, симульованих фішингових атак, результатів кібернавчань та тренувальних сценаріїв реагування.
5. Відповідність стандартам та аудитам – проходження зовнішніх або внутрішніх аудитів без критичних зауважень (наприклад, відповідність ISO 27001, GDPR, NIST CSF тощо) демонструє високий рівень зрілості управління ризиками.

Важливим аспектом оцінки є використання цифрових дашбордів і звітів, які агрегують дані з SIEM, GRC та інших систем безпеки. Вони дозволяють у реальному часі відслідковувати показники ефективності, виявляти «вузькі місця» та оцінювати прогрес у впровадженні заходів.

Для забезпечення об’єктивності також варто залучати зовнішніх експертів або аудит – незалежна оцінка допомагає уникнути «сліпих зон», які можуть виникати через внутрішні упередження або недостатній технічний досвід.

Ще одним підходом є моделювання сценаріїв атак до та після впровадження заходів. Це дозволяє оцінити, чи дійсно вжиті дії зменшують імовірність успішного впливу загроз або знижують очікувані збитки. Таке моделювання може бути виконано з використанням засобів аналізу ризиків (наприклад, RiskLens, FAIR-аналітики) або шляхом проведення пентестів.

Крім цього, важливо враховувати і економічну ефективність заходів – порівняння вартості реалізації з очікуваними збитками, яких вдалося уникнути. Наприклад, інвестиції в SIEM можуть бути виправданими, якщо вони дозволили своєчасно виявити і заблокувати загрозу, що могла призвести до суттєвих фінансових або репутаційних втрат.

На завершення, оцінка ефективності повинна бути не разовою дією, а безперервним процесом**,** інтегрованим у загальну систему управління ризиками. Рекомендовано проводити періодичний перегляд стратегії безпеки, базуючись на зворотному зв’язку, аналізі результатів заходів та зміні загрозового ландшафту.

У результаті, ретельна оцінка ефективності дозволяє не лише підвищити загальний рівень захищеності організації, але й сформувати культуру безпеки, орієнтовану на постійне вдосконалення та адаптацію до нових викликів кіберпростору.

Висновок до розділу 3

У третьому розділі було розглянуто ключові стратегії та інструменти, спрямовані на мінімізацію кіберризиків, які є критичними для забезпечення стабільної роботи інформаційних систем сучасної організації. Проаналізовано технічні, організаційні заходи, а також підходи до автоматизації процесів управління ризиками та оцінки їх ефективності.

До основних технічних засобів зниження ризиків належать впровадження SIEM-систем (таких як IBM QRadar, Splunk, AlienVault), використання принципів Zero Trust, багатофакторної автентифікації (MFA), контролю доступу, а також систем виявлення вразливостей. Ці засоби дозволяють оперативно виявляти й реагувати на кіберзагрози, знижуючи ймовірність їхнього впливу на критичні активи[60].

Організаційні заходи, зокрема розробка політик інформаційної безпеки, підвищення обізнаності персоналу, регулярні кібернавчання та тестування на проникнення, є не менш важливими. Вони сприяють формуванню культури безпеки, зменшують вплив людського фактору та забезпечують злагоджену взаємодію технічних рішень з управлінськими процесами.

Особлива увага була приділена автоматизації процесу управління ризиками – через використання GRC-платформ, інтеграцію з SIEM, формування звітності та моніторингових панелей. Це забезпечує підвищення ефективності, прозорості та швидкості прийняття рішень[35-38].

У підрозділі 3.4 доведено, що ефективність заходів мінімізації ризиків повинна оцінюватись системно, з урахуванням кількісних та якісних показників.

Регулярний аудит, повторна оцінка залишкового ризику, аналіз інцидентів, а також порівняння фактичних результатів з очікуваними – все це дозволяє об’єктивно визначити доцільність обраних заходів і оптимізувати кіберзахист.

Ефективне управління кіберризиками вимагає інтегрованого підходу, що поєднує сучасні технічні рішення, чітко регламентовані організаційні процеси та автоматизовані системи моніторингу. Лише комплексна реалізація всіх перелічених компонентів дозволяє суттєво знизити рівень загроз та підвищити кіберстійкість організації в умовах динамічного загрозового середовища.

Розділ 4 ПРАКТИЧНА РЕАЛІЗАЦІЯ СИСТЕМИ ОЦІНКИ УПРАВЛІННЯ КІБЕРРИЗИКАМИ

4.1 Впровадження системи оцінки кіберризиків у тестовому середовищі

Практична реалізація системи управління кіберризиками є ключовим етапом у підвищенні рівня інформаційної безпеки організації. Для апробації обраної методики – зокрема, комбінації підходу FAIR з використанням інструментів виявлення вразливостей (Nessus, OpenVAS) – було створено тестове середовище, яке моделює IT-інфраструктуру середньої організації зі стандартною архітектурою: сервери баз даних, вебсервер, сегментована внутрішня мережа, засоби автентифікації та периферійні пристрої[6].

Першим кроком реалізації стала ідентифікація критичних активів (табл.4.1). Було виокремлено сервер баз даних з клієнтською інформацією, вебпортал із зовнішнім доступом, файл-сервер із внутрішньою документацією, а також контролери доступу. Для кожного з активів було визначено потенційні загрози: несанкціонований доступ, експлуатація вразливостей, атаки типу DoS, фішинг тощо.

Таблиця 4.1.

Дентифікація активів і загроз

№	Назва активу	Тип	Критичність	Власник
1	Сервер баз даних	Фізичний/логічний	Висока	IT-відділ
2	Веб-додаток	Логічний	Висока	Розробка
3	Пошта (Exchange Online)	Хмарний сервіс	Середня	Адміністрація
4	Робочі станції	Фізичний	Середня	Усі відділи

Далі здійснено виявлення вразливостей за допомогою сканерів Nessus і OpenVAS, що дозволило створити технічний профіль ризику. Зокрема, для вебпорталу було виявлено кілька застарілих компонентів PHP та відкриті порти, які не мали обґрунтування з боку бізнесу. Це дало змогу сформувати перші технічні метрики впливу та вірогідності успішної атаки.

На базі методології FAIR, дивись табл.4.2., було розраховано оцінку ризику в кількісному вигляді. Наприклад, ймовірність реалізації атаки через виявлену вразливість PHP було оцінено як «середню» на основі CVSS-балу (7.3), а вплив – у фінансовому еквіваленті близько 50 000 дол. США з урахуванням втрати доступу до системи, порушення конфіденційності та можливої репутаційної шкоди. Загальний рівень ризику був класифікований як високий, що стало підставою для ініціювання заходів з мінімізації.

Таблиця 4.2.

Приклад FAIR-аналізу

Параметр	**Оцінка**
Частота атаки (Annual Rate)	4 рази/рік
Ймовірність успіху	30%
Середній збиток за інцидент	$25,000
Очікуваний річний збиток	$30,000

У тестовому середовищі також було апробовано побудову матриці ризиків**,** дивись табл.4.3., у якій поєднувалася оцінена ймовірність виникнення загроз (за шкалою: низька, середня, висока) з очікуваним впливом (незначний, помірний, критичний). Це дозволило ранжувати ризики за пріоритетом реагування й окреслити зони, що потребують негайного втручання[9].

Ключовим елементом стало формування звітності**,** яка включала:

1. перелік виявлених активів і вразливостей;
2. обґрунтовану оцінку ризиків;
3. рекомендації щодо впровадження технічних та організаційних заходів;
4. прогнозоване зниження ризиків після впровадження контрзаходів.

Цей підхід продемонстрував високу ефективність для інтеграції у внутрішню політику безпеки організації. Методика легко масштабувалася, дозволяла комбінувати експертні оцінки з технічними скануваннями та забезпечувала прозорість для управлінського рівня[7].

Таблиця 4.3.

Таблиця ризиків та матриця пріоритетів

ID	Загроза	Актив	Ймовірність	Вплив	Ризик ($)	Рівень ризику
R1	SQL-ін'єкція	Сервер БД	Висока	Висока	30,000	Високий
R2	Фішинг	Пошта	Середня	Середня	10,000	Середня
R3	RDP-атака	Робоча станція	Низька	Висока	5,000	Низька

Рис. 4.1. Графіки з оцінками ризику

У результаті проведеного тестування було підтверджено доцільність впровадження даної моделі в реальних умовах організації. Її практичне

застосування забезпечує як гнучкість в адаптації до змін, так і можливість регулярного моніторингу ризиків із подальшою актуалізацією захисних заходів[16].

4.2 Моделювання загроз та оцінка впливу атак

Моделювання загроз є одним із центральних етапів процесу управління кіберризиками, оскільки дозволяє виявити потенційні сценарії атак на інформаційні активи та оцінити можливі наслідки для організації. Цей процес базується на структурованому підході до аналізу векторів атак, оцінки вразливостей і визначення можливих дій з боку зловмисників. У межах цього дослідження було застосовано методики STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) та DREAD (Damage, Reproducibility, Exploitability, Affected users, Discoverability) у тестовому середовищі, що імітує типову IT-інфраструктуру організації, (табл.4.4) [58-59].

Таблиця 4.4.

Оцінка ризику за моделлю DREAD для основних загроз

№	Загроза	Damage (D)	Reproducibility (R)	Exploitability (E)	Affected Users (A)	Discoverability (D)
1	SQL-ін’єкція	9	8	7	8	6
2	Атака типу DoS (відмова в обслуговуванні)	8	6	6	7	5
3	Несанкціонований доступ до облікового запису (Spoofing)	9	7	8	9	6
4	Витік конфіденційної інформації	10	7	6	9	4

На основі моделі STRIDE було здійснено класифікацію загроз для ключових компонентів інфраструктури. Наприклад[8]:

- Spoofing (Підробка) – ризик компрометації автентифікаційної системи через підбір паролів або викрадення сесій.
- Tampering (Підміна даних) – модифікація даних у БД через SQL-ін’єкції.
- Repudiation (Відмова від дій) – недостатній рівень журналювання може дозволити зловмисникам уникати відповідальності.
- Information Disclosure (Розкриття даних) – ризик витоку персональної або фінансової інформації.
- Denial of Service (Відмова у обслуговуванні) – потенційні атаки на вебсервіс, які блокують доступ до ресурсу.
- Elevation of Privilege (Підвищення привілеїв) – використання вразливостей для отримання прав адміністратора.

Кожна загроза була співвіднесена з відповідним активом та вразливістю, виявленою під час попереднього етапу. Наприклад, для вебпорталу, що обслуговує клієнтів, було змодельовано загрозу SQL-ін’єкції. Вона класифікується за STRIDE як Tampering, а її вплив – як значний, оскільки може призвести до знищення або викрадення критичних даних.

Для кожної загрози було проведено оцінку за критеріями DREAD, де кожен параметр оцінювався за шкалою від 1 до 10. Приклад оцінки атаки SQL-ін’єкції:

- Damage Potential (Шкода): 9
- Reproducibility (Відтворюваність): 8
- Exploitability (Можливість експлуатації): 7
- Affected Users (Кількість постраждалих користувачів): 8
- Discoverability (Ймовірність виявлення вразливості): 6

Середній бал становив 7.6, що вказує на високий рівень ризику. Подібна оцінка дозволяє ранжувати загрози та визначати пріоритет реагування на інциденти.

Матриця, яка допомагає визначити пріоритет реагування на основі ймовірності загрози та її впливу (табл.4.5).

Таблиця.4.5.

Матриця ризику (ймовірність × вплив)

	Низький вплив	Середній вплив	Високий вплив
Низька ймовірність	Низький ризик	Низький ризик	Середній ризик
Середня ймовірність	Низький ризик	Середній ризик	Високий ризик
Висока ймовірність	Середній ризик	Високий ризик	Критичний ризик

Приклад розміщення загроз у матриці:

- SQL-ін’єкція – Висока ймовірність, Високий вплив → Критичний ризик
- DoS-атака – Середня ймовірність, Середній вплив → Середній ризик
- Витік даних – Середня ймовірність, Високий вплив → Високий ризик

У рамках моделювання загроз та оцінки впливу атак важливо побудувати дерево атак (Attack Tree), (рис.4.1), яке наочно відображає можливі шляхи досягнення зловмисником цільової атаки.

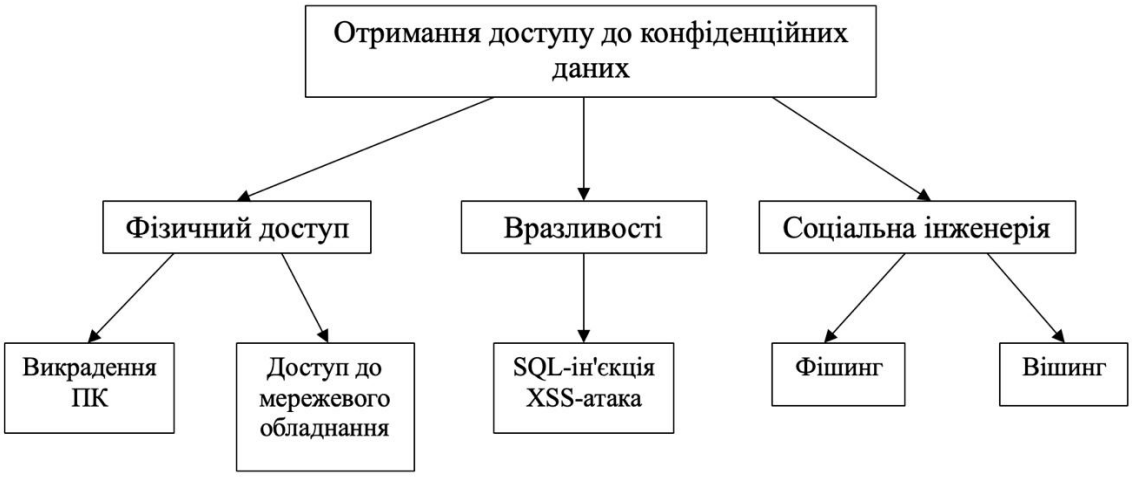

Рис. 4.1. Дерево атак

У даному випадку розглядається ситуація, коли зловмисник прагне отримати доступ до конфіденційних даних, що зберігаються або обробляються на веб-сервері організації.

Першим рівнем дерева виступають три основні вектори атаки: фізичний доступ, використання вразливостей вебдодатку та методи соціальної інженерії.

Фізичний доступ передбачає пряме втручання у фізичну інфраструктуру інформаційної системи. Одним із шляхів реалізації є викрадення персонального комп’ютера користувача, який має доступ до захищених систем, що потенційно дозволяє обійти логічні механізми захисту, використовуючи скомпрометований пристрій. Інший можливий варіант – несанкціонований доступ до мережевого обладнання, такого як маршрутизатори або комутатори. Це дозволяє зловмиснику перехоплювати мережевий трафік, змінювати конфігурацію пристроїв або впроваджувати атаки «людина посередині».

Вразливості вебдодатку є другим основним напрямком атаки. Зокрема, застосування SQL-ін'єкцій дозволяє виконати неавторизовані запити до бази даних через введення спеціально сформованого коду у поля вводу на вебсторінці. Це може призвести до витоку конфіденційної інформації. Іншим поширеним методом є XSS-атаки (міжсайтове скриптування), що передбачають впровадження шкідливих скриптів у вебсторінки, які виконуються у браузерах легітимних користувачів, крадучи їхні сесії або облікові дані.

Соціальна інженерія – це третій вектор атак, заснований на маніпулюванні поведінкою людини. Одним з методів є фішинг – масове надсилання підроблених електронних листів, які імітують легітимні повідомлення і містять посилання або вкладення, що крадуть облікові дані користувачів. Ще один варіант – вішинг, тобто телефонне шахрайство, у якому зловмисник переконує жертву добровільно надати чутливу інформацію, видаючи себе за представника офіційної організації.

Кожна гілка дерева атак репрезентує окремий шлях до досягнення кінцевої мети зловмисника – компрометації конфіденційних даних. Кінцеві вузли дерева, або листки, відображають конкретні інструменти або дії, що можуть бути застосовані. За потреби дерево можна деталізувати шляхом додавання ваг або ймовірностей для проведення кількісної оцінки ризику за моделлю, наприклад, FAIR. Такий підхід дозволяє системно і структуровано

аналізувати загрози, виявляти найкритичніші вектори атак та розробляти ефективні заходи протидії.

Для наочності моделювання була побудована дерево атак (Attack Tree), яке демонструє можливі послідовності дій зловмисника для досягнення цілі – компрометації даних користувачів. Також було сформовано матрицю ризиків, що об’єднує оцінку ймовірності реалізації загрози та її впливу.

Оцінка загроз була підтримана результатами сканування з Nessus та OpenVAS, які надали точні дані щодо рівня небезпеки виявлених вразливостей (CVSS бал), що було використано як один із факторів для побудови моделі ризику. Це дало змогу об'єднати моделювання загроз з реальними технічними даними, що значно підвищило точність оцінки.

Застосування структурованого підходу до моделювання загроз дозволило не лише виявити потенційно небезпечні сценарії атак, але й кількісно оцінити їх вплив на критичні активи організації. Поєднання моделей STRIDE і DREAD зі скануванням вразливостей створює основу для прийняття обґрунтованих рішень щодо впровадження контрзаходів та управління ризиками в динамічному середовищі загроз.

4.3 Використання програмних засобів для виявлення ризиків

В умовах зростання кількості кіберзагроз та ускладнення інформаційної інфраструктури сучасних організацій, виявлення ризиків вручну стає недостатньо ефективним. Саме тому програмні засоби для виявлення ризиків відіграють ключову роль у системі кіберзахисту. Вони забезпечують автоматизацію процесів аналізу, виявлення вразливостей, оцінювання ступеня загроз, а також формування рекомендацій для зниження потенційних ризиків. Завдяки цим інструментам організації можуть оперативно реагувати на нові виклики безпеки, зменшуючи ймовірність успішних атак.

Одним із найпоширеніших рішень для сканування вразливостей є Nessus – продукт компанії Tenable, що дозволяє виявляти понад 50 тисяч відомих вразливостей у системах, мережевих сервісах, веб-застосунках і програмному забезпеченні. Nessus використовує базу даних CVE та систему оцінювання CVSS (Common Vulnerability Scoring System) для класифікації ризиків, дивись табл.4.6. Результати сканування містять як технічну інформацію про виявлені уразливості, так і рекомендації щодо їх усунення.

Таблиця 4.6.

Таблиця прикладу результатів сканування Nessus

Ідентифікатор CVE	Назва вразливості	Рівень ризику	Опис	Рекомендація
CVE-2021-34527	PrintNightmare	Критичний	Уразливість у службі Windows Print Spooler	Встановити останнє оновлення від Microsoft
CVE-2020-060	Windows CryptoAPI Spoofing	Високий	Можливість підробки сертифікатів	Застосувати оновлення безпеки
CVE-2019-0708	Remote Desktop Services Remote Code Execution	Високий	RDP-сервіс дозволяє виконання коду	Вимкнути RDP або оновити систему

Ще один потужний інструмент – OpenVAS (Greenbone Vulnerability Management), є безкоштовною альтернативою комерційним рішенням. Його використовують для активного сканування мережі, виявлення відомих вразливостей, помилок конфігурації, відсутніх оновлень безпеки. OpenVAS є частиною комплексної платформи управління вразливостями Greenbone Security Manager, яка дозволяє інтегрувати результати сканування у процеси оцінки ризиків.

Qualys Vulnerability Management – це хмарна платформа, яка забезпечує безперервний моніторинг IT-інфраструктури. Система автоматично виявляє зміни в середовищі, нові пристрої, порти та сервіси, що дозволяє своєчасно реагувати на появу нових загроз. Qualys підтримує масштабування до великих середовищ і використовується у великих корпораціях, де безперервність бізнес-процесів має критичне значення.

Інший популярний інструмент – Rapid7 InsightVM – забезпечує не лише сканування, а й інтеграцію з іншими компонентами кіберзахисту. InsightVM дозволяє створювати інтерактивні дашборди для візуалізації рівня ризику, пріоритизувати уразливості залежно від критичності активів, автоматизувати реагування на інциденти. Цей підхід дозволяє зосередитися на найважливіших проблемах безпеки, що суттєво знижує операційне навантаження на IT-персонал.

Для виявлення ризиків у веб-застосунках часто використовують Burp Suite**,** що дозволяє проводити динамічне тестування безпеки (DAST), виявляючи XSS, SQL-ін’єкції, CSRF, та інші критичні вразливості. Burp Suite активно застосовується у фазі розробки (DevSecOps), інтегруючись із CI/CD-пайплайнами, що дозволяє виявляти ризики ще до того, як застосунок буде розгорнуто у продуктивне середовище.

Окрім цього, сучасні рішення часто використовують машинне навчання та поведінкову аналітику для виявлення аномалій. Наприклад, платформи на кшталт Darktrace або Cortex XDR (Palo Alto Networks) здатні виявити невідомі раніше загрози шляхом аналізу поведінки користувачів і систем у мережі. Вони використовують алгоритми штучного інтелекту для побудови моделей "нормальної поведінки", і на цій основі виявляють підозрілі дії, які можуть свідчити про потенційну атаку.

Також важливим є використання спеціалізованих платформ для централізованого управління ризиками, таких як Archer GRC або RiskLens**,** які дозволяють інтегрувати результати сканування вразливостей із загальними моделями оцінки ризику, зокрема за методикою FAIR**.** Наприклад, RiskLens

дозволяє перекладати технічні дані про вразливості у кількісні показники ризику, виражені у грошовому еквіваленті, що полегшує прийняття управлінських рішень на рівні керівництва.

Приклад типового результату сканування Nessus може включати такі поля: ідентифікатор CVE, назву вразливості, рівень ризику (за шкалою від низького до критичного), опис потенційного впливу та рекомендації з усунення. Ці дані можуть бути представлені у вигляді таблиць, графіків або інтерактивних звітів.

Таким чином, використання програмних засобів для виявлення ризиків дозволяє забезпечити:

- автоматизовану перевірку IT-інфраструктури на наявність технічних вразливостей;
- постійний моніторинг змін у середовищі;
- інтеграцію з процесами управління ризиками;
- підвищення точності оцінки рівня загроз;
- своєчасне реагування на інциденти безпеки.

Застосування таких інструментів є невід’ємною складовою сучасної стратегії кібербезпеки, що дозволяє забезпечити гнучкість, адаптивність та ефективність у боротьбі з новими викликами кіберпростору.

4.4 Аналіз отриманих результатів та розробка рекомендацій

Після впровадження моделі оцінки кіберризиків у тестовому середовищі, з використанням сучасних інструментів аналізу та управління ризиками (зокрема FAIR, RiskLens, Archer GRC, Nessus, OpenVAS), було проведено комплексний аналіз отриманих результатів з метою виявлення найуразливіших елементів інформаційної системи, оцінки ефективності застосованих заходів кіберзахисту та формування конкретних рекомендацій для покращення рівня безпеки організації[54-57].

Результати сканування інфраструктури за допомогою OpenVAS і Nessus виявили понад 60 уразливостей, з яких 12 класифіковано як критичні, 25 як високого рівня ризику, решта – середні та низькі. Найпоширенішими проблемами були незакриті порти, відсутність оновлень, вразливості у веб-додатках, слабкі або типові паролі, а також відсутність шифрування на деяких сервісах. Ці знахідки свідчать про необхідність впровадження централізованої політики управління вразливостями.

За допомогою платформи RiskLens, що реалізує підхід FAIR, було проведено кількісну оцінку ризиків для ключових цифрових активів організації. Наприклад, ризик несанкціонованого доступу до клієнтської бази CRM-системи було оцінено у потенційні щорічні втрати близько 120 000 доларів США, з імовірністю інциденту 40% і частотою його настання двічі на рік. Подібні розрахунки дозволяють не лише усвідомити масштаб проблеми, а й обґрунтовано планувати витрати на кібербезпеку, виходячи з конкретних очікуваних збитків.

Також було виявлено відсутність централізованого моніторингу подій безпеки, що ускладнює вчасне реагування на потенційні інциденти. Не проводяться регулярні тести на проникнення, що створює загрозу залишення частини критичних ризиків невиявленими. Крім того, політики контролю доступу не реалізують принципу найменших привілеїв, що підвищує ймовірність внутрішніх загроз.

На основі проведеного аналізу сформульовано низку практичних рекомендацій. Передусім рекомендується впровадити SIEM-рішення (наприклад, IBM QRadar або Splunk), які дозволять централізовано збирати, аналізувати та корелювати події інформаційної безпеки в режимі реального часу. Також необхідно запровадити політику Zero Trust із сегментацією мережі та обмеженням доступу до ресурсів лише на основі доведених потреб користувачів. Важливо повсюдно застосувати багатофакторну автентифікацію (MFA), зокрема для адміністративного доступу та віддалених з’єднань.

Крім технічних змін, необхідно впровадити регулярні навчання персоналу з кібергігієни, проводити моделювання фішинг-атак та імітаційні навчання реагування на інциденти. Варто оновити політики інформаційної безпеки, визначити відповідальних осіб за реалізацію кожного контрольного заходу та провести аудит поточних процесів. Щоб забезпечити прозорість управління ризиками, слід розробити метрики та індикатори для оцінки ефективності вжитих заходів (наприклад, KPI, KRI), а також впровадити регулярну звітність про залишкові ризики для вищого керівництва.

Результати практичного впровадження моделі оцінки кіберризиків свідчать про доцільність комплексного підходу, що поєднує кількісні оцінки, автоматизовані інструменти виявлення загроз, технічні засоби моніторингу та активну участь персоналу. Реалізація запропонованих рекомендацій дозволить суттєво зменшити як імовірність, так і наслідки реалізації кіберзагроз, а також створить основу для подальшого вдосконалення системи управління ризиками в організації[53].

Висновок до розділу 4

У ході практичної реалізації моделі управління кіберризиками було доведено ефективність застосування комплексного підходу, що поєднує методики кількісного та якісного аналізу, автоматизовані засоби виявлення вразливостей, програмні рішення для оцінки ризиків, а також організаційні заходи реагування. Впровадження методики FAIR дало змогу отримати точні числові оцінки потенційних втрат від кіберінцидентів, що значно полегшує процес прийняття управлінських рішень на основі ризик-орієнтованого підходу. Моделювання загроз та оцінка впливу атак засвідчили, що навіть окремі недоліки в конфігурації систем можуть спричинити суттєві економічні втрати або витоки критичної інформації. Завдяки інструментам OpenVAS та Nessus було виявлено критичні вразливості в інформаційній інфраструктурі, що дозволило оперативно вжити заходів з їх усунення. Застосування RiskLens, у

свою чергу, забезпечило прозорість та обґрунтованість ризик-менеджменту шляхом моделювання сценаріїв атак та аналізу їхнього потенційного впливу.

Оцінка результатів засвідчила, що найбільш ефективними заходами є не лише технічні інструменти виявлення та реагування, але й організаційна підготовка: розробка політик безпеки, проведення навчань для персоналу, регулярне тестування на проникнення та аудит захищеності. Також важливою стала роль автоматизації процесу управління ризиками, яка дозволяє значно зменшити час на виявлення, аналіз та усунення загроз.

У результаті аналізу та практичних дій було розроблено рекомендації щодо зміцнення захисту інформаційних активів, удосконалення процедур оцінки управління ризиками та формування системи безпеки в організації. Отже, практичний розділ підтвердив, що впровадження сучасної системи оцінки є не лише можливим, але й необхідним кроком для підвищення стійкості інформаційної системи до сучасних кіберзагроз.

ВИСНОВКИ

У межах проведеного дослідження було розглянуто сучасні підходи до оцінки та управління кіберризиками, проаналізовано методики їх кількісної та якісної оцінки, а також проведено практичне моделювання загроз та оцінку впливу кіберінцидентів на інформаційні активи організації. Робота мала на меті дослідити ефективність існуючих інструментів і методів управління кіберризиками, обґрунтувати вибір оптимального підходу для конкретної організаційної структури та запропонувати практичні заходи мінімізації ризиків. Усі поставлені завдання були успішно виконані.

У теоретичній частині були розглянуті ключові системи та моделі аналізу і оцінки ризиків, такі як ISO/IEC 27005, NIST SP 800-30, FAIR, OCTAVE, а також інструменти виявлення вразливостей (Nessus, OpenVAS), які активно використовуються в галузі кібербезпеки. Проведений аналіз дозволив виокремити їхні переваги, обмеження та сфери застосування. Було також сформовано матрицю ризиків і здійснено їх оцінку за ймовірністю та впливом на організацію.

У практичній частині дослідження реалізовано впровадження обраної моделі у складі системи у тестовому середовищі із використанням інструментів RiskLens, Open FAIR, SIEM-систем (Splunk, QRadar), засобів автентифікації (MFA, Zero Trust) та систем моніторингу вразливостей. Моделювання загроз продемонструвало високу ефективність застосування програмних рішень для ідентифікації, аналізу та оцінки ризиків з метою їх мінімізації. Було сформовано звіти, побудовано сценарії атак, проведено аналіз наслідків та розроблено перелік заходів реагування.

Результати дослідження підтверджують відповідність поставленій меті та завданням**,** зокрема:

- досягнуто комплексного розуміння методів оцінки кіберризиків;
- виконано порівняльний аналіз відповідних стандартів та інструментів;
- впроваджено практичну модель управління ризиками;

- оцінено ефективність запропонованих технічних та організаційних заходів.

Практичні рекомендації щодо впровадження результатів роботи включають:

1. Запровадження постійного моніторингу вразливостей за допомогою автоматизованих засобів (Nessus, OpenVAS).
2. Інтеграція SIEM-рішень (QRadar, Splunk) для централізованого аналізу подій безпеки.
3. Застосування методики FAIR для обґрунтованої оцінки фінансових ризиків кіберзагроз.
4. Розробка політик інформаційної безпеки та впровадження процедур реагування на інциденти.
5. Проведення регулярних кібернавчань і тестів на проникнення для підвищення рівня готовності персоналу.
6. Автоматизація процесів управління ризиками для зниження людського фактору та забезпечення оперативності реагування.

Загалом дослідження підтвердило, що ефективне управління кіберризиками можливе лише за умов поєднання сучасних технічних засобів, методологічного підходу до аналізу загроз і високого рівня організаційної зрілості в сфері інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Агенція кібербезпеки та інфраструктурної безпеки США (CISA). Основи кібербезпеки. 2023. URL: https://www.cisa.gov (дата звернення 18.03.2025)

2. Андерсон Р. Інженерія безпеки: посібник зі створення надійних розподілених систем. 3-є вид. Гобокен: Wiley, 2020. 1184 с.

3. Архітектура нульової довіри. NIST SP 800-207. Гейтерсбург: NIST, 2020.

4. Бенді Дж. Ефективна кібербезпека: посібник із найкращих практик і стандартів. Себастопол: O'Reilly Media, 2018. 434 с.

5. Вітман М.Е., Маттord Г.Дж. Основи інформаційної безпеки. 6-е вид. Бостон: Cengage Learning, 2017. 672 с.

6. Палко, Д., & Мирутенко, Л. (2024). МЕТОД КОМПЛЕКСНОЇ ОЦІНКИ РИЗИКІВ КІБЕРБЕЗПЕКИ В РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(26), 487–502. https://doi.org/10.28925/2663-4023.2024.26.731.

7. Дослідницький інститут Capgemini. Розрив цифрової довіри. Париж: Capgemini, 2021.

8. Інститут FAIR. Таксономія ризиків FAIR – Факторний аналіз інформаційного ризику. Пало-Альто: FAIR Institute, 2021.

9. Інститут Ponemon. Звіт про вартість порушення даних 2023. Анн-Арбор: IBM Security, 2023.

10. Інститут SANS. Критичні контрольні заходи безпеки. 2023. URL: https://www.sans.org (дата звернення 26.03.2025)

11. Каур Х., Гілл Н.С. Систематичний огляд архітектури нульової довіри. International Journal of Information Management. 2021. Т. 58.

12. Лі Е. та ін. Кількісний аналіз ризику FAIR у хмарних середовищах. ACM Computing Surveys. 2022.

13. Модель сертифікації зрілості кібербезпеки (CMMC). Міноборони США, 2023. URL: https://www.federalregister.gov/documents/2023/12/26/2023-27280/cybersecurity-maturity-model-certification-cmmc-program (дата звернення 05.04.2025)

14. Національна база вразливостей (NVD). NIST, 2024. URL: https://nvd.nist.gov (дата звернення 05.04.2025)

15. Програма Cyber Essentials. Національний центр кібербезпеки Великої Британії, 2023.URL: https://www.ncsc.gov.uk/cyberessentials/overview (дата звернення 06.04.2025)

16. Пфлігер К.П., Пфлігер С.Л. Безпека в обчисленнях. 5-е вид. Аппер Седл Рівер: Prentice Hall, 2015. 848 с.

17. Регламент (ЄС) 2016/679 Європейського парламенту та Ради (Загальний регламент захисту даних – GDPR). Офіційний журнал ЄС, 2016.

18. Росс Р., МакЕвіллі М., Орен Дж. Інженерія безпеки систем. Гейтерсбург: NIST SP 800-160, 2016.

19. Сталінгс В., Браун Л. Комп'ютерна безпека: принципи та практика. 4-е вид. Бостон: Pearson, 2018. 704 с.

20. Фонд OWASP. Десять основних загроз безпеки вебдодатків OWASP – 2023. URL: https://owasp.org/www-project-top-ten/ (дата звернення 09.04.2025)

21. Центр Інтернет-безпеки. CIS Controls v8, 2021. URL: https://www.cisecurity.org/controls (дата звернення 10.04.2025)

22. Шнайєр Б. Прикладна криптографія: протоколи, алгоритми та вихідний код на С. 20-річне ювілейне видання. Нью-Йорк: Wiley, 2015. 784 с.

23. Accenture. Стан кіберстійкості 2023. Дублін: Accenture, 2023. URL: https://www.accenture.com/us-en/insights/security/state-cybersecurity (дата звернення 06.04.2025)

24. AlienVault. Посібник з об'єднаного управління безпекою. AT&T Cybersecurity, 2023. URL: https://cybersecurity.att.com/documentation/ (дата звернення 08.04.2025)

25. CERT-UA. Кіберзагрози в Україні: щорічний звіт 2023. Київ: Держспецзв'язку, 2023. URL: https://cip.gov.ua/ua/news/kiberoperaciyi-rf-novi-cili-instrumenti-ta-grupi-analitika-khakerskikh-atak-proti-ukrayini-za-2-pivrichchya-2023-roku (дата звернення 09.04.2025)

26. Check Point. Звіт з кібербезпеки 2023. Сан-Карлос: Check Point, 2023. URL: https://www.checkpoint.com/resources/report-4fd2/report-cyber-security-report-2023 (дата звернення 10.04.2025)

27. Cisco. Щорічний звіт з безпеки 2023. Сан-Хосе: Cisco Systems, 2023. URL: https://blog.talosintelligence.com/cisco-talos-2023-year-in-review/ (дата звернення 10.04.2025)

28. CrowdStrike. Глобальний звіт про загрози 2023. Санівейл: CrowdStrike, 2023. URL: https://www.crowdstrike.com/resources/reports/2023-global-threat-report/ (дата звернення 10.04.2025)

29. ENISA. Звіт про кіберкризові навчання. Іракліон: ENISA, 2021. URL: https://www.enisa.europa.eu/publications/enisa-cyber-crisis-management-exercise-report-cyclone (дата звернення 11.04.2025)

30. ENISA. Ландшафт кіберзагроз 2022. Іракліон: Агенція ЄС з кібербезпеки, 2022. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (дата звернення 11.04.2025)

31. FireEye Mandiant. M-Trends 2023. Рестон: FireEye, 2023. URL: https://www.mandiant.com/resources/m-trends-2023 (дата звернення 12.04.2025)

32. Fortinet. Глобальний ландшафт загроз 2023. Санівейл: Fortinet, 2023. URL: https://www.fortinet.com/fortiguard/threat-research/threat-landscape-report (дата звернення 12.04.2025)

33. Gartner. Магічний квадрант SIEM-рішень 2023. Стемфорд: Gartner, 2023.

34. Google Cloud. Стан DevSecOps 2023. Маунтін-В'ю: Google, 2023. URL: https://cloud.google.com/devops/state-of-devops (дата звернення 14.04.2025)

35. Harvard Business Review. Чому компанії повинні кількісно оцінювати кіберризики. 2022. https://hbr.org/ (дата звернення 14.04.2025)

36. IBM QRadar. Огляд SIEM-платформи. IBM, 2023. URL: https://www.ibm.com/products/qradar-siem (дата звернення 15.04.2025)

37. IBM X-Force. Індекс розвідки загроз 2023. IBM Corporation, 2023. URL: https://www.ibm.com/downloads/cas/2Y35J6EL (дата звернення 16.04.2025)

38. ISACA. Стан кібербезпеки 2023. Шомбург: ISACA, 2023. URL: https://www.isaca.org/ (дата звернення 17.04.2025)

39. ISC². Дослідження кадрового потенціалу в сфері кібербезпеки 2023. ISC², 2023.

40. ISO/IEC 27001:2013. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. Женева: ISO, 2013. 30 с.

41. ISO/IEC 27002:2022. Кодекс практики для контролю інформаційної безпеки. https://www.dqsglobal.com/uk-ua/navchajtesya/blog/pereglyad-iso-27002.-e-zmini (дата звернення 05.04.2025)

42. ISO/IEC 27005:2018. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки. Женева: ISO, 2018. 68 с.

43. ISO/IEC 27035-1:2022. Управління інцидентами інформаційної безпеки – Принципи управління інцидентами.

44. ISO/IEC 27701:2019. Розширення до ISO/IEC 27001 і ISO/IEC 27002 щодо управління конфіденційністю.

45. Kaspersky ICS CERT. Threat landscape for industrial automated systems. Kaspersky, 2023.

46. Microsoft. Звіт з цифрового захисту 2023. Редмонд: Microsoft, 2023.

47. MITRE. База знань ATT&CK®. 2023. URL: https://attack.mitre.org (дата звернення 02.05.2025)

48. Nessus Professional. Посібник зі сканування вразливостей. Tenable, 2023.

49. NIST SP 800-30 Rev. 1. Посібник з проведення оцінки ризиків. Стоунбернер Г., Гогюен А., Ферінга А. Гейтерсбург: NIST, 2012. 49 с.

50. NIST SP 800-53 Rev. 5. Контроль безпеки та конфіденційності для інформаційних систем та організацій. Гейтерсбург: NIST, 2020. 486 с.

51. Open Group. Стандарт аналізу ризиків Open FAIR. Сан-Франциско: Open Group, 2017. URL: https://www.opengroup.org/certifications/open-fair (дата звернення 18.04.2025)

52. OpenVAS. Огляд управління вразливостями. Greenbone, 2023. URL: https://www.greenbone.net/en/community-edition/ (дата звернення 19.04.2025)

53. PCI DSS v4.0. Рада стандартів безпеки PCI, 2022.URL: https://www.pcisecuritystandards.org/document_library/ (дата звернення 20.04.2025)

54. Qualys. Стан вразливостей 2023. Фостер-Сіті: Qualys, 2023.URL: https://www.qualys.com/info/reports/ (дата звернення 21.04.2025)

55. Rapid7. Звіт про інтелектуальні вразливості 2023. Бостон: Rapid7, 2023. URL: https://www.rapid7.com/info/voice-of-the-vulnerability-analyst/ (дата звернення 22.04.2025)

56. Шульга,В. П., Іванченко,Є. В., Вишневська,Н. С.,& Бербер, А. С. (2024). Дослідження методів та моделей оцінювання кіберзахисту критичної інфраструктури держави. Сучасний захист інформації, 3(59), 6–19. https://doi.org/10.31673/2409-7292.2024.030001.

57. Splunk Security Essentials. Випадки використання виявлення та аналітики. Splunk, 2023. URL: https://www.splunk.com/en_us/software/splunk-security-essentials.html (дата звернення 23.04.2025)

58. Splunk. Стан безпеки 2023. Сан-Франциско: Splunk, 2023. URL: https://www.splunk.com/en_us/form/state-of-security.html (дата звернення)

59. Trellix. Звіт про кіберзагрози 2023. Мілпітас: Trellix, 2023. URL: https://www.trellix.com/en-us/threat-center/threat-reports.html (дата звернення 25.04.2025)

60. Verizon. Звіт про порушення даних 2023. Нью-Йорк: Verizon, 2023. URL: https://www.verizon.com/business/resources/reports/dbir/ (дата звернення 02.05.2025).