Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(освітній рівень)

на тему: "Інтерпретація системи оцінки вразливостей, як методу для оцінки ризиків"

Виконав: студент (ка)

Спеціальності:
125 «Кібербезпека та захист інформації»
(шифр і назва напряму підготовки, спеціальності)
Ревура Дмитро Степанович
підпис (прізвище та ініціали)

Керівник Козак Р.О.
підпис (прізвище та ініціали)

Нормоконтроль Тимощук Д.І.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2024

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека та захист інформації
(шифр і назва спеціальності)

Студенту Ревурі Дмитру Степановичу
(прізвище, ім'я, по батькові)

1. Тема роботи Інтерпретація системи оцінки вразливостей, як методу для оцінки ризиків

Керівник роботи Козак Руслан Орестович, кандидат технічних наук, доцент.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «20» 11 2024 року № 4/7-1112

2. Термін подання студентом завершеної роботи 16.12.2024

3. Вихідні дані до роботи Дані компанії, які включають: вразливості, матрицю ризиків, яку використовує компанія та оцінку вразливостей експерта з ризиків

4. Зміст роботи (перелік питань, які потрібно розробити)
1 Перелік умовних позначень, символів, одиниць, скорочень і термінів, Вступ, 1 Огляд систем оцінки вразливостей та ризиків, 1.1 Поняття систем оцінки вразливостей, 1.2 Підходи до оцінки ризиків, 1.2.1 Якісний метод оцінки ризиків, 1.2.2 Кількісний метод оцінки ризиків, 1.2.3 Порівняльний аналіз методів, 2 Потенціал CVSS 3.0 для оцінки ризиків, 2.1 Комплексний аналіз системи оцінки вразливостей CVSS 3.0, 2.2 Аналіз літератури для інтерпретації, 2.3 Нормалізація як метод інтерпретації CVSS, 3 Інтерпретація CVSS як методу для оцінки ризиків, 3.1 Вхідні дані, 3.1.1 Вразливості, 3.1.2 Матриця ризиків, 3.1.3 Оцінка вразливостей експерта з ризиків, 3.2 Розробка алгоритму, 3.3 Застосування та результати алгоритму, 3.4 Порівняння результатів, 3.5 Висновки та рекомендації, 4 Охорона праці та безпека в надзвичайних ситуаціях, 4.1 Охорона праці, 4.2 Здоровий спосіб життя людини та його вплив на професійну діяльність, Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М., к.т.н., доцент		
Безпека в надзвичайних ситуаціях	Клепчик В.М., проректор з адміністративно-господарської роботи та будівництва		

7. Дата видачі завдання 23.09.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	20.09 – 22.09	Виконано
2.	Пошук і підбір наукових джерел за темою роботи	26.09-01.10	Виконано
3.	Переклад та опрацювання наукових джерел про	02.10-08.10	Виконано
	проблематику інтеграції CVSS		
4.	Оформлення розділу «Огляд систем оцінки вразливостей	09.10-20.10	Виконано
	та ризиків»		
5.	Аналіз системи оцінки вразливостей	21.10–30.10	Виконано
6.	Аналіз літератури для інтерпретації	31.10–10.11	Виконано
7.	Оформлення розділу «Потенціал CVSS 3.0 для оцінки	11.11–14.11	Виконано
	ризиків»		
8.	Розробка та застосування алгоритму	15.11-01.12	Виконано
9.	Порівняльний аналіз результатів	02.12–11.12	Виконано
10.	Оформлення розділу «Інтерпретація CVSS як методу для	12.12–14.12	Виконано
	оцінки ризиків»		
11.	Виконання завдання до підрозділу «Охорона праці та	14.12–15.12	Виконано
	безпека в надзвичайних ситуаціях»		
12.	Нормоконтроль	16.12 – 19.12	
13.	Перевірка на плагіат	20.12	
14.	Попередній захист кваліфікаційної роботи	21.12–22.12	
15.	Захист кваліфікаційної роботи	28.12.2024	

Студент _____ Ревура Д.С.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Козак Р.О.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Інтерпретація системи оцінки вразливостей, як методу для оцінки ризиків // ОР «Магістр» // Ревура Дмитро Степанович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2024 // С. 83, рис. – 9, табл. – 9 , кресл. – , додат. – 1.

Ключові слова: CVSS, ризик, загроза, вразливість, оцінка, нормалізація, управління ризиками.

Кваліфікаційна робота присвячена дослідженню можливості застосування системи оцінки вразливостей CVSS як методу для оцінки ризиків інформаційної безпеки. У роботі проведено огляд існуючих систем оцінки вразливостей і ризиків, включаючи аналіз підходів до оцінки ризиків та їх порівняння. Особливу увагу приділено комплексному аналізу системи CVSS 3.0, її базових метрик та потенціалу для оцінювання ризиків.

У ході дослідження розроблено алгоритм, який забезпечує нормалізацію та масштабування показників CVSS для їхньої адаптації до матриці ризиків. Для перевірки методу проведено тестування на вразливостях. Отримані результати порівняно з експертними оцінками, що дозволило визначити точність і практичну застосовність запропонованого підходу.

Результати роботи підтверджують, що запропонована методика дозволяє інтегрувати CVSS у процеси оцінки ризиків, забезпечуючи стандартизований і автоматизований підхід. Поєднання алгоритмічного підходу з експертним аналізом дозволяє підвищити точність оцінки ризиків, забезпечити стандартизовану звітність і оптимізувати використання ресурсів для реагування на виявлені вразливості. Запропонована методика є перспективною для великих організацій із високим рівнем автоматизації кіберзахисту та може слугувати основою для подальших досліджень у сфері управління ризиками.

ABSTRACT

Interpretation of a Vulnerability Assessment System as a method for Risk Evaluation // Thesis of educational level "Master"// Dmytro Revura // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБс-61 // Ternopil, 2024 // P. 83, figs. 9, tables 9, drawings , added. – 1.

Keywords: CVSS, risk, threat, vulnerability, assessment, risk management.

The qualification work is dedicated to the study of the applicability of the CVSS (Common Vulnerability Scoring System) as a method for assessing information security risks. The work includes a review of existing vulnerability and risk assessment systems, including an analysis of risk assessment approaches and their comparison. Special attention is paid to a comprehensive analysis of the CVSS 3.0 system, its base metrics, and its potential for risk evaluation.

During the study, an algorithm was developed to normalize and scale CVSS metrics for adaptation to a risk matrix. To validate the method, testing was conducted on vulnerabilities. The obtained results were compared with expert evaluations, which allowed for determining the accuracy and practical applicability of the proposed approach.

The results of the work confirm that the proposed methodology enables the integration of CVSS into risk assessment processes, providing a standardized and automated approach. Combining the algorithmic method with expert analysis enhances the accuracy of risk assessments, ensures standardized reporting, and optimizes resource allocation for addressing identified vulnerabilities. The proposed methodology is promising for large organizations with a high level of cybersecurity automation and can serve as a foundation for further research in the field of risk management.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

CVE	—	Common Vulnerabilities and Exposures
CVSS	—	Common Vulnerability Scoring System
NVD	—	National Vulnerability Database
OWASP	—	Open Web Application Security Project
VD	—	Vulnerability Database
Вразливість	—	слабкість у системі, програмному забезпеченні або процесі, яка може бути використана для завдання шкоди або компрометації
Загроза	—	потенційна подія чи дія, яка може скористатися вразливістю для завдання шкоди інформаційним системам, активам або процесам.
Ризик	—	оцінка ймовірності та наслідків реалізації загрози через використання вразливості, що може вплинути на безпеку інформаційних активів.

ВСТУП

Актуальність теми. У сучасних умовах стрімкого зростання кількості кібератак, безпека інформаційних систем стає одним із пріоритетних завдань будь-якої організації. Вразливості, що виявляються в інфраструктурі, безпосередньо впливають на рівень ризику й можуть бути використані зловмисниками для компрометації систем. Зростання кількості загроз створює потребу в простих, ефективних і доступних методах оцінювання ризиків.

Система загальної оцінки вразливостей CVSS (Common Vulnerability Scoring System) широко використовується для визначення критичності вразливостей, але її потенціал можна реалізувати й для оцінки ризиків. Базові показники CVSS містять характеристики, які відповідають категоріям впливу та ймовірності, що створює можливість використання цих даних для розрахунку ризиків. Однак безпосереднє перенесення рейтингу CVSS у корпоративні матриці ризиків ускладнюється через відмінні підходи до оцінювання та пріоритизації загроз. Це призводить до значного залучення експертів, великого обсягу ручної роботи та потенційного недооцінювання окремих ризиків.

Дослідження методів інтерпретації CVSS для узгодження з корпоративними системами управління ризиками є актуальним, оскільки сприяє оптимізації ресурсів, підвищенню швидкості аналізу безпеки та забезпеченню оперативнішого реагування на виявлені вразливості.

Мета і задачі дослідження. Метою кваліфікаційної роботи є дослідження можливості застосування характеристик із системи оцінки вразливостей CVSS для спрощення процесу оцінювання ризиків. Використання показників впливу та ймовірності, наданих цією системою, дозволить автоматизувати оцінювання вразливостей, підвищити ефективність процесу управління ризиками та зменшити витрати часу й інших ресурсів.

Для досягнення поставленої мети передбачено кілька ключових завдань. Спершу необхідно провести аналіз існуючих методів оцінки вразливостей та ризиків у сфері інформаційної безпеки, що дозволить виявити їхні недоліки та

можливості вдосконалення. Далі буде здійснено детальне вивчення структури та компонентів CVSS 3.0, зокрема базової метрики, яка містить необхідні характеристики для інтеграції до матриці ризиків.

Наступним етапом є розробка алгоритму перетворення показників CVSS (Exploitability, Impact) у формат корпоративної 5×5 матриці ризиків, який забезпечить сумісність із наявними системами управління ризиками. Після цього розроблений метод буде протестовано на реальних вразливостях, що дозволить оцінити його практичну застосовність.

На основі отриманих результатів буде проведено порівняльний аналіз із оцінками ризиків експерта.

Об’єкт дослідження. Об’єктом дослідження є процес оцінювання ризиків у сфері інформаційної безпеки.

Предмет дослідження. Предметом дослідження є методика інтеграції базової метрики CVSS у процес оцінки ризиків інформаційної безпеки.

Наукова новизна одержаних результатів кваліфікаційної роботи. Наукова новизна полягає у розробці та тестуванні методики інтеграції базової метрики CVSS 3.0 (Exploitability, Impact) у формат корпоративної матриці ризиків 5×5. Уперше було запропоновано алгоритм (інтеграції) показників CVSS, який передбачає нормалізацію та масштабування даних за допомогою методу «мін-макс» для автоматизованого розрахунку критичності вразливостей. У роботі здійснено емпіричне тестування розробленого підходу, результати якого порівняли з оцінками експертів із ризиків. Доведено, що запропонований підхід сприяє підвищенню швидкості оцінювання ризиків, мінімізації ручної роботи та зменшенню ймовірності недооцінки загроз.

Отримані результати розширюють існуючі підходи до управління ризиками, надаючи організаціям ефективний інструмент для пріоритизації виправлення вразливостей та оптимізації використання ресурсів.

Практичне значення одержаних результатів. Результати дослідження можуть бути покладені в основу впровадження або вдосконалення систем управління ризиками в організаціях, де використовуються CVSS-звіти для

оцінки вразливостей. Запропонована методика дає змогу автоматизувати значну частину рутинної роботи експертів, забезпечуючи при цьому релевантну оцінку критичності кожної вразливості. Упровадження методу дозволяє скоротити витрати часу й інших ресурсів, знижує імовірність помилок, пов’язаних із людським фактором.

Практичне впровадження розробленого алгоритму є корисним для організацій, які прагнуть оптимізувати процес управління ризиками та забезпечити стандартизацію оцінювання вразливостей. Алгоритм дозволяє швидко визначати базовий рівень ризику завдяки комбінованому підходу, поєднуючи автоматизовані обчислення з експертним аналізом, що додає контекст та враховує специфіку бізнесу.

Застосування цієї методики є особливо ефективним для великих організацій із значним обсягом вразливостей та високим рівнем автоматизації кіберзахисту. Вона забезпечує стандартизовані звіти, які можуть слугувати основою для ухвалення стратегічних рішень, спрямованих на підвищення рівня безпеки та стійкості інформаційних систем.

Апробація результатів магістерської роботи. Основні результати проведених досліджень обговорювались на: XII науково-технічній конференції «Інформаційні моделі, системи та технології.

Публікації. Основні результати кваліфікаційної роботи опубліковано у працях конференції (див. Додаток А).

РОЗДІЛ 1 ОГЛЯД СИСТЕМ ОЦІНКИ ВРАЗЛИВОСТЕЙ ТА РИЗИКІВ

1.1 Поняття систем оцінки вразливостей

Системи оцінки вразливостей (англ. Vulnerability Scoring Systems) представляють собою комплекс методологій, метрик та інструментів, призначених для ідентифікації, класифікації та кількісної або якісної оцінки слабких місць у програмному забезпеченні, апаратних засобах чи інформаційних системах [1]. Головна мета таких систем – надати уніфікований підхід до визначення ступеня небезпеки вразливостей, що дозволяє полегшити їх пріоритизацію та прийняття рішень щодо першочергових заходів з усунення або нейтралізації потенційних загроз.

Ключова цінність систем оцінки вразливостей полягає в тому, що вони встановлюють спільну «мову» для комунікації між фахівцями з інформаційної безпеки, розробниками програмного забезпечення, керівниками проєктів та іншими зацікавленими сторонами. Універсальність представлених метрик та підходів спрощує процес обміну даними, аналізу результатів та ухвалення інженерних і управлінських рішень. Застосування узгоджених методик стає відправною точкою для формування єдиних стандартів, рекомендованих практик та розробки інтегрованих процесів управління вразливостями.

Основні інструменти та методології оцінки вразливостей, які сьогодні активно застосовуються в галузі, включають:

– Common Vulnerability Scoring System (CVSS): Найпоширеніша відкрита стандартна методологія, яка забезпечує універсальний формат оцінки вразливостей за допомогою обчислювальної формули і чітко визначених метрик (базових, тимчасових та контекстних). CVSS дозволяє отримати чисельний бал від 0 до 10, що відображає ступінь небезпеки вразливості та полегшує її порівняння з іншими [2].

- Common Weakness Scoring System (CWSS): Спрямована на оцінку слабких місць програмного коду та програмних архітектур. CWSS допомагає розробникам і аудиторам безпеки структуровано оцінювати вразливості ще на етапі розробки або тестування, тим самим сприяючи зниженню кількості критичних проблем після релізу [3].
- DREAD (Damage, Reproducibility, Exploitability, Affected Users, Discoverability): Якісна система оцінки вразливостей, що враховує кілька факторів: потенційні збитки, відтворюваність атаки, складність експлуатації, кількість постраждалих користувачів та ймовірність виявлення вразливості [4]. Хоча DREAD менш формалізований у порівнянні з CVSS, він пропонує гнучкий підхід до оцінки ризиків на ранніх стадіях, а також може слугувати корисним доповненням до формальних методик.

Оцінювання вразливостей саме по собі не є кінцевою метою, а радше проміжним етапом у ширшому процесі забезпечення безпеки. Поєднання результатів оцінювання з інформацією про потенційні загрози, активи та бізнес-процеси організації формує підґрунтя для комплексної оцінки ризиків, ухвалення рішень про розподіл ресурсів та реалізації належних заходів протидії. У такий спосіб, системи оцінки вразливостей сприяють покращенню загального стану кібербезпеки, підвищенню прозорості процесів та забезпечують більш проактивний і стандартизований підхід до управління ризиками інформаційних систем.

1.2 Еволюція CVSS та її еталонний статус

Загальний розвиток систем оцінки вразливостей увійшов у нову фазу з появою Common Vulnerability Scoring System (CVSS). Якщо спершу основні підходи базувалися переважно на суб’єктивних судженнях чи внутрішньокорпоративних методиках, то стандартизація оцінки у вигляді CVSS стала значним кроком уперед. Ця система не лише впровадила зрозумілу шкалу

від 0 до 10, а й принесла із собою чітко окреслені категорії показників, що уможливили більш об’єктивну та уніфіковану оцінку вразливостей, посилили взаєморозуміння між фахівцями та прискорили ухвалення рішень щодо захисту критичних активів.

Далі буде розглянуто ключові етапи розвитку CVSS. Перші версії системи були зосереджені головним чином на технічних аспектах вразливостей та основних параметрах експлуатації. Проте з часом стало очевидним, що для точнішого оцінювання потрібно враховувати динаміку загроз, доступність виправлень, особливості середовища та вплив на бізнес-процеси.

– CVSS 1.0: Початкова редакція заклала фундамент спільної «мови» для оцінювання, проте бракувало деталізації та контексту, а застосування цієї версії на практиці було порівняно обмеженим.
– CVSS 2.0: Наступна версія надала чітку структуру базових, тимчасових і контекстних метрик, що дало змогу точніше оцінювати динамічні чинники, на кшталт наявності публічних експлойтів чи виправлень. Ця версія стала широко застосовуватися у провідних базах даних, як-от National Vulnerability Database (NVD), і фактично закріпила CVSS як загальноприйнятий стандарт.

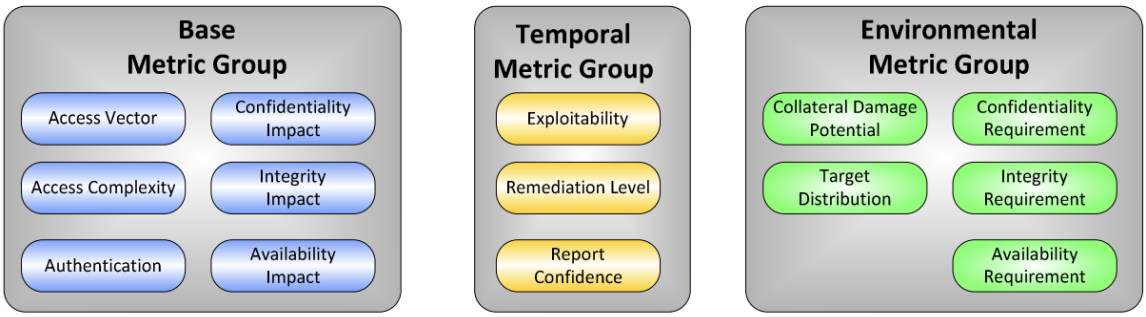

Рисунок 1.1 – Групи метрик у системі CVSS 2.0

З ускладненням інформаційних систем та ескалацією загроз з’явилася потреба у ще більш точному й гнучкому інструментарії. Вихід CVSS 3.0 мав на меті розширити діапазон показників, врахувати складність атаки, потребу у

взаємодії з користувачем, додаткові контекстуальні аспекти та покращити оцінку впливу на конфіденційність, цілісність й доступність.

CVSS 3.1 є подальшим еволюційним кроком, що вдосконалив формулювання метрик. У CVSS 3.1, порівняно з 3.0, розширили та уточнили документацію, що описує використання метрик, зокрема "Privileges Required" і "Scope", для усунення неоднозначностей. Оновлення зробили стандарт більш зрозумілим і зручним для впровадження, зберігши методику розрахунків без змін. CVSS 3.0 залишається основоположним стандартом у сфері оцінювання вразливостей, який широко використовується як еталон завдяки своїй інтеграції у численні проєкти, системи та аналітичні платформи. Чинники, які визначають цей статус 3.0, включають:

– Широку інтеграцію: Багато проєктів, систем та аналітичних платформ вже використовують 3.0, що робить повний перехід на 3.1 часовитратним і не завжди доцільним.
– Накопичений досвід: Фахівці мають глибоке розуміння логіки й метрик 3.0. Значна кількість історичних даних, досліджень та практичних кейсів саме на базі цієї версії забезпечують високу передбачуваність та співставність результатів.

З огляду на стрімкий розвиток загроз та вдосконалення технологій захисту, CVSS 4.0 покликана стати наступним важливим етапом у розвитку системи оцінки вразливостей. Очікується, що нова версія ще краще враховуватиме актуальні тенденції в галузі інформаційної безпеки, пропонуватиме більш гнучкі та точні метрики, а також розширені можливості для моделювання складних сценаріїв застосування у різних середовищах [5]. Втім, станом на сьогодні CVSS 4.0:

– Перебуває на стадії впровадження: Організації та фахівці з безпеки ще не накопичили значного практичного досвіду використання 4.0. Програмні інструменти та бази даних вразливостей перебувають у процесі адаптації до нових вимог і принципів оцінки, закладених у CVSS 4.0.

– Потребує часу для перевірки та оцінювання ефективності: Необхідний певний період апробації, під час якого можна буде об’єктивно порівняти ефективність 4.0 із попередніми версіями, оцінити реальну точність та корисність її метрик для практичних завдань безпеки.

Поява CVSS 4.0 демонструє прагнення професійної спільноти продовжувати вдосконалення підходів до оцінки вразливостей. Попри те, що нині загальновизнаним еталоном залишається CVSS 3.0, у майбутньому, після набуття практичного досвіду впровадження й експлуатації, саме CVSS 4.0 може стати новим стандартом точності, гнучкості та актуальності.

1.3 Підходи до оцінки ризиків

Процес оцінки ризиків в інформаційній безпеці має на меті надати цілісне розуміння небезпек, що загрожують інформаційним активам організації, та визначити пріоритетні напрями використання ресурсів для мінімізації потенційних втрат. На відміну від оцінки вразливостей, що зосереджена переважно на технічних недоліках систем, оцінка ризиків враховує ширший контекст: типи загроз, критичність активів, імовірність реалізації шкідливих сценаріїв та можливий масштаб наслідків.

Оцінка вразливостей відповідає на запитання «де слабке місце?», натомість оцінка ризиків ставить ширше питання: «який негативний вплив на організацію може мати реалізація цієї слабкості разом із конкретною загрозою?». Вразливість – це відсутність або недосконаліть контролю безпеки, а ризик – це імовірність того, що певна загроза скористається вразливістю, завдавши шкоди. З огляду на це, оцінка ризиків базується на поєднанні технічних, організаційних, економічних та управлінських аспектів безпеки.

Ураховуючи дані аспекти, у практиці управління інформаційною безпекою виокремлюють дві категорії ризиків – початкові (inherent) та залишкові (residual) [6]. Такий поділ дає змогу краще зрозуміти ефективність уже застосованих

заходів захисту та визначити, де саме варто сконцентрувати подальші зусилля для мінімізації потенційних втрат.

Початкові ризики характеризуються їхнім існуванням до впровадження будь-яких контрольних заходів чи захисних механізмів. Вони відображають ту загрозу, яка була б актуальною за повної відсутності будь-яких протидій [7]. Аналіз початкових ризиків дозволяє зрозуміти вихідний рівень небезпеки та сформувати відправну точку для подальшого оцінювання. Завдяки цьому можна визначити масштаб потенційних збитків, оцінити ймовірність настання негативних подій без урахування жодних запобіжних заходів та обґрунтувати доцільність інвестицій у системи контролю. Вивчення початкових ризиків надає можливість усвідомити, які загрози в умовах відсутності захисту є найбільш критичними, що, у свою чергу, сприяє більш ефективній розробці стратегії захисту та формуванню пріоритетів у впровадженні контрзаходів.

Водночас основний фокус сучасних досліджень і практичних впроваджень у сфері інформаційної безпеки зміщується саме на аналіз залишкових ризиків. Вони відображають той рівень загрози, який залишається після реалізації заходів захисту та контролю. Залишкові ризики дозволяють отримати реалістичну оцінку стану безпеки системи в актуальних умовах, коли частину загроз уже було нівельовано чи зменшено. Цей підхід дає змогу обґрунтовано визначити, наскільки ефективними виявилися впроваджені механізми захисту, і чи вдалося знизити рівень небезпеки до прийнятних меж. Аналіз залишкових ризиків сприяє оптимальному розподілу ресурсів організації, адже вони допомагають виявити проблемні напрями, які все ще потребують уваги, вдосконалення або додаткових інвестицій. Фактично, залишкові ризики – це найбільш практично значущий об’єкт для аналізу під час ухвалення управлінських рішень у сфері інформаційної безпеки. Вони сигналізують про потребу коригування існуючих заходів безпеки, інтегруються у процес безперервного покращення системи захисту та демонструють реальну картину того, як організація реагує на виклики динамічного інформаційного середовища.

Сконцентрованість на залишкових ризиках випливає з факту, що у більшості міжнародних стандартів та регуляторних документів, зокрема таких як ISO 27001, пріоритет надається саме управлінню ризиками, які залишаються після впровадження контролів [8]. Цим підкреслюється прагматичний підхід: оскільки повна ліквідація всіх загроз майже неможлива, реалістичною метою є досягнення прийнятного рівня ризику, що відповідає ризик-апетиту організації. Таким чином, залишкові ризики фокусують увагу не на теоретичному уявленні про те, наскільки небезпечним міг би бути світ без захисту, а на реальному стані речей та ефективності наявних рішень.

Оцінювання залишкових ризиків є ключовим аспектом розуміння динаміки взаємодії між загрозами та захисними механізмами, оскільки воно ґрунтується на фактичних даних про роботу систем безпеки, аналізі інцидентів, технологічних та організаційних змінах. Це дозволяє встановити, чи виправдані витрати, понесені на впровадження контролів, і наскільки вони трансформували початковий профіль ризиків. Таким чином, кореляція між початковими та залишковими ризиками відображає міру успішності стратегій з управління безпекою. Водночас наявність певного залишкового ризику визнається нормальною та неминучою: управління ризиками – це не тільки зменшення їх до нуля (що практично неможливо), а й досягнення оптимального балансу між захищеністю, вартістю заходів та організаційною ефективністю.

Зрештою, хоча початкові ризики виконують важливу роль у формуванні загальної картини загроз та побудові початкової стратегії захисту, саме залишкові ризики є основним орієнтиром для подальшого вдосконалення системи безпеки. Такий підхід дозволяє адаптивно керувати захисними заходами, забезпечує актуальність оцінок та сприяє прийняттю раціональних управлінських рішень. Для наочності співвідношення та відмінності між початковими і залишковими ризиками можуть бути представлені у вигляді узагальненої таблиці, що демонструє зміни рівня загроз до та після впровадження контролів, а також допомагає наочно відобразити динаміку управлінських рішень у контексті інформаційної безпеки.

Загальний процес оцінки ризиків або як і ще кажуть, типовий процес оцінки ризиків включає такі ключові етапи:

- Ідентифікація активів: Виявлення та класифікація інформаційних ресурсів (дані, системи, програмні продукти), що мають цінність для організації.
- Визначення загроз: Аналіз потенційних джерел небезпеки (зовнішні зловмисники, внутрішні помилки, технічні збої, природні катастрофи тощо).
- Аналіз імовірності та впливу: Визначення, наскільки вірогідною є реалізація кожної загрози та який масштаб наслідків вона може мати (фінансові втрати, витік конфіденційної інформації, зупинка бізнес-процесів).
- Формування стратегії реагування: Обрання оптимальних засобів зниження ризиків – зменшення впливу, зниження імовірності реалізації, передача ризику третім сторонам (страхування) або його прийняття, якщо втрати є прийнятними.

Оцінку ризиків, поділяють на два типи підходів, якісні та кількісні підходи. Залежно від доступності даних, мети аналізу, ресурсів та компетенцій фахівців, застосовують різні методології оцінки ризиків. Найбільш поширеним є поділ на якісні та кількісні методи.

1.3.1 Якісний метод оцінки ризиків

Якісний метод оцінки ризиків базується на використанні експертних суджень, описових категорій і стандартів для ідентифікації, аналізу та оцінювання ризиків [9]. Цей підхід передбачає суб’єктивний аналіз, заснований на знаннях, досвіді та інтуїції фахівців, які оцінюють ймовірність настання ризикової події та її потенційні наслідки. Для визначення рівня ризику часто використовуються шкали оцінки, наприклад, "низький", "середній" та "високий", що дає змогу класифікувати ризики та впорядкувати їх за пріоритетом.

Основною перевагою якісного методу є його висока гнучкість та здатність охоплювати різноманітні аспекти ризику навіть за умов недостатності кількісних даних. Це робить його особливо актуальним для аналізу нових або технічно складних систем, де визначення точних числових показників є проблематичним. Додатково, якісний підхід сприяє швидкому ідентифікуванню критичних ризиків, які вимагають негайного реагування, та забезпечує оперативність у прийнятті управлінських рішень, що є ключовим у динамічному середовищі.

Для впровадження якісної оцінки ризиків використовуються різноманітні інструменти, серед яких матриці ризиків, дерева рішень та сценарний аналіз. Матриця ризиків є одним із найбільш поширених та ефективних інструментів, оскільки вона дозволяє наочно зіставити ймовірність настання ризику із його потенційними наслідками [10]. Такий підхід не лише сприяє інтуїтивно зрозумілій інтерпретації отриманих результатів, але й забезпечує їх практичну придатність для подальшого стратегічного планування та ухвалення рішень.

Проте якісний метод має і певні обмеження. Він залишається суб’єктивним, оскільки результати оцінювання можуть варіюватися залежно від рівня компетентності, упереджень або індивідуального досвіду експертів. Це створює ризик неоднорідності оцінок, що ускладнює їхню узгодженість та надійність. Відсутність кількісних даних також обмежує можливість інтеграції отриманих результатів у складні автоматизовані системи управління ризиками, які потребують точності та стандартизації. Окрім цього, метод не дозволяє проводити об'єктивний порівняльний аналіз різних ризиків, що може бути критичним у процесах стратегічного планування та управління безпекою [11].

Якісний метод оцінки ризиків є корисним інструментом для початкового аналізу та пріоритизації ризиків, особливо у ситуаціях, коли отримання точних кількісних показників є складним або неможливим. Його застосування доцільне у випадках, що вимагають швидких рішень, однак для забезпечення більш точного й обґрунтованого управління ризиками рекомендується доповнювати його іншими підходами.

1.3.2 Кількісний метод оцінки ризиків

Кількісний метод оцінки ризиків базується на аналізі даних і використанні числових показників для визначення ймовірності настання ризикових подій і розрахунку їхнього потенційного впливу [12]. Цей підхід використовує математичні моделі, статистичні методи та спеціалізовані інструменти для забезпечення об’єктивності та точності оцінки. Основою кількісного аналізу є збір і обробка даних, таких як частота інцидентів, фінансові втрати, час простою систем або інші вимірювані параметри.

Важливим етапом у процесі кількісного аналізу є визначення ймовірності ризикових подій. Для визначення ймовірності ризикових подій використовуються методи, що спираються на аналіз історичних даних, проведення імітаційних симуляцій та використання ймовірнісних розподілів. Методи, засновані на історичних даних, дозволяють оцінити ризики на основі попередніх подій, враховуючи частоту їхнього виникнення та пов’язані з ними наслідки. Імітаційні симуляції надають можливість моделювати складні системи та прогнозувати поведінку ризиків у різних сценаріях. Застосування ймовірнісних розподілів дозволяє враховувати невизначеність у прогнозах, забезпечуючи більш гнучкий і точний підхід до аналізу. Такі методи є критично важливими для отримання об’єктивних оцінок, особливо у випадках, коли немає достатніх емпіричних даних. Водночас розрахунок впливу ґрунтується на кількісних оцінках потенційних втрат, що можуть бути виражені у фінансових, часових або інших вимірюваних величинах. Результати цих оцінок дозволяють визначити рівень ризику у вигляді числового значення, що спрощує їх порівняння та ранжування.

Основною перевагою кількісного методу є його об'єктивність і здатність забезпечувати високу точність у процесі оцінювання ризиків. Завдяки використанню математичних моделей та статистичних методів цей підхід дозволяє проводити глибокий аналіз ризиків, враховуючи їхні ймовірності та впливи на систему [13]. Кількісний метод сприяє визначенню сукупного впливу

ризиків, що є критично важливим для стратегічного управління. Наприклад, методи аналізу вартості ймовірних збитків дозволяють ефективно розподіляти ресурси, оптимізуючи їх між різними варіантами управління ризиками. Це забезпечує економічну обґрунтованість рішень, що особливо актуально в умовах обмежених ресурсів та високого рівня невизначеності.

Кількісний підхід має низку обмежень, які слід враховувати під час його впровадження. По-перше, для реалізації цього підходу необхідний значний обсяг надійних даних, що може бути складним завданням у випадках нових систем або нестандартних ситуацій, де історичні дані або статистична інформація є недоступними або обмеженими [14]. По-друге, складність математичних моделей і алгоритмів, які використовуються для кількісного аналізу, вимагає високого рівня технічної експертизи. Це може ускладнювати впровадження методу в організаціях із недостатнім рівнем технологічної підготовки або обмеженими кадровими ресурсами. Нарешті, використання спеціалізованих інструментів та програмного забезпечення для аналізу часто пов’язане зі значними часовими та фінансовими витратами, що може бути критичним у проектах із жорсткими обмеженнями на бюджет або терміни виконання. Таким чином, попри високий потенціал точності й об'єктивності, кількісний метод оцінки ризиків потребує ретельної підготовки для його успішної реалізації.

Таким чином, кількісний метод оцінки ризиків є потужним інструментом для глибокого аналізу ризиків, що забезпечує точність і обґрунтованість прийнятих рішень. Його застосування доцільне в умовах доступності надійних даних і потреби у високоточному управлінні ризиками. Водночас, для підвищення ефективності процесу оцінки ризиків кількісний метод може бути інтегрований із якісним підходом.

1.3.3 Порівняльний аналіз методів

Порівняльний аналіз якісних та кількісних методів оцінки ризиків дозволяє виявити суттєві відмінності в їхньому концептуальному підході, обсязі

необхідних даних, точності результатів та придатності для конкретних умов застосування. Якісні методи в основі своїй покладаються на експертні судження, інтуїтивний досвід і суб’єктивні оцінки. Вони дають змогу оперативно й без надмірних витрат ідентифікувати й упорядкувати ризики за пріоритетністю, використовуючи описові шкали типу "низький/середній/високий". Цей підхід є корисним на початкових етапах аналізу або в ситуаціях, коли неможливо отримати точні кількісні показники. Однак значним недоліком якісного методу є його суб’єктивність та обмежена відтворюваність результатів, що ускладнює порівняння ризиків між різними проектами чи системами.

Натомість кількісні методи оцінки ризиків ґрунтуються на використанні об’єктивних статистичних даних, математичних моделей і числових розрахунків. Вони забезпечують точніші, обґрунтованіші й зіставні результати, наприклад, у вигляді грошових еквівалентів можливих збитків або ймовірностей настання певних подій. Такий підхід дозволяє моделювати різні сценарії, будувати прогнози та оптимально розподіляти ресурси для мінімізації негативних наслідків.

Разом із тим, впровадження кількісних методів часто потребує значних зусиль: необхідні великі обсяги достовірних статистичних даних, застосування спеціалізованих програмних засобів, залучення кваліфікованих аналітиків. Це може збільшити витрати та подовжити час аналізу порівняно з більш простими, але менш точними якісними методами.

Враховуючи наведені аспекти, обираючи між якісними та кількісними методами, варто керуватися доступністю інформації, вимогами до точності, термінами прийняття рішень та наявністю ресурсів. У багатьох випадках оптимальним рішенням є поєднання обох підходів: використання якісних методів для первинного відбору критичних ризиків та застосування кількісних методик для більш детального аналізу й фінансового обґрунтування рішень. Поєднання підходів дозволяє забезпечити комплексний аналіз ризиків, враховуючи як суб’єктивні, так і об’єктивні аспекти. Такий підхід сприяє

підвищенню якості прийняття управлінських рішень. Для зручності узагальнення наведені основні характеристики обох методів у вигляді таблиці:

Таблиця 1.1 – Порівняльна таблиця якісних та кількісних

Критерій	Якісні методи	Кількісні методи
Основний принцип	Оцінка експертами, категоризація ризиків	Використання чисельних показників, статистичних моделей
Необхідні дані	Загальні знання, експертні судження	Статистичні дані, історичні записи, ринкові аналоги
Зручність	Легко зрозуміти, швидко впровадити	Потребують спеціальних знань, додаткових ресурсів
Точність	Відносно суб’єктивні, труднощі з відтворюваністю	Більш точні, але залежать від доступності якісних даних
Результати	Рівні ризиків (низький/середній/високий)	Кількісні оцінки (грошовий еквівалент збитків, ймовірність)
Переваги	Швидкість, простота, придатність для первинної оцінки	Об’єктивність, порівнюваність, можливість прогнозування
Недоліки	Суб’єктивність, відсутність чіткої метричної шкали	Складність, залежність від наявних даних, вартість проведення

Таким чином, вибір методу оцінки ризиків залежить від потреб та можливостей конкретної організації. Якісні методи стануть у пригоді для оперативного формування первинного уявлення про ризики, а кількісні – для глибшого аналізу та ухвалення стратегічних рішень щодо інвестування в заходи безпеки.

Часто застосовують комбінацію обох підходів, поєднуючи гнучкість та швидкість якісних методів із точністю та об’єктивністю кількісних. Це дозволяє сформувати більш повну картину ризиків, сприяючи ефективнішому розподілу ресурсів та підвищенню загального рівня інформаційної безпеки.

2 ПОТЕНЦІАЛ CVSS 3.0 ДЛЯ ОЦІНКИ РИЗИКІВ

2.1 Комплексний аналіз системи оцінки вразливостей CVSS 3.0

Система CVSS версії 3.0 є міжнародно визнаним стандартом для оцінки рівня серйозності вразливостей. Її впровадження та популярність у сфері кібербезпеки зумовлені низкою переваг, які забезпечують її ефективність та надійність у процесі оцінювання ризиків, одночасно спрощуючи та стандартизуючи процедури аналізу.

Стандартизований підхід CVSS 3.0 надає універсальну та узгоджену методологію для визначення серйозності вразливостей. Це забезпечує єдиний формат представлення інформації, який визнається всіма провідними організаціями, такими як NIST, FIRST та MITRE [15]. Завдяки цьому інтеграція CVSS у процеси автоматизації значно спрощується, оскільки результати оцінок є сумісними з більшістю існуючих систем безпеки.

Формули та показники CVSS 3.0 були розроблені з урахуванням можливості програмної реалізації. Ключові метрики, такі як Exploitability Score та Impact Score, обчислюються за чіткими математичними формулами, що дозволяє легко автоматизувати процес оцінювання. Крім того, CVSS 3.0 враховує реальні умови експлуатації вразливостей [15]. Наприклад, метрика Scope (S) дозволяє визначити, чи може вразливість вплинути на інші компоненти системи, а метрика Privileges Required (PR) враховує рівень доступу, необхідний для експлуатації.

CVSS 3.0 сумісна з основними базами даних вразливостей, такими як NVD, CVE та VulDB [16]. Це забезпечує безперешкодну інтеграцію з цими джерелами під час розробки автоматизованих рішень. Крім того, детально задокументовані формули для обчислення метрик, таких як Exploitability та Impact, роблять CVSS 3.0 ідеальною для автоматизації. На відміну від CVSS 4.0, де формули для нових показників ще не представлені у відкритому доступі, CVSS 3.0 забезпечує повну прозорість і готовність до впровадження в існуючі системи.

Порівняно з CVSS 4.0, CVSS 3.0 має кілька ключових переваг. По-перше, на момент написання цієї роботи, більшість інструментів автоматизації та бази даних підтримують саме CVSS 3.0. Для CVSS 4.0 підтримка ще перебуває на етапі впровадження, що ускладнює її інтеграцію. По-друге, як будь-яка нова технологія, CVSS 4.0 потребує часу для перевірки та адаптації. CVSS 3.0 є зрілою, перевіреною часом версією, яка широко використовується в галузі. Крім того, нові показники CVSS 4.0, такі як Evaluation Bias та Provider Bias, більше орієнтовані на ручний аналіз, тоді як CVSS 3.0 забезпечує спрощені й стандартизовані метрики, ідеальні для автоматизації.

Вибір CVSS 3.0 замість CVSS 3.1 також є виправданим. CVSS 3.1 не містить змін у формулах чи математичних розрахунках порівняно з версією 3.0, а лише уточнює інтерпретацію деяких показників [17]. Документація CVSS 3.0 включає всі необхідні формули, значення та рекомендації для автоматизації, що робить її повністю придатною для досягнення цілей роботи. Оскільки основна мета роботи полягає у спрощенні процесу оцінки ризиків та забезпеченні його ефективності, вибір CVSS 3.0 є цілком обґрунтованим. Ця версія системи надає оптимальний баланс між функціональністю та простотою інтеграції, що дозволяє уникати зайвого ускладнення під час реалізації. Стабільність, зрілість і повна підтримка CVSS 3.0 у провідних базах даних та інструментах забезпечують її надійність як стандарту для автоматизації оцінки вразливостей.

Базові метрики CVSS 3.0 відображають внутрішні характеристики вразливості, які залишаються незмінними з часом і в різних середовищах користувачів. Вони складаються з двох наборів: метрик експлуатованості та метрик впливу. Метрики експлуатованості описують легкість і технічні засоби, за допомогою яких вразливість може бути використана. Це характеристики самого вразливого компонента, який може бути програмним забезпеченням, модулем, драйвером або апаратним пристроєм. Метрики впливу, навпаки, відображають наслідки успішного використання вразливості. Вони описують вплив на компонент, який зазнав негативного впливу, і цим компонентом може бути як програмне забезпечення, так і апаратний пристрій або мережева служба.

Особливістю CVSS 3.0 є можливість оцінки наслідків, які виходять за межі самого вразливого компонента . Це означає, що вплив може поширюватися на інші частини системи або ресурси, залежно від контексту. Ця властивість відображається через метрику "Область впливу" (Scope), яка враховує потенціал поширення впливу поза початкові межі.

Тимчасові метрики (Temporal Metric Group) відображають характеристики вразливості, які можуть змінюватися з часом, але залишаються незмінними для різних середовищ користувачів. Наприклад, наявність простого у використанні експлойт-коду збільшує оцінку CVSS, оскільки полегшує експлуатацію вразливості. Натомість створення офіційного патча, який закриває вразливість, знижує її оцінку, оскільки зменшується ймовірність використання.

Екологічні метрики (Environmental Metric Group) відображають характеристики вразливості, які мають значення тільки для конкретного середовища користувача. Ці метрики дозволяють аналітику врахувати наявність заходів безпеки, які можуть зменшити наслідки експлуатації, а також скоригувати значення оцінки відповідно до бізнес-ризиків. Таким чином, екологічні метрики дозволяють адаптувати оцінку критичності вразливості до унікальних умов конкретної організації.

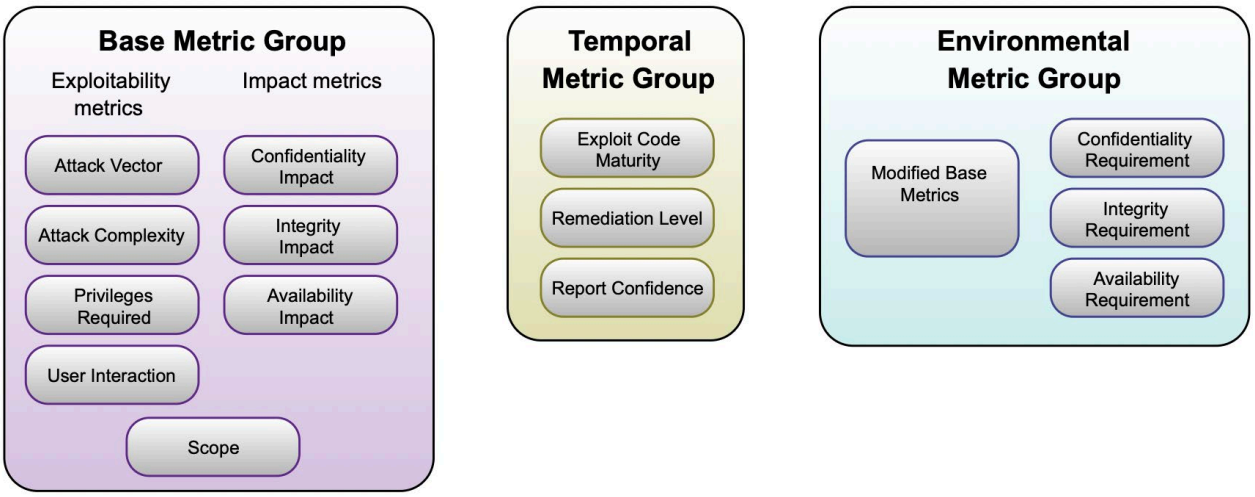

Рисунок 2.1 – Групи метрик у системі CVSS 3.0

Базовий бал (Base Score) у CVSS 3.0 складається з двох основних компонентів: експлуатованості (Exploitability) та впливу (Impact).

Exploitability складається з наступних метрик:

- Attack Vector (AV).
- Attack Complexity (AC).
- Privileges Required (PR).
- User Interaction (UI).

Метрика Attack Vector (AV) відображає контекст, за якого можлива експлуатація вразливості. Чим більш віддаленим є вектор атаки, як логічно, так і фізично, тим вищим буде значення цієї метрики, оскільки кількість потенційних зловмисників, що можуть спробувати використати вразливість, зростатиме з ширшою доступністю. Якщо вразливий компонент можна атакувати через мережу, тобто з будь-якої точки Інтернету, значення буде максимальним. Такий варіант позначають як Network (N). Якщо ж атака можлива лише в межах локальної чи логічно суміжної мережі, значення відповідає варіанту Adjacent (A). Коли вразливість потребує локального доступу до системи, використовується варіант Local (L), а у випадку, коли експлуатація потребує фізичного контакту з обладнанням, застосовується значення Physical (P).

Наприклад, мережевий вектор може охоплювати ситуацію, коли зловмисник ініціює відмову в обслуговуванні через спеціально сформовані пакети. Для векторів Adjacent типовим прикладом є атаки, що потребують перебування у тій самій підмережі, наприклад, ARP-флудинг, що спричиняє відмову в обслуговуванні. Local означає, що атакувальник має можливість виконувати операції з файлом чи процесом без мережевого впливу, і, можливо, навіть увійти до системи. Physical припускає безпосередній фізичний доступ до пристрою, наприклад, для зчитування даних з оперативної пам’яті чи використання вразливості через периферійні інтерфейси.

Метрика Attack Complexity (AC) описує умови, які не залежать від зловмисника, але необхідні для успішної експлуатації вразливості. Якщо таких додаткових умов немає, використовується значення Low (L), що означає високу

передбачуваність успіху атаки без додаткових зусиль. Якщо ж успішний напад вимагає рідкісних обставин або додаткових дій, які складно забезпечити (наприклад, потрібне специфічне налаштування системи, підготовка середовища, виявлення унікальних параметрів чи обхід складних механізмів захисту), використовується значення High (H). Це вказує на складніший сценарій, коли зловмиснику доведеться інвестувати більше часу і ресурсів у підготовку атаки, наприклад, зібрати докладну інформацію про ціль або багаторазово повторювати атаку, щоб подолати випадкові чи складні захисні заходи.

Метрика Privileges Required (PR) відображає рівень привілеїв, якими повинен володіти зловмисник до моменту атаки. Якщо жодних попередніх привілеїв не потрібно, використовується значення None (N). Це вказує на найсприятливіший для зловмисника сценарій, коли він не має початкового доступу до системи.

Якщо необхідні базові привілеї, наприклад, звичайного користувача з обмеженим впливом на конфігурації або дані, які не є критичними, застосовується значення Low (L). Значення High (H) означає, що для успішної експлуатації вразливості потрібні суттєві привілеї, зокрема адміністративні, які дають змогу модифікувати широке коло налаштувань чи файлів у масштабах усього компонента.

Метрика User Interaction (UI) визначає, чи потрібно залучення користувача, відмінного від зловмисника, для успішної компрометації системи. Якщо взаємодія користувача не потрібна, значення буде None (N). Це означає, що зловмисник може здійснити атаку самостійно й безпосередньо. Якщо ж успішне використання вразливості залежить від дії користувача, наприклад, встановлення програмного пакета адміністратором або відкриття користувачем шкідливого файлу, використовується значення Required (R). Така ситуація свідчить, що атака повністю не підконтрольна зловмиснику, оскільки він мусить розраховувати на поведінку та дії стороннього користувача.

Метрики впливу описують властивості компонента, який зазнає негативних наслідків у разі успішної експлуатації вразливості. Якщо успішна атака стосується одного або кількох компонентів, для оцінки слід обрати той, який зазнає найгіршого та найбільш очевидного та передбачуваного результату. Іншими словами, аналітик має орієнтуватися на реалістичний кінцевий наслідок, у досягненні якого зловмисник може бути впевненим.

Якщо область впливу не змінюється, метрики впливу відображають збитки для конфіденційності, цілісності та доступності саме вразливого компонента. Проте, якщо область впливу змінюється, оцінка проводиться з урахуванням того компонента (вразливого чи додатково залученого), який потерпає найбільше.

Метрика Confidentiality Impact (C) вимірює вплив на конфіденційність інформаційних ресурсів, якими оперує програмний компонент. Конфіденційність означає обмежений доступ до інформації, що передбачає недопущення несанкціонованого розкриття даних. Значення цієї метрики зростає зі ступенем втрати даних:

- High (H) означає повну втрату конфіденційності або витік критично важливої інформації.
- Low (L) вказує на частковий витік, який не завдає прямої серйозної шкоди.
- None (N) означає відсутність втрати конфіденційності.

Метрика Integrity Impact (I) оцінює вплив на цілісність даних чи ресурсів, якими керує компонент. Цілісність визначає довіру до достовірності та правильності інформації:

- High (H) означає повну втрату цілісності або можливість зловмисника змінювати файли та дані довільним чином з серйозними наслідками.
- Low (L) свідчить, що зловмисник може здійснювати певні модифікації, але вони не становлять безпосередньої, значної загрози.
- None (N) означає, що цілісність компонента не порушена.

Метрика Availability Impact (A) оцінює вплив на доступність ресурсу. Доступність означає можливість користувачів безперешкодно отримувати доступ до інформаційних ресурсів:

– High (H) означає повну втрату доступності, коли зловмисник може цілковито заблокувати доступ або створити умови, за яких ресурс стане недоступним.
– Low (L) вказує на зниження продуктивності чи переривання доступу, проте без повного відключення і без серйозних наслідків.
– None (N) означає, що доступність ресурсу залишається незмінною.

Таким чином, ці три метрики (C, I та A) допомагають визначити ступінь шкоди, яку зазнає компонент у разі успішної атаки, а зміна області впливу дає змогу врахувати наслідки і для інших компонентів, якщо вони теж піддаються негативному впливу.

Наведена таблиця демонструє числові значення, що присвоюються різним рівням метрик в CVSS 3.0. Кожна метрика має кілька якісних значень, які переводяться у числовий коефіцієнт. Ці коефіцієнти використовуються у формулах розрахунку базового бала, впливаючи на загальну оцінку критичності вразливості. Чим вищим є коефіцієнт певної метрики, тим сильніше вона впливає на підвищення кінцевого бала.

Особливу увагу слід приділити метриці Privileges Required (PR).Залежно від того, чи змінюється «область впливу» (Scope), числові значення для Low та High різняться.

Якщо Scope залишається незмінним, застосовується наступні значення:

– Для рівня привілеїв "Low" значення 0.62.
– Для рівня привілеїв "High" значення 0.27.

Проте, коли Scope змінюється (тобто вразливість може вплинути на інші компоненти поза межами початкового контексту), ці значення змінюються, підвищуючись до 0.68 (для Low) та 0.50 (для High).

Це відображає посилення критичності ситуації, коли вразливість виходить за рамки початкової сфери, адже навіть при високих привілеях умови атаки стають серйознішими.

Таблиця 2.1 – Числові значення метрик

Metric	Metric Value	Numerical Value
Attack Vector / Modified Attack Vector	Network Adjacent Network Local Physical	0.85 0.62 0.55 0.2
Attack Complexity / Modified Attack Complexity	Low High	0.77 0.44
Privilege Required / Modified Privilege Required	None Low High	0.85 0.62 (0.68 if Scope) 0.27 (0.50 if Scope)
User Interaction / Modified User Interaction	None Required	0.85 0.62
C,I,A Impact / Modified C,I,A Impact	High Low None	0.56 0.22 0

Базовий бал розраховується на основі підсумкових значень Impact та Exploitability, які враховують різні характеристики вразливості. Остаточний результат залежить також від метрики Scope, яка визначає, чи обмежується вплив лише одним компонентом, чи може поширюватися на інші.

Розрахунок базового бала здійснюється за такою логікою:

– Якщо підсумкове значення впливу (Impact sub score) дорівнює 0 або є меншим за 0, вразливість не має критичного впливу, а отже: Base Score=0;
– В іншому випадку підсумковий бал визначається залежно від Scope.

Якщо Scope не змінюється, формула виглядає наступним чином:

$$\text{Base Score} = \text{roundUp}(\min(\text{Impact} + \text{Exploitability}, 10)) \quad (2.1)$$

Якщо Scope змінюється:

$$\text{Base Score} = \text{roundUp}(\min(1.08 \times(\text{Impact} + \text{Exploitability}, 10)) \quad (2.2)$$

Функція roundUp округлює значення у бік збільшення до найближчої десятої частки, що забезпечує плавний перехід між результатами. Максимальне значення бала обмежується 10, оскільки це верхня межа шкали CVSS.

Підсумковий вплив обчислюється з урахуванням параметрів конфіденційності (C), цілісності (I) та доступності(A). Спершу розраховується проміжне значення ISCBase, яке визначається за формулою:

$$ISCBase = 1 - ((1 - Conf) \times (1 - Integ) \times (1 - Avail)) \qquad (2.3)$$

ISCBase (Initial Severity Calculation Base) це проміжна метрика, яка використовується для оцінки впливу (Impact) вразливості в системі CVSS. Вона відображає узагальнений рівень впливу, що базується на трьох основних компонентах:

- ImpactConf (Confidentiality Impact): Рівень впливу на конфіденційність даних.
- ImpactInteg (Integrity Impact): Рівень впливу на цілісність даних.
- ImpactAvail (Availability Impact): Рівень впливу на доступність системи або даних.

Ця формула показує сумарний вплив:

- Якщо жоден із параметрів не зазнав впливу, добуток (1−C)×(1−I)×(1−A) дорівнює 1, а ISCBase=0.
- Якщо хоча б один із параметрів має значення High або Low, значення ISCBase зростає, відображаючи посилення критичності.

Далі підсумкове значення впливу обчислюється залежно від Scope. Якщо Scope не змінюється:

$$Impact = 6.42 \times [ISCBase] \qquad (2.4)$$

Якщо Scope змінюється:

$$Impact_{changed} = 7.52 \times (ISCBase - 0.029) - 3.25 \times \\ \times (ISCBase - 0.02)^{15} \quad (2.5)$$

Формула для випадку зміни області впливу є більш складною, оскільки вона враховує додаткові коригувальні зсуви та степеневі залежності, що забезпечують точніший розподіл результатів. Коефіцієнти 6.42, 7.52 та 3.25 були визначені на основі емпіричних досліджень та моделювання, що дозволило оптимально зіставити оцінки критичності вразливостей їхній реальній вагомості. Таке налаштування параметрів формули забезпечує поступове зростання значення при максимальному впливі на конфіденційність (C), цілісність (I) та доступність (A), дозволяючи досягти верхньої межі шкали (10) у випадках із найвищою критичністю.

Розрахунок експлуатованості (Exploitability sub score) здійснюється за допомогою формули:

$$Exploitability = 8.22 \times AV \times AC \times PR \times UI \quad (2.6)$$

Коефіцієнт 8.22 слугує для масштабування підсумкового значення експлуатованості, щоб його внесок у розрахунок базового бала був співмірним із показником впливу. Цей коефіцієнт забезпечує баланс між двома частинами формули, дозволяючи отримати коректну й узгоджену оцінку критичності вразливості на основі реалістичних сценаріїв атаки.

2.2 Аналіз літератури для інтерпретації

Під час дослідження були розглянуті та проаналізовані наукові роботи, присвячені вдосконаленню процесів управління ризиками, зокрема за допомогою уніфікованих підходів і кількісного аналізу та оптимізації процесів безпеки у програмних і хмарних середовищах. Метою аналізу було знайти

методи, які забезпечують точну, стандартизовану оцінку ризиків та водночас полегшують інтерпретацію отриманих результатів.

У дослідженні "Normalization Framework for Vulnerability Risk Management in Cloud" розглядається проблема управління ризиками вразливостей у хмарних середовищах, зокрема виклики, пов'язані з використанням різних баз даних вразливостей (VD) та їхніх неоднорідних систем оцінки серйозності вразливостей [18]. Ця робота була представлена на Міжнародній конференції IEEE, присвяченій дослідженням у сфері Інтернету речей і хмарних технологій (FiCloud).

Різні бази даних вразливостей використовують різні системи оцінки серйозності, що призводить до розбіжностей у рейтингах одних і тих самих вразливостей. Це створює труднощі для фахівців з безпеки при оцінці ризиків та визначенні пріоритетності виправлень. Тому було запропоновано фреймворк нормалізації, який об'єднує оцінки серйозності з різних VD, приводячи їх до єдиної шкали на основі обраного рівня забезпечення безпеки. Це дозволяє отримати узгоджену оцінку серйозності для кожної вразливості.

Основна мета нормалізації полягає в усуненні розбіжностей між різними базами даних вразливостей і їхніми системами оцінки серйозності. Для реалізації цього підходу використовуються числові оцінки CVSS Base Score (версії v2.0 та v3.x), які є базою для нормалізації. Також здійснюється конвертація якісних оцінок із баз DSA та USN у числові значення на основі стандартів CVSS, що забезпечує уніфікацію даних.

Нормалізація безпосередньо застосовується до CVSS, де версія v3.x використовується як еталон для конвертації якісних оцінок у числові значення. Це дозволяє забезпечити узгодженість показників серйозності для інтеграції у загальний фреймворк оцінки ризиків, що робить його більш адаптованим до потреб користувачів.

Етапи застосування нормалізації включають інтеграцію даних з різних баз VD, таких як NVD, USN і DSA. На етапі збору даних усі оцінки серйозності перетворюються до єдиного числового формату, що уніфікує подальшу обробку.

Після цього, на етапі оцінки ризиків, нормалізовані дані використовуються для створення уніфікованої матриці ризиків. Ця матриця дозволяє організувати оцінки серйозності вразливостей у вигляді категорій ризиків, забезпечуючи точнішу пріоритизацію виправлень і планування дій з усунення вразливостей.

Матриця базується на нормалізованих значеннях CVSS Base Score, які класифікуються за певними інтервалами залежно від обраного рівня Vulnerability Management Mode (VMM):

- Basic VMM: забезпечує мінімальний рівень безпеки, орієнтований на системи з обмеженим впливом загроз.
- Standard VMM: враховує середній рівень ризиків і підходить для систем із підвищеним рівнем загроз.
- Restrictive VMM: використовується для критичних систем, що потребують суворого дотримання нормативів і стандартів.

CVSS v3.x Score	Qualitative Rate	Basic VMM	Standard VMM	Restrictive VMM
0.0	None	0	0	0
0.1-3.9	Low	0.1	2	3.9
4.0-6.9	Medium	4.0	5.45	6.9
7.0-8.9	High	7.0	7.95	8.9
9.0-10.0	Critical	9.0	9.5	10.0

Рисунок 2.2 – Уніфікована матриця ризиків

Ця структура забезпечує узгоджену пріоритизацію, оскільки вразливості, незалежно від джерела даних, класифікуються та пріоритизуються відповідно до єдиних, чітко визначених критеріїв. Завдяки цьому фахівці з безпеки отримують стандартизований інструмент для оцінки серйозності вразливостей, що полегшує процес прийняття рішень про їх усунення.

Крім того, нормалізація дозволяє значно скоротити кількість вразливостей, що залишаються без оцінок ("Not Available"), навіть за умов різних рівнів Vulnerability Management Mode (VMM). Це забезпечує ширше охоплення вразливостей у складних середовищах, де неоднорідність даних із різних баз даних раніше створювала труднощі для повноцінного аналізу.

Результати застосування нормалізації показали значне покращення покриття оцінок CVE-ID. Наприклад, ідентифікатори, які залишалися без оцінки в базах USN чи DSA, отримали числові значення завдяки нормалізації. Це суттєво зменшило кількість необроблених CVE-ID навіть за умов різних рівнів "Vulnerability Management Mode" (Basic, Standard, Restrictive).

Нормалізація також покращила узгодженість даних і розподіл оцінок серйозності між CVE-ID у різних базах. Використання нормалізованих даних дозволило розширити покриття CVE-ID у складних хмарних середовищах, таких як IaaS. Таким чином, підтверджено, що використання кількох баз VD разом із нормалізацією забезпечує більш ефективну класифікацію та пріоритизацію виправлень, що є важливим для оптимізації процесів управління ризиками вразливостей.

У дослідженні "Defining and Assessing Quantitative Security Risk Measures Using Vulnerability Lifecycle and CVSS Metrics" розглядається проблема оцінки ризиків безпеки, пов’язаних із вразливостями програмного забезпечення, з акцентом на використання життєвого циклу вразливостей та метрик CVSS для кількісного аналізу [19]. Це дослідження було представлено на міжнародній конференції SAM'11, що об’єднує фахівців із комп’ютерної безпеки.

Вразливості, які залишаються невиправленими після виявлення, становлять значний ризик для організацій. Вони можуть бути експлуатовані навіть до публічного розкриття. Основна мета роботи полягає в розробці формальних кількісних методів оцінки ризиків, які дозволяють визначати пріоритетність виправлень і оптимізувати управління безпекою. Запропонований підхід поєднує формальні теоретичні моделі ризиків із практичними методами, які використовуються в галузі.

Розглядається концепція ризику, яка визначається як добуток ймовірності експлуатації вразливості та впливу цієї події. Для моделювання ризиків використовується стохастичний підхід, що враховує можливі стани в життєвому циклі вразливості: створення, виявлення, публічне розкриття, виправлення та експлуатація. Ймовірності переходу між станами моделюються за допомогою

Марковських процесів, що дозволяє оцінити ризик для окремих вразливостей та систем загалом.

Метрики CVSS, зокрема базові, використовуються для визначення ймовірності експлуатації та впливу вразливостей. Ці метрики нормалізуються, що дозволяє стандартизувати оцінки ризиків і порівнювати їх між різними системами. У цьому контексті дослідження використовує принципи, аналогічні методу Min-max, щоб забезпечити узгодженість оцінок ризиків у межах єдиного діапазону. Застосування такого підходу дозволяє легко порівнювати ризики між різними вразливостями чи системами, навіть якщо початкові дані мають різні діапазони значень. Нормалізація також забезпечує зручність у візуалізації даних та агрегуванні ризиків.

Запропонований підхід також дозволяє оцінювати ризик для невиправлених вразливостей, зокрема під час "вікон ризику" - періодів між публічним розкриттям і виправленням. Використовуючи симуляцію даних, дослідження демонструє, як ризик змінюється з часом для різних систем, таких як операційні системи чи браузери.

Результати показують, що запропонована методологія дозволяє не лише оцінити ризики для окремих систем, але й порівнювати ризики між альтернативними програмними рішеннями. Це сприяє оптимізації виправлень і прийняттю стратегічних рішень в організаціях. Для майбутніх досліджень рекомендовано вдосконалення методів оцінки швидкостей переходу між станами життєвого циклу та розробка більш точних моделей впливу.

У контексті спрощення інтерпретації отриманих результатів оцінки ризиків методологія оцінки ризиків OWASP демонструє свою ефективність завдяки структурованому підходу до ранжування ризиків залежно від їхньої серйозності. Ця методологія дозволяє розділяти ризики на чітко визначені категорії, такі як "Низький", "Середній", "Високий" і "Критичний" [20]. Подібна класифікація має велике значення для організацій, оскільки дає змогу швидко визначати пріоритети в управлінні безпекою. Завдяки цьому компанії можуть

спрямовувати свої зусилля та ресурси на найбільш серйозні загрози, зменшуючи потенційний вплив інцидентів і оптимізуючи процеси безпеки.

Методологія OWASP приділяє особливу увагу визначенню серйозності ризиків через аналіз їхніх складових. Вона інтегрує оцінку ймовірності того, що вразливість може бути експлуатована, та оцінку потенційного впливу такого інциденту. Такий підхід забезпечує прозорість і стандартизацію процесу оцінювання, що є важливим для організацій, які працюють у складних середовищах із великою кількістю вразливостей.

Ймовірність оцінюється за кількома критеріями, які охоплюють технічні й організаційні аспекти, зокрема:

- Рівень навичок зловмисника: Відсутність досвіду або висока майстерність.
- Мотив: Ступінь зацікавленості зловмисника.
- Можливості: Доступ до ресурсів і системи.
- Розмір групи загрози: Кількість потенційних зловмисників.
- Інші фактори, як-от складність експлуатації вразливості чи поширеність атак.

Ці фактори враховуються разом, що дає змогу об'єктивно оцінити ймовірність реалізації загрози. Важливим аспектом є те, що методологія дозволяє агрегувати ці оцінки, забезпечуючи стандартизований результат, який легко інтегрувати в загальну систему управління ризиками [21].

Іншим важливим компонентом оцінки є вплив потенційної атаки. Методологія OWASP враховує наступні аспекти:

- Втрату конфіденційності: Розкриття критичної інформації.
- Втрату цілісності: Модифікація або пошкодження даних.
- Втрату доступності: Порушення роботи систем.
- Фінансові збитки: Економічний вплив.
- Репутаційні втрати: Вплив на довіру до організації.
- Регуляторні порушення: Штрафи або санкції за недотримання нормативів.

Аналіз цих параметрів дозволяє організаціям оцінити, наскільки серйозними можуть бути наслідки успішної атаки.

Остаточна серйозність ризику визначається як добуток оцінок ймовірності та впливу. Цей результат використовується для класифікації ризиків у зазначені категорії, кожна з яких передбачає певні дії. Наприклад, "Критичні" ризики потребують негайного втручання, оскільки їхній потенційний вплив може бути катастрофічним. Для таких ризиків зазвичай розробляються оперативні плани дій із виправлення вразливості. Водночас "Середні" ризики можуть розглядатися у рамках планового усунення, тоді як "Низькі" ризики часто лише моніторяться, без негайного втручання.

Особливістю методології OWASP є її адаптивність. Вона дозволяє організаціям налаштовувати оцінку ризиків відповідно до власних бізнес-цілей і ресурсів. Наприклад, у критичних середовищах, таких як фінансові установи, можна використовувати більш суворі критерії оцінки. Водночас у середовищах із меншим рівнем загроз методологія дозволяє зосередитися на найбільш значущих ризиках, мінімізуючи витрати на безпеку.

OWASP також підкреслює важливість прозорості в оцінці ризиків. Використання чітких категорій і стандартів дозволяє забезпечити зрозуміле пояснення результатів не тільки для технічних фахівців, а й для нефахівців, таких як менеджери або керівники. Це сприяє ефективній комунікації всередині організації, забезпечуючи визначення пріоритетів і узгодженість дій.

Було розглянуто та проаналізовано різні підходи до оцінки ризиків, які ґрунтуються на стандартизованих показниках впливу та ймовірності експлуатації вразливостей. На основі аналізу наукових робіт, таких як "Normalization Framework for Vulnerability Risk Management in Cloud" та "Defining and Assessing Quantitative Security Risk Measures Using Vulnerability Lifecycle and CVSS Metrics", було визначено ключові переваги використання методу нормалізації для інтерпретації CVSS.

Метод ранжування був проаналізований, але не обраний як основний підхід для подальшого дослідження оцінки ризиків через низку обмежень, що впливають на точність і автоматизацію процесу. Одним із ключових недоліків є суб'єктивність результатів. Методи ранжування значною мірою залежать від

експертної оцінки, що може бути суб'єктивною та змінюватися залежно від контексту, досвіду фахівця або специфіки організації. У випадках великої кількості вразливостей це призводить до розбіжностей і неузгодженості пріоритетів [21].

Ще одним обмеженням є відсутність кількісної стандартизації, оскільки ранжування зазвичай оперує якісними показниками, такими як "високий", "середній" чи "низький". Це ускладнює їх інтеграцію у математичні моделі ризиків або автоматизовані системи, не дозволяючи точно порівнювати ризики між собою та застосовувати єдині формули для подальшого аналізу. Крім того, метод ранжування виявився неефективним для автоматизації, оскільки він потребує експертного втручання на кожному етапі, що значно ускладнює його інтеграцію в автоматизовані системи оцінки ризиків. У великих організаціях, де кількість вразливостей обчислюється тисячами, цей підхід є трудомістким і неефективним.

Недостатня гнучкість також є важливим обмеженням. Ранжування не враховує нюанси масштабування, коли ризики повинні бути адаптовані до конкретних умов середовища, як-от критичні системи або менш значущі сервіси. Відсутність єдиної числової шкали обмежує можливість гнучкої зміни інтервалів для конкретного рівня безпеки.

Для подолання цих обмежень необхідний підхід, який забезпечує стандартизоване та кількісне представлення оцінок ризиків. Аналіз показав, що нормалізація ефективно справляється з цими викликами, усуваючи неоднорідність даних та створюючи єдину основу для подальшого аналізу.

Нормалізація показників CVSS забезпечує уніфікацію оцінок ризиків шляхом приведення їх до єдиного діапазону значень. Це дозволяє уникнути неоднорідності даних, які надходять із різних баз вразливостей, зокрема NVD, USN та DSA. Такий підхід полегшує інтеграцію результатів і спрощує їх порівняння незалежно від джерела інформації.

Процес оцінювання ризиків стає стандартизованим завдяки методам, як Min-max нормалізація. Цей метод створює єдину кількісну шкалу, що сприяє

побудові уніфікованої матриці ризиків. Отримані значення легко інтерпретуються й застосовуються для прийняття обґрунтованих рішень.

Застосування нормалізації також розширює покриття вразливостей, мінімізуючи кількість випадків, коли відсутні числові оцінки (наприклад, CVE-ID зі статусом "Not Available"). Завдяки цьому навіть такі вразливості отримують числове значення на основі CVSS Base Score, що особливо корисно для організацій, які працюють у великих та хмарних середовищах.

Перевагою нормалізації є те, що нормалізовані значення можуть бути масштабовані на наступному етапі. Це дозволяє адаптувати їх до конкретних потреб організації або умов використання. Зокрема нормалізовані значення можуть бути використані для інтеграції у матрицю ризиків, що дозволяє чітко класифікувати вразливості за категоріями ризиків. Масштабування забезпечує ще більшу гнучкість у подальшій інтеграції результатів до систем управління ризиками та полегшує роботу фахівцям з безпеки завдяки їхній уніфікації та стандартизації.

Таким чином, метод нормалізації, який забезпечує числову стандартизацію показників, був обраний як основний завдяки його точності, можливості автоматизації та гнучкій адаптації до різних умов. Нормалізація мінімізує суб'єктивні фактори, дозволяє об'єднати дані з різних джерел і забезпечує єдину уніфіковану основу для кількісного аналізу та подальшої інтерпретації результатів.

2.3 Нормалізація як метод інтерпретації CVSS

Min-max нормалізація є базовим і ефективним методом попередньої обробки даних, що широко використовується у машинному навчанні, статистиці та аналізі даних. Її головна мета полягає у масштабуванні вихідних значень у заданий діапазон, найчастіше від 0 до 1 [22]. Такий підхід забезпечує коректний та пропорційний внесок усіх ознак у модель чи систему аналізу, незалежно від початкових масштабів їхніх значень.

Процес нормалізації реалізується за допомогою лінійного масштабування за формулою:

$$x' = \frac{x - \min(x)}{\max(x) - \min(x)} \quad (2.7)$$

Опис параметрів для нормалізації:

– x початкове значення, що підлягає нормалізації;
– x' нормалізоване значення;
– min(x) мінімальне значення показника у вибірці;
– max(x) максимальне значення показника у вибірці.

Нормалізація переводить усі значення у діапазон [0, 1], де мінімальні значення отримують значення, наближені до 0, а максимальні значення, наближені до 1. Це забезпечує пропорційний розподіл даних та полегшує їх подальшу обробку й аналіз у різних системах.

Цей метод ефективно вирішує проблеми, пов'язані з різними масштабами числових ознак. Без нормалізації показники з більшими діапазонами можуть некоректно впливати на результати аналізу та знижувати точність моделей.

У контексті CVSS (Common Vulnerability Scoring System) метод Min-max нормалізації є важливим інструментом для стандартизації та інтерпретації показників Exploitability Score та Impact Score, оскільки початкові значення цих показників можуть значно відрізнятися залежно від систем або джерел даних. Щоб привести значення Exploitability Score та Impact Score до єдиного діапазону для забезпечення узгодженого порівняння, використовуються наступні формули:

$$Normalized\ Exploitability = \frac{Exploitability\ Score - Min}{Max - Min} \quad (2.8)$$

$$Normalized\ Impact = \frac{Impact\ Score - Min}{Max - Min} \quad (2.9)$$

Значення Min та Max у цьому контексті позначають граничні значення, що відповідають мінімальним та максимальним можливим показникам, які використовуються для нормалізації даних. Формули для їх розрахунку ґрунтуються на підходах до максимізації впливу ключових факторів, визначених у CVSS (Common Vulnerability Scoring System).

Для Exploitability мінімізація досягається шляхом підстановки найнижчих можливих значень для всіх параметрів. У цьому випадку значення будуть відрізнятися залежно від Scope Unchanged та Scope Changed, оскільки для зміненого Scope коригується коефіцієнт Privileges Required.

Для Scope Unchanged використовуються наступні мінімальні значення:

- Attack Vector: Physical = 0.2
- Attack Complexity: High = 0.44
- Privileges Required: High = 0.27
- User Interaction: Required = 0.62

Підставивши ці значення у формулу (2.6), отримаємо мінімальне значення Exploitability для Scope Unchanged:

$$Exploitability_{min,unchanged} = 8.22 \times 0.2 \times 0.44 \times 0.27 \times 0.62$$

$$Exploitability_{min,unchanged} = 0.1210$$

Для Scope Changed відбувається зміна коефіцієнта Privileges Required, оскільки для зміненого Scope значення High підвищується до 0.5. Інші параметри залишаються незмінними:

- Attack Vector: Physical = 0.2
- Attack Complexity: High = 0.44
- Privileges Required (Scope Changed): High = 0.5
- User Interaction: Required = 0.62

Підставивши ці значення у формулу(2.6), отримаємо:

$$Exploitability_{min,changed} = 8.22 \times 0.2 \times 0.44 \times 0.5 \times 0.62$$
$$Exploitability_{min,changed} = 0.2242$$

Таким чином, для мінімізації показника Exploitability значення залежать від обраного Scope. Для Scope Unchanged мінімальне значення становить 0.1210, а для Scope Changed 0.2242. Ці розрахунки показують різницю у впливі параметра Privileges Required.

Максимізація досягається шляхом підстановки найвищих можливих значень для всіх параметрів, що дає однаковий результат як для Scope Unchanged, так і для Scope Changed.

Максимальні коефіцієнти є наступними:

- Attack Vector: Network = 0.85
- Attack Complexity: Low = 0.77
- Privileges Required: None = 0.85
- User Interaction: None = 0.85

Підставивши ці значення у формулу (2.6), отримуємо максимальне значення Exploitability:

$$Exploitability_{max} = 8.22 \times 0.85 \times 0.77 \times 0.85 \times 0.85$$
$$Exploitability_{max} = 3.8870$$

Отже, максимальне значення Exploitability становить приблизно 3.8870. Це значення є однаковим для Scope Unchanged та Scope Changed, оскільки всі параметри приймають свої найвищі значення, а коефіцієнт Privileges Required для обох випадків максимізується як None = 0.85.

Для Impact мінімальне значення обчислюється за умови, що хоча б один із показників впливу конфіденційність, цілісність або доступність має значення Low = 0.22, тоді як два інших показники дорівнюють None = 0.0. У такому випадку рівень впливу є мінімально підвищеним, що дозволяє отримати нижню межу значення Impact.

Розрахунок мінімального Impact для Scope Unchanged ґрунтується на використанні проміжного показника ISCBase. Розглянемо випадок, коли ImpactConf = 0.22 (Low), а ImpactInteg і ImpactAvail дорівнюють 0.0 (None). Підставивши ці значення у формулу (2.3), отримаємо:

$$ISCBase = 1 - ((1 - 0.22) \times (1 - 0.0) \times (1 - 0.0))$$
$$ISCBase = 1 - (0.78 \times 1 \times 1)$$
$$ISCBase = 0.22$$

Тепер для Scope Unchanged застосовується формула (2.4):

$$Impact_{min,unchanged} = 6.42 \times 0.22$$
$$Impact_{min,unchanged} = 1.4124$$

Таким чином, мінімальне значення Impact для Scope Unchanged становить 1.4124.

Для Scope Changed розрахунок мінімального Impact враховує додаткові коефіцієнти й виконується за розширеною формулою (2.5). Підставимо значення ISCBase = 0.22 у формулу:

$$Impact_{min,changed} = 7.52 \times (0.22 - 0.029) - 3.25 \times$$
$$\times (0.22 - 0.02)^{15}$$
$$Impact_{min,changed} = 1.4363$$

Отже, мінімальне значення Impact для Scope Unchanged становить 1.4124, а для Scope Changed 1.4363.Розрахунки демонструють незначне підвищення значення Impact у випадку зміни області впливу, що пов’язано з додатковими коригувальними коефіцієнтами у формулі для Scope Changed.

Максимальне значення обчислюється шляхом встановлення найвищих можливих значень для всіх трьох компонентів впливу. Згідно зі стандартами CVSS v3.0, значення High = 0.56 є максимальним для кожного з цих показників.

Для Scope Unchanged розрахунок виконується на основі базової формули Impact (2.3). Підставимо максимальні значення для всіх трьох компонентів впливу:

$$ISCBase = 1 - ((1 - 0.56) \times (1 - 0.56) \times (1 - 0.56))$$
$$ISCBase = 0.9148$$

Тепер підставимо значення ISCBase у формулу (2.4):

$$Impact_{max,unchanged} = 6.42 \times 0.9148$$
$$Impact_{max,unchanged} = 5.8731$$

Для Scope Changed використовується розширена формула, що враховує додаткові коригувальні коефіцієнти. Оскільки значення ISCBase вже обчислене і дорівнює 0.9148, підставимо його у формулу (2.5):

$$Impact_{max,changed} = 7.52 \times (0.9148 - 0.029) - 3.25 \times$$
$$\times (0.9148 - 0.02)^{15}$$
$$Impact_{max,changed} = 6.0477$$

Отже, максимальні значення Impact для Scope Unchanged та Scope Changed демонструють вплив вразливостей на систему у двох різних контекстах:

Для Scope Unchanged максимальне значення становить 5.8731.

Для Scope Changed максимальне значення становить 6.0477.

Ці розрахунки дозволяють об'єктивно оцінити вплив вразливостей залежно від контексту та підготувати дані для подальшої нормалізації.

РОЗДІЛ 3 ІНТЕРПРЕТАЦІЯ CVSS ЯК МЕТОДУ ДЛЯ ОЦІНКИ РИЗИКІВ

3.1 Вхідні дані

Об'єктом дослідження є компанія, яка працює в галузі розробки вебсайтів і маркетингових послуг для інших компаній. Діапазон її співробітників складає від 50 до 100 працівників.

Інфраструктура компанії включає локальну мережу, веб-додатки та сервери, які забезпечують функціонування основних бізнес-процесів.

У зв’язку з умовами угоди про нерозголошення інформації (NDA), деталі щодо ідентифікації компанії та її інфраструктури не розголошуються.

Будемо розглядати такі дані як:

– Вразливості, які були виявлені в цій компанії.
– Матриця ризиків, яку використовує компанія.
– Оцінка вразливостей експерта з ризиків.

3.1.1 Вразливості

У ході оцінювання безпеки було виявлено та проаналізовано низку вразливостей, пов’язаних як із застарілими компонентами інфраструктури, так і з конфігураційними недоліками. Ці вразливості охоплюють різні сервіси та протоколи, що використовуються в мережі компанії. Нижче подано розширені назви цих виявлених вразливостей разом із їхнім українським перекладом, оцінкою та вектором CVSS.

Нижче наведено перелік цих вразливостей:

– Unsupported Microsoft Windows Operating System (Непідтримувана операційна система Microsoft Windows).
– Microsoft RDP (Remote Desktop Protocol) Remote Code Execution (RCE) (Віддалене виконання коду через протокол віддаленого робочого столу Microsoft RDP).

- Microsoft Windows Server Service Remote Code Execution (MS08-067) (Віддалене виконання коду у службі серверу Microsoft Windows (MS08-067)).
- Default Password for 'admin' Account (Пароль за замовчуванням для облікового запису 'admin').
- OpenSSH Multiple Vulnerabilities (Множинні вразливості в OpenSSH).
- SSL Version 2 and 3 Protocol Detection (Виявлення використання протоколу SSL версій 2 та 3).
- Apache Multiple Vulnerabilities (Множинні вразливості в Apache).
- OpenSSL Multiple Vulnerabilities (Множинні вразливості в OpenSSL).
- Microsoft Windows SMB Server Vulnerability (MS17-010) (Вразливість SMB-сервера Microsoft Windows (MS17-010)).
- OpenSSL Heartbeat Information Disclosure (Heartbleed) (Розголошення інформації через Heartbeat у OpenSSL (Heartbleed)).
- IPMI v2.0 Password Hash Disclosure (Розголошення хешів паролів у IPMI v2.0).
- SMB NULL Session Authentication (Аутентифікація SMB з нульовою сесією).
- SSH Protocol Version 1 Session Key Retrieval (Отримання ключа сесії для протоколу SSH версії 1).
- TLS Version 1.0 Protocol Detection (Виявлення використання протоколу TLS версії 1.0).
- TLS Version 1.1 Protocol Detection (Виявлення використання протоколу TLS версії 1.1).
- Unencrypted Telnet Server (Незашифрований Telnet-сервер).
- JQuery Multiple XSS (Множинні XSS-вразливості в JQuery).
- SSH Terrapin Prefix Truncation Weakness (Слабкість усічення префіксу в SSH Terrapin).
- SMB Signing not required (SMB-підписання не вимагається).

- SSH Weak Key Exchange Algorithms Enabled (Увімкнено слабкі алгоритми обміну ключами SSH).
- SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) (Модуль Diffie-Hellman для SSL/TLS ≤1024 біти (Logjam)).
- SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE) (Вразливість Padding Oracle у SSLv3 при пониженні шифрування (POODLE)).

Під час проведення оцінки вразливостей (Vulnerability Assessment) було ідентифіковано та верифіковано 22 уразливості з відповідними оцінками за системою CVSS. Ці вразливості пройшли ретельну перевірку, в тому числі з використанням ручного аналізу, що підтвердило їх актуальність і реальний вплив. Оцінки CVSS були присвоєні з урахуванням методик та експертизи спеціаліста, який проводив тестування, що забезпечує точність і відповідність прийнятим стандартам оцінки ризиків.

У таблиці представлено перелік виявлених вразливостей, що включає назву кожної вразливості, оцінку її критичності за стандартом CVSS та відповідний вектор атаки. Назва вразливості дає змогу легко ідентифікувати проблему в інфраструктурі, тоді як оцінка CVSS відображає загальний рівень ризику, який вона створює. Вектор атаки деталізує умови експлуатації вразливості, такі як спосіб доступу, складність атаки, необхідність взаємодії з користувачем, а також вплив на конфіденційність, цілісність і доступність даних.

Ці дані будуть використані для застосування розробленого алгоритму, який базується на аналізі векторів атак. Вектори атак слугуватимуть вхідними параметрами для інтеграції метрик CVSS до корпоративної матриці ризиків.

Таблиця 3.1 – Виявлені вразливості із зазначенням оцінки CVSS та векторів

Name	Score	Vector
Unsupported Windows OS	9.8	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Продовження таблиці 3.1

Name	Score	Vector
Microsoft RDP RCE (CVE-2019-0708) (BlueKeep)	9.8	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Default Password (admin)	9.8	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
MS08-067	8.1	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
MS17-010	8.1	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
OpenSSL Heartbeat (Heartbleed)	7.5	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
IPMI v2.0 Password Hash Disclosure	7.5	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
SMB NULL Session Authentication	7.3	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
Unencrypted Telnet Server	7.3	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
OpenSSH Multiple Vulnerabilities	7.0	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L
SSL Version 2 and 3 Protocol Detection	6.4	AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L
JQuery 1.2 < 3.5.0 Multiple XSS	6.1	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
TLS Version 1.0 Protocol Detection	5.9	AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N
TLS Version 1.1 Protocol Detection	5.9	AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N
SSH Terrapin Prefix Truncation Weakness	5.9	AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N
Apache Multiple Vulnerabilities	5.6	AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L
OpenSSL Multiple Vulnerabilities	5.6	AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L

Продовження таблиці 3.1

Name	Score	Vector
SSH Protocol Version 1 Key Retrieval	5.6	AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L
SMB Signing not required	5.3	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
SSH Weak Key Exchange Algorithms Enabled	3.7	AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	3.7	AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N
SSLv3 Padding Oracle (POODLE)	3.0	AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N

3.1.2 Матриця ризиків

Наведена матриця на рисунку 3.1 використовується якісна матриця ризиків 5×5 для оцінки вразливостей та управління вразливостями у діяльності об’єкта дослідження. Вона побудована на двох основних складових: ймовірності (Probability) та впливу (Impact). Поєднання цих параметрів дозволяє визначити початковий рівень загроз для подальшого аналізу, зокрема оцінки залишкових ризиків після врахування засобів захисту.

Risk Matrix		Impact				
		Insignificant	Minor	Moderate	Major	Severe
Likelihood	Very Likely	Medium	Significant	High	Critical	Critical
	Likely	Low	Medium	Significant	High	Critical
	Possible	Low	Medium	Significant	High	High
	Unlikely	Low	Medium	Medium	Significant	High
	Rare	Low	Low	Medium	Significant	Significant

Рисунок 3.1 – Гібридна матриця ризиків 5×5

Для більш чіткого розуміння логіки функціонування матриці доцільно виокремити три ключові групи показників: компоненти вірогідності, компоненти впливу та оцінку ступеня ризику. Саме завдяки цим трьом складовим можливо систематизовано і послідовно оцінювати початкові ризики.

Матриця використовує якісні категорії для ймовірності настання подій (Rare, Unlikely, Possible, Likely, Very Likely). Аналогічно, вплив (Impact) описується за допомогою лексичних означень (Insignificant, Minor, Moderate, Major, Severe).

Матриця містить якісну градацію кінцевої оцінки ризику: від Low (низький) до Critical (критичний). Ці категорії є якісними показниками, оскільки не спираються на точні числові значення, а відображають загальний рівень небезпеки та терміновість реагування. Такий підхід полегшує інтерпретацію результатів, адже оперувати чітко сформульованими рівнями ризику значно простіше для різних груп користувачів — від аналітиків до керівників.

Передусім увага зосереджується на ймовірності (Probability), адже саме цей показник допомагає визначити частоту, з якою може виникати та чи інша подія. Застосовуючи різні категорії ймовірності, від рідкісної до майже неминучої, організація отримує орієнтири, які дозволяють зрозуміти рівень невизначеності майбутніх ситуацій. Чим вищою є ймовірність, тим більш цілеспрямованих і наполегливих дій потребує система управління ризиками, спрямовуючи ресурси та увагу на мінімізацію негативних наслідків або повне уникнення небажаних подій. Нижче наведено градацію рівнів ймовірності:

- Rare (Рідкісна) – подія з дуже низькою ймовірністю настання.
- Unlikely (Малоймовірна) – подія, що здебільшого не відбудеться.
- Possible (Ймовірна) – подія зі середнім шансом настання.
- Likely (Вірогідна) – подія з високою ймовірністю реалізації.
- Very Likely (Дуже Ймовірна) – подія, яка майже напевно станеться.

Наступним аспектом аналізу є вплив (Impact), що оцінює негативні наслідки, котрі може спричинити певний ризик. Цей показник розкриває масштаб потенційних втрат чи дестабілізацію процесів компанії. Важливо враховувати не лише безпосередній ефект однієї події, але й можливе накопичення її наслідків у довгостроковій перспективі. Саме завдяки цій оцінці стає зрозуміло, які ресурси необхідні для протидії ризику й наскільки суттєвими мають бути управлінські заходи. Нижче наведено градацію рівнів впливу залежно від можливих збитків:

- Insignificant (Мізерний) – мінімальний вплив, практично непомітний для основних процесів.
- Minor (Незначний) – вплив, що відчутний, але не є критичним для загальної діяльності.
- Moderate (Помірний) – помітний вплив, що може вимагати коригування ресурсів або додаткових заходів.
- Major (Значний) – істотний негативний вплив, який може перешкоджати досягненню стратегічних цілей та потребує термінових управлінських рішень.

– Severe (Критичний) – надзвичайно сильний вплив із потенційно тривалими негативними наслідками та значними збитками.

Зрештою, поєднання оцінок ймовірності та впливу формує загальний ступінь ризику (Risk Rating). Він відображає комплексну оцінку загрози. Чітко означені категорії від низького до критичного дозволяють аналітикам та керівництву легше орієнтуватися у ризиковому середовищі, своєчасно коригувати внутрішні процеси та впроваджувати антикризові стратегії. Нижче наведено узагальнені підходи та конкретні кроки реагування для кожного рівня ризику, починаючи з найменшого до найвищого. Такий підхід забезпечує чітку регламентацію дій, підвищуючи ефективність процесу управління ризиками та мінімізуючи можливі негативні наслідки.

Low (Низький) – рівень ризику настільки незначний, що його вплив на діяльність організації є мінімальним. Такий ризик не здатний суттєво змінити робочі процеси, тому не потребує активного втручання чи додаткових ресурсів. Достатньо зрідка відстежувати стан справ і, у разі виявлення легко усуваних вразливостей, вживати відповідних заходів. Підсумовуючи це у конкретні рекомендовані дії, на даному рівні потрібно:

– Здійснювати нечастий моніторинг (раз на рік), щоб упевнитися у стабільності ризикового профілю.
– Дотримуватися наявних внутрішніх процедур без коригувань, оскільки потреби у зміні процесів немає.
– Якщо існує проста та недорога можливість усунути вразливість одразу, зробити це без зволікань.

Medium (Середній) – ризик є помірним і може викликати певні, але не значні наслідки. На цьому етапі ймовірність погіршення ситуації зростає, тому варто здійснювати частіший моніторинг і наперед визначити шляхи реагування. Якщо можливо швидко та економічно доцільно знизити ризик до низького рівня, це слід зробити одразу. Підсумовуючи це у конкретні рекомендовані дії, на даному рівні потрібно:

– Проводити більш частий моніторинг (двічі на рік).

- Розробити план заходів із чіткими строками, визначеними ресурсами та відповідальними особами на випадок погіршення ситуації.
- Якщо можна швидко та недорого зменшити рівень ризику, варто реалізувати превентивні заходи негайно.

Significant (Значний) – ризик вищий за помірний, але ще не сягає того рівня негативного впливу, що притаманний "High". У такій ситуації є реальна ймовірність суттєво ускладнити роботу організації в короткостроковій перспективі, тому потрібна активніша протидія, іноді навіть оперативна зміна внутрішніх процедур чи перерозподіл ресурсів. Підсумовуючи це у конкретні рекомендовані дії, на даному рівні потрібно:

- Посилений моніторинг: відстежувати стан справ щоквартalу або частіше, якщо ризик швидко зростає.
- Оперативне реагування: визначити критичні точки у процесах та посилити їх (додатковий персонал, розширення бюджетів тощо).
- Коригування внутрішніх регламентів: оновити деякі процедури, аби зменшити ймовірність негативних наслідків.
- Запобігання ескалації: створити “план В” із чітким розподілом ресурсів, щоб уникнути подальшого погіршення ситуації.

High (Високий) – ризик може суттєво вплинути на важливі аспекти діяльності організації, через що необхідно діяти негайно. Зволікання або недостатні заходи можуть призвести до серйозного збою у функціонуванні ключових напрямів. Підсумовуючи це у конкретні рекомендовані дії, на даному рівні потрібно:

- Негайно впровадити визначені заходи з мінімізації впливу ризику (посилити контроль, вдосконалити окремі процедури).
- Переглянути та вдосконалити внутрішні регламенти, щоб краще відповідати новим умовам.
- Забезпечити готовність до невідкладного реагування, визначивши умови переходу до кризового плану та наявність потрібних ресурсів.

– Налагодити ефективну комунікацію між усіма підрозділами для оперативного обміну інформацією та координації дій.

Critical (Критичний) – ризик перебуває на максимальному рівні загрози та безпосередньо ставить під сумнів стабільне функціонування організації. Вкрай важливо негайно перейти до невідкладних дій, залучити керівництво вищого рівня, скерувати додаткові ресурси та інформувати зацікавлені сторони щодо плану реагування. Підсумовуючи це у конкретні рекомендовані дії, на даному рівні потрібно:

– Негайно активувати план невідкладного реагування і суворо дотримуватися його положень.
– Залучити вище керівництво до ухвалення оперативних рішень у режимі реального часу.
– Швидко перерозподілити ресурси (персонал, технічні засоби, фінанси) на усунення або мінімізацію загроз.
– Забезпечити оперативну комунікацію з усіма зацікавленими сторонами, попереджаючи можливі негативні інформаційні ефекти.

Таким чином, послідовна і чітко визначена система дій для кожного рівня ризику не лише дає змогу ефективно розподіляти ресурси та прискорювати ухвалення управлінських рішень, а й створює передумови для належного планування, своєчасного запровадження превентивних заходів, оперативного реагування на зміни ситуації та мінімізації негативних наслідків. Це, у свою чергу, сприяє підвищенню загальної стійкості організації, здатності адаптуватися до нових викликів та підтримувати стабільну діяльності у довгостроковій перспективі.

Для зручності всі дані були перенесені в таблицю, щоб вони виглядали структуровано і були легшими для сприйняття. Це допомагає швидко знайти необхідну інформацію та краще організувати її для подальшого використання.

Табличний формат дозволяє зменшити кількість помилок під час аналізу, полегшує порівняння параметрів між собою та забезпечує наочність отриманих результатів.

Таблиця 3.2 – Виявлені вразливості із зазначенням оцінки CVSS та векторів

Рівень ризику	Пріоритет	Рекомендовані дії	Терміни реалізації та перевірок
Critical (Критичний)	1	- Негайно активувати план невідкладного реагування і суворо дотримуватися його положень. - Залучити вище керівництво для ухвалення рішень у режимі реального часу. - Швидко перерозподілити ресурси (персонал, фінанси, обладнання) для усунення або мінімізації загроз. - Забезпечити оперативну комунікацію із зацікавленими сторонами.	Immediate (Негайно)
High (Високий)	2	- Негайно впровадити заходи з мінімізації впливу (посилити контроль, удосконалити процедури). - Переглянути та вдосконалити внутрішні регламенти для адаптації до актуальних умов. - Підготуватися до оперативного реагування: визначити умови переходу до кризового плану та потрібні ресурси. - Налагодити ефективну комунікацію між усіма підрозділами.	Immediate (Негайно)
Significant (Значний)	3	- Посилений моніторинг: відстежувати стан справ щокварталу чи частіше. - Оперативне реагування: визначити критичні точки та підсилити їх (додаткові ресурси, збільшений бюджет тощо). - Коригування регламентів: оновити процедури для зменшення ймовірності негативних наслідків. - План В: забезпечити чіткий розподіл ресурсів для запобігання ескалації.	Quarterly (Щоквартально)
Medium (Середній)	4	- Проводити моніторинг двічі на рік (за необхідності частіше). - Розробити план заходів із визначеними ресурсами та строками на випадок погіршення ситуації. - Якщо можна швидко та недорого знизити ризик, реалізувати превентивні заходи негайно.	Twice a year (Двічі на рік)
Low (Низький)	5	- Здійснювати нечастий моніторинг (раз на рік). - Дотримуватися наявних процедур без суттєвих змін. - Якщо є проста й недорога можливість усунути вразливість, зробити це одразу.	Annually (Щорічно)

3.1.3 Оцінка вразливостей експерта з ризиків

Виявлення та оцінка ризиків є одним із ключових етапів процесу управління інформаційною безпекою компанії. Саме цей етап дозволяє сформувати цілісну картину потенційних загроз, визначити їхній вплив на бізнес-процеси та забезпечити ефективну пріоритизацію заходів із захисту. У цьому розділі розглядається результати роботи спеціаліста, який здійснив аналіз наявних активів, вразливостей та можливих сценаріїв атак, застосовуючи загальноприйняті принципи оцінювання ризиків.

Фахівець розпочав із перевірки вже наявного переліку активів компанії й оновлення інформації про їхню важливість у поточних бізнес-процесах. Цей етап не вимагав масштабного дослідження, оскільки детальна інвентаризація систем та їхньої критичності для діяльності була виконана раніше. Тож спеціаліст лише переконався, що жодні нові сервери чи підсистеми не з’явилися після попереднього аудиту, а також перевірив актуальність доступних методів резервного копіювання та захисту.

На першому етапі експерт розрахував початкові ризики, враховуючи ймовірність реалізації загроз і їхній потенційний вплив на конфіденційність, цілісність і доступність (CIA) інформаційних активів. Узагальнених даних про можливі вразливості вистачало, оскільки компанія періодично проводить базове сканування безпеки й отримує повідомлення про відомі недоліки від іншої компанії з кібербезпеки, послугами якої вони користуються.

Після цього було здійснено сортування: виявлені загрози згрупували за рівнем потенційного впливу на бізнес та ймовірністю їхньої реалізації. У результаті було сформовано остаточний перелік вразливостей, кожна з яких прив’язувалася до конкретного активу, що міг постраждати. Далі фахівець використав внутрішню матрицю оцінювання, щоб дати інтегральну оцінку кожній вразливості за двома ключовими характеристиками: ймовірністю експлуатації та впливом на бізнес-процеси. Внесення цих даних у матрицю

дозволило отримати чітке уявлення про початкові ризики, що забезпечило кращу структуризацію інформації для подальшого аналізу.

Ця інформація стала основою для етапу обчислення залишкових ризиків. Під час цього етапу до кожної вразливості додавалася оцінка грошового впливу та враховувалися існуючі засоби захисту. Завдяки цьому було визначено, які ризики залишаються після впровадження поточних заходів безпеки, а також пріоритети для усунення найбільш критичних із них.

Незважаючи на те, що робота з початковими ризиками була проведена максимально ефективно з точки зору витраченого часу, завдяки значному досвіду фахівця у роботі з активами компанії та її інструментами, загалом спеціаліст витратив близько 70 робочих годин, щоб завершити весь процес. У підсумку було враховано 22 ідентифіковані вразливості.

Якщо припустити, що кожна з них вимагала однакового обсягу досліджень і перевірок, то орієнтовно виходить приблизно 3 години на одну вразливість. Такий показник охоплює як аналіз загрози, так і внесення відповідної інформації до загальної матриці ризиків. Цей підхід до оцінки виявився достатньо точним, щоб прийняти обґрунтовані рішення щодо посилення безпеки інфраструктури та оптимізації витрат ресурсів.

На рисунку 3.2 представлено підсумкові результати оцінки початкових ризиків, виконані спеціалістом на основі аналізу знайдених загроз та їхньої прив’язки до бізнес-активів. Зображення ілюструє рівні критичності вразливостей, визначені з урахуванням ймовірності їхньої експлуатації та ступеня потенційного впливу.

ЕКСПЕРТ			
Vulnerability	**Likelihood**	**Impact**	**Risk Rating**
Unsupported Windows OS	Very Likely	Severe	Critical
RDP (BlueKeep)	Very Likely	Severe	Critical
MS08-067	Likely	Major	High
Default Password (admin)	Very Likely	Severe	Critical
OpenSSH Multiple Vulns	Possible	Major	High
SSL v2/v3	Likely	Moderate	Significant
OpenSSH Multiple Vulns	Possible	Moderate	Significant
OpenSSL Multiple Vulns	Very Likely	Moderate	High
MS17-010 (EternalBlue)	Possible	Severe	High
OpenSSL Heartbleed	Very Likely	Moderate	High
IPMI v2.0 Hash Disclosure	Possible	Major	High
SMB NULL Session	Very Likely	Moderate	High
SSH v1 Key Retrieval	Possible	Moderate	Significant
TLS 1.0 Detection	Likely	Minor	Medium
TLS 1.1 Detection	Likely	Minor	Medium
Unencrypted Telnet	Possible	Major	High
JQuery XSS	Likely	Moderate	Medium
SSH Terrapin Weakness	Possible	Moderate	Significant
SMB Signing not required	Very Likely	Insignificant	Medium
SSH Weak Key Exchange Algs	Possible	Insignificant	Low
SSL/TLS DH ≤ 1024 Bits (Logjam)	Possible	Insignificant	Low
SSLv3 Padding Oracle (POODLE)	Possible	Insignificant	Low

Рисунок 3.2 – Результати оцінки початкових ризиків експертом

3.2. Розробка алгоритму

Для оцінки та інтерпретації початкових ризиків на основі вразливостей пропонується алгоритм, який включає нормалізацію даних, масштабування показників та їх подальшу інтеграцію у матрицю ризиків, представлену на основі ймовірності та впливу.

На першому етапі проводиться нормалізація показників Exploitability та Impact методом Min-max. Нормалізовані значення дозволяють стандартизувати різні вхідні дані для подальшого використання. Для розрахунків будуть використовуватись формули 2.8 та 2.9, які забезпечують збереження пропорційності між показниками, необхідними для об’єктивного аналізу критичності вразливостей.

На другому етапі значення Exploitability та Impact масштабуються до діапазону [1, 5] за допомогою лінійного масштабування. Це дозволяє перевести нормалізовані значення у формат, зручний для інтеграції у матрицю ризиків:

$$Scaled\ Exploitability = Normalized\ Exploitability \times (5 - 1) + 1$$
$$Scaled\ Impact = Normalized\ Impact \times (5 - 1) + 1$$

На третьому етапі масштабовані показники інтегруються у матрицю ризиків для визначення остаточного рівня загрози.

Для візуального представлення процесу алгоритму наведено блок-схему, яка ілюструє послідовність етапів.

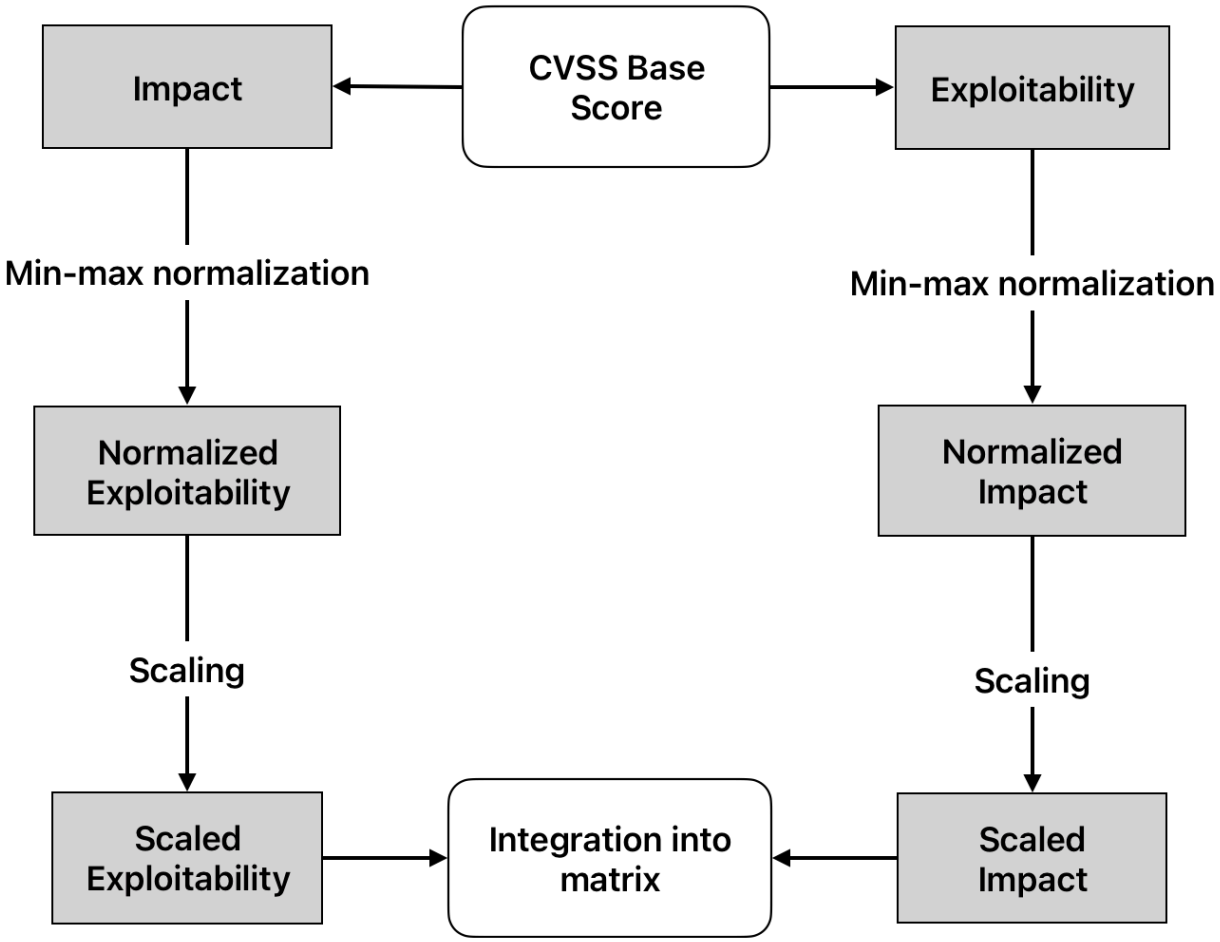

Рисунок 3.3 – Блок-схема алгоритму оцінки та інтерпретації початкових ризиків

Розроблений алгоритм буде застосований у практичній частині для демонстрації його ефективності та перевірки на даних компанії. Це дозволить оцінити практичну доцільність кожного етапу, від нормалізації до інтеграції у матрицю початкових ризиків.

3.3. Застосування та результати алгоритму

Розроблений алгоритм застосовано у практичній частині для демонстрації його ефективності та перевірки на даних компанії. Це дозволяє оцінити практичну доцільність кожного етапу, від нормалізації до інтеграції у матрицю ризиків. На прикладі п’яти вразливостей із різними CVSS-оцінками детально продемонстровано послідовність розрахунків та остаточні значення показників Exploitability й Impact, а також результати нормалізації і масштабування, завдяки чому кожну вразливість було інтегровано у матрицю і визначено підсумковий рівень початкового ризику.

Таблиця 3.3 – Розрахунок для Unsupported Microsoft Windows Operating System

Unsupported Microsoft Windows Operating System	
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	
Exploitability	$8.22 \times 0.85 \times 0.77 \times 0.85 \times 0.85 = 3.887$
ISCBase	$1 - (1 - 0.56) \times (1 - 0.56) \times (1 - 0.56) = 0.9148$
Impact	$6.42 \times 0.9148 = 5.8731$
Normalized Exploitability	$\frac{3.887 - 0.121}{3.887 - 0.121} = 1.0$
Normalized Impact	$\frac{5.8731 - 1.4124}{5.8731 - 1.4124} = 1.0$
Scaled Exploitability	$1.0 \times (5 - 1) + 1 = 5.0$
Scaled Impact	$1.0 \times (5 - 1) + 1 = 5.0$

На підставі максимальних значень показників рівень ризику класифіковано як “Critical”.

Таблиця 3.4– Розрахунок для MS08-067

MS08-067	
CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	
Exploitability	$8.22 \times 0.85 \times 0.44 \times 0.85 \times 0.85 = 2.2212$
ISCBase	$1 - (1 - 0.56) \times (1 - 0.56) \times (1 - 0.56) = 0.9148$
Impact	$6.42 \times 0.9148 = 5.8731$
Normalized Exploitability	$\frac{2.2212 - 0.121}{3.887 - 0.121} = 0.5577$
Normalized Impact	$\frac{5.8731 - 1.4124}{5.8731 - 1.4124} = 1.0$
Scaled Exploitability	$0.5577 \times (5 - 1) + 1 = 3.2307$
Scaled Impact	$1.0 \times (5 - 1) + 1 = 5.0$

З урахуванням високих значень рівень ризику для MS08-067 визначено як “High”.

Таблиця 3.5 – Розрахунок для SSL Version 2 and 3 Protocol Detection

SSL Version 2 and 3 Protocol Detection	
CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L	
Exploitability	$8.22 \times 0.62 \times 0.44 \times 0.85 \times 0.85 = 1.6201$
ISCBase	$1 - (1 - 0.56) \times (1 - 0.22) \times (1 - 0.22) = 0.7323$
Impact	$6.42 \times 0.7323 = 4.7014$
Normalized Exploitability	$\frac{1.6201 - 0.121}{3.887 - 0.121} = 0.3981$
Normalized Impact	$\frac{4.7014 - 1.4124}{5.8731 - 1.4124} = 0.7373$
Scaled Exploitability	$0.3981 \times (5 - 1) + 1 = 2.5923$
Scaled Impact	$0.7373 \times (5 - 1) + 1 = 3.9493$

Спираючись на співвідношення ймовірності експлуатації та впливу, рівень ризику для SSL Version 2 and 3 Protocol Detection класифіковано як Significant: він перевищує середній рівень, але не досягає критичної небезпеки, характерної для категорії "High".

Таблиця 3.6 – Розрахунок для JQuery 1.2 < 3.5.0 Multiple XSS

JQuery 1.2 < 3.5.0 Multiple XSS	
CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N	
Exploitability	$8.22 \times 0.85 \times 0.77 \times 0.85 \times 0.62 = 2.8353$
ISCBase	$1 - (1 - 0.22) \times (1 - 0.22) \times (1 - 0.0) = 0.3916$
Impact	$7.52 \times (0.3916 - 0.029) - 3.25 \times (0.3916 - 0.02)^{15} = 2.7268$
Normalized Exploitability	$\frac{2.8353 - 0.2242}{3.887 - 0.2242} = 0.7129$
Normalized Impact	$\frac{2.7268 - 1.4363}{6.0477 - 1.4363} = 0.2798$
Scaled Exploitability	$0.7129 \times (5 - 1) + 1 = 3.8514$
Scaled Impact	$0.2798 \times (5 - 1) + 1 = 2.1194$

На основі середніх значень відповідних показників рівень ризику для JQuery 1.2 < 3.5.0 Multiple XSS було класифіковано як "Medium".

Таблиця 3.7 – SSH Weak Key Exchange Algorithms Enabled

SSH Weak Key Exchange Algorithms Enabled	
CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N	
Exploitability	$8.22 \times 0.85 \times 0.44 \times 0.85 \times 0.85 = 2.2212$
ISCBase	$1 - (1 - 0.22) \times (1 - 0.0) \times (1 - 0.0) = 0.22$
Impact	$6.42 \times 0.22 = 1.4124$
Normalized Exploitability	$\frac{2.2212 - 0.121}{3.887 - 0.121} = 0.5577$
Normalized Impact	$\frac{1.4124 - 1.4124}{5.8731 - 1.4124} = 0.0$
Scaled Exploitability	$0.5577 \times (5 - 1) + 1 = 3.2307$
Scaled Impact	$0.0 \times (5 - 1) + 1 = 1.0$

Зважаючи на низькі значення показників ймовірності та впливу, рівень ризику для SSH Weak Key Exchange Algorithms Enabled розраховано до категорії "Low".

На рисунку 3.4 представлено результати оцінки ризиків за допомогою алгоритму.

АЛГОРИТМ			
Vulnerability	**Likelihood**	**Impact**	**Risk Rating**
Unsupported Windows OS	Very Likely	Severe	Critical
RDP (BlueKeep)	Very Likely	Severe	Critical
MS08-067	Possible	Severe	High
Default Password (admin)	Very Likely	Severe	Critical
OpenSSH Multiple Vulns	Possible	Major	High
SSL v2/v3	Possible	Moderate	Significant
OpenSSH Multiple Vulns	Possible	Moderate	Significant
OpenSSL Multiple Vulns	Very Likely	Moderate	High
MS17-010 (EternalBlue)	Possible	Severe	High
OpenSSL Heartbleed	Very Likely	Moderate	High
IPMI v2.0 Hash Disclosure	Very Likely	Moderate	High
SMB NULL Session	Very Likely	Moderate	High
SSH v1 Key Retrieval	Possible	Moderate	Significant
TLS 1.0 Detection	Possible	Major	High
TLS 1.1 Detection	Possible	Major	High
Unencrypted Telnet	Possible	Severe	High
JQuery XSS	Likely	Moderate	Medium
SSH Terrapin Weakness	Possible	Moderate	Significant
SMB Signing not required	Very Likely	Insignificant	Medium
SSH Weak Key Exchange Algs	Possible	Insignificant	Low
SSL/TLS DH ≤ 1024 Bits (Logjam)	Possible	Insignificant	Low
SSLv3 Padding Oracle (POODLE)	Possible	Insignificant	Low

Рисунок 3.4 – Результати оцінки вразливостей за допомогою алгоритму

3.4. Порівняння результатів

Порівняння дозволяє виявити суттєві розбіжності та краще зрозуміти механізми, що впливають на формування кінцевих оцінок ризику. Алгоритм, розроблений на основі формул CVSS, далі йде використовується нормалізація та масштабування показників впливу та експлуатованості, інтегруючи їх у матрицю початкових ризиків. Експертний підхід до оцінки початкових ризиків передбачає аналіз вразливостей, зазначених у звітах про безпеку (наприклад, CVSS, CVE), визначення потенційних загроз для кожного активу, а також оцінку наслідків реалізації цих загроз стосовно конфіденційності, цілісності та доступності.

У процесі аналізу було виявлено кілька прикладів, де результати алгоритму та експерта відрізнялися у категоріях Likelihood та Impact, але загальна оцінка Risk Rating залишалася однаковою. Такі випадки свідчать про те, що алгоритм та

експерт використовують різні шляхи обґрунтування, що однак призводять до однакових висновків щодо рівня ризику. На рисунку 3.5 зображено порівняння оцінок ризиків, отриманих за допомогою експертного та алгоритмічного підходів.

ЕКСПЕРТ			
Vulnerability	**Likelihood**	**Impact**	**Risk Rating**
Unsupported Windows OS	Very Likely	Severe	Critical
RDP (BlueKeep)	Very Likely	Severe	Critical
MS08-067	Likely	Major	High
Default Password (admin)	Very Likely	Severe	Critical
OpenSSH Multiple Vulns	Possible	Major	High
SSL v2/v3	Likely	Moderate	Significant
OpenSSH Multiple Vulns	Possible	Moderate	Significant
OpenSSL Multiple Vulns	Very Likely	Moderate	High
MS17-010 (EternalBlue)	Possible	Severe	High
OpenSSL Heartbleed	Very Likely	Moderate	High
IPMI v2.0 Hash Disclosure	Possible	Major	High
SMB NULL Session	Very Likely	Moderate	High
SSH v1 Key Retrieval	Possible	Moderate	Significant
TLS 1.0 Detection	Likely	Minor	Medium
TLS 1.1 Detection	Likely	Minor	Medium
Unencrypted Telnet	Possible	Major	High
JQuery XSS	Likely	Moderate	Medium
SSH Terrapin Weakness	Possible	Moderate	Significant
SMB Signing not required	Very Likely	Insignificant	Medium
SSH Weak Key Exchange Algs	Possible	Insignificant	Low
SSL/TLS DH ≤ 1024 Bits (Logjam)	Possible	Insignificant	Low
SSLv3 Padding Oracle (POODLE)	Possible	Insignificant	Low

АЛГОРИТМ			
Vulnerability	**Likelihood**	**Impact**	**Risk Rating**
Unsupported Windows OS	Very Likely	Severe	Critical
RDP (BlueKeep)	Very Likely	Severe	Critical
MS08-067	Possible	Severe	High
Default Password (admin)	Very Likely	Severe	Critical
OpenSSH Multiple Vulns	Possible	Major	High
SSL v2/v3	Possible	Moderate	Significant
OpenSSH Multiple Vulns	Possible	Moderate	Significant
OpenSSL Multiple Vulns	Very Likely	Moderate	High
MS17-010 (EternalBlue)	Possible	Severe	High
OpenSSL Heartbleed	Very Likely	Moderate	High
IPMI v2.0 Hash Disclosure	Very Likely	Moderate	High
SMB NULL Session	Very Likely	Moderate	High
SSH v1 Key Retrieval	Possible	Moderate	Significant
TLS 1.0 Detection	Possible	Major	High
TLS 1.1 Detection	Possible	Major	High
Unencrypted Telnet	Possible	Severe	High
JQuery XSS	Likely	Moderate	Medium
SSH Terrapin Weakness	Possible	Moderate	Significant
SMB Signing not required	Very Likely	Insignificant	Medium
SSH Weak Key Exchange Algs	Possible	Insignificant	Low
SSL/TLS DH ≤ 1024 Bits (Logjam)	Possible	Insignificant	Low
SSLv3 Padding Oracle (POODLE)	Possible	Insignificant	Low

Рисунок 3.5 – Порівняння результатів оцінки ризиків, проведених експертом та алгоритмом

Наприклад, у випадку з MS08-067 експерт визначив ймовірність реалізації як "Likely" і вплив як "Major", тоді як алгоритм оцінив ймовірність як "Possible", а вплив – як "Severe". Вектор CVSS (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H) вказує на високу складність атаки (AC:H), яку алгоритм врахував, знизивши ймовірність. Водночас високий вплив на конфіденційність, цілісність і доступність (C:H/I:H/A:H) пояснює підвищення оцінки впливу до Severe. Незважаючи на це, обидва підходи класифікували рівень ризику як "High".

Подібна ситуація спостерігається у випадку SSL v2/v3, де експерт визначив ймовірність як "Likely", тоді як алгоритм оцінив її як "Possible". Вектор CVSS (AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L) демонструє, що доступ до атаки можливий лише через локальну мережу (AV:A), що знизило оцінку ймовірності

алгоритмом. Однак високий вплив на конфіденційність (C:H) залишає рівень ризику "Significant" для обох підходів.

Розбіжності між оцінками Impact та Likelihood також спостерігалися у випадку IPMI v2.0 Password Hash Disclosure. Експерт оцінював ймовірність реалізації як "Possible" і вплив як "Major", тоді як алгоритм класифікував ймовірність як "Very Likely", але знизив вплив до "Moderate". Вектор CVSS (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) пояснює цю різницю: низька складність атаки (AC:L) та відсутність необхідності привілеїв (PR:N) підвищують ймовірність експлуатації, тоді як обмежений вплив на цілісність (I:N) та доступність (A:N) виправдовує оцінку "Moderate". У підсумку рівень ризику залишився "High" для обох підходів.

У випадку Unencrypted Telnet алгоритм підвищив оцінку впливу з "Major" до "Severe". Вектор CVSS (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L) вказує на високу доступність атаки (AV:N) та низьку складність (AC:L), що вплинуло на рішення алгоритму підвищити вплив. Помірний рівень впливу на конфіденційність, цілісність та доступність (C:L/I:L/A:L) також створює додатковий ризик, який був врахований алгоритмом.

Варто зазначити, що розбіжності в оцінці категорії ризику були зафіксовані у випадках з TLS 1.0 Detection та TLS 1.1 Detection. Алгоритм знизив ймовірність реалізації до "Possible", враховуючи високий рівень складності атаки (AC:H) та доступність лише через локальну мережу (AV:A). Водночас алгоритм суттєво підвищив оцінку впливу до "Major", що обумовлено високим впливом на конфіденційність (C:H) та помірним впливом на цілісність (I:L), тоді як відсутність впливу на доступність (A:N) мала меншу вагу. Це підвищення оцінки впливу пояснює зміну категорії ризику з "Medium" до "High", оскільки вразливості протоколів шифрування несуть значний ризик для захисту інформації в сучасних умовах.

Експерт, у свою чергу, оцінив ймовірність реалізації як "Likely", зважаючи на можливість легшої реалізації цих вразливостей у разі локального доступу до мережі. При цьому вплив було оцінено як "Minor", враховуючи обмежений вплив

на цілісність (I:L) та відсутність впливу на доступність (A:N). Такий підхід відображає початковий контекст оцінки ризику, де основна увага приділяється потенційним наслідкам експлуатації цих вразливостей без урахування додаткових заходів захисту. У результаті ризик було класифіковано як "Medium", оскільки наслідки для конфіденційності (C:H) хоча й мають певну вагу, але не призводять до суттєвих загроз у відсутності інших критичних чинників.

Порівняння цих результатів для цієї вразливості свідчить, що алгоритм акцентує увагу на високому впливі на конфіденційність, що відповідає сучасним стандартам оцінки ризиків. Натомість експерт зосередився на складності реалізації атаки та обмежених наслідках для цілісності й доступності, що може відображати початковий контекст аналізу та оцінку ризиків на основі наявних даних. Ця різниця в підходах пояснює розбіжність у категоріях ризику, підкреслюючи різні пріоритети в оцінюванні початкового впливу.

Рисунок 3.6 деталізує порівняння, представлене на рисунку 1, шляхом виділення розбіжностей між оцінками експерта та алгоритму. Виділені відмінності демонструють, як саме два підходи можуть розходитися у значеннях ймовірності, впливу та рівня ризику.

ЕКСПЕРТ			
Вразливість	**Likelihood**	**Impact**	**Risk Rating**
Unsupported Windows OS	Very Likely	Severe	Critical
RDP (BlueKeep)	Very Likely	Severe	Critical
MS08-067	Likely	Major	High
Default Password (admin)	Very Likely	Severe	Critical
OpenSSH Multiple Vulns	Possible	Major	High
SSL v2/v3	Likely	Moderate	Significant
OpenSSH Multiple Vulns	Possible	Moderate	Significant
OpenSSL Multiple Vulns	Very Likely	Moderate	High
MS17-010 (EternalBlue)	Possible	Severe	High
OpenSSL Heartbleed	Very Likely	Moderate	High
IPMI v2.0 Hash Disclosure	Possible	Major	High
SMB NULL Session	Very Likely	Moderate	High
SSH v1 Key Retrieval	Possible	Moderate	Significant
TLS 1.0 Detection	Likely	Minor	Medium
TLS 1.1 Detection	Likely	Minor	Medium
Unencrypted Telnet	Possible	Major	High
JQuery XSS	Likely	Moderate	Medium
SSH Terrapin Weakness	Possible	Moderate	Significant
SMB Signing not required	Very Likely	Insignificant	Medium
SSH Weak Key Exchange Algs	Possible	Insignificant	Low
SSL/TLS DH ≤ 1024 Bits (Logjam)	Possible	Insignificant	Low
SSLv3 Padding Oracle (POODLE)	Possible	Insignificant	Low

АЛГОРИТМ			
Вразливість	**Likelihood**	**Impact**	**Risk Rating**
Unsupported Windows OS	Very Likely	Severe	Critical
RDP (BlueKeep)	Very Likely	Severe	Critical
MS08-067	Possible	Severe	High
Default Password (admin)	Very Likely	Severe	Critical
OpenSSH Multiple Vulns	Possible	Major	High
SSL v2/v3	Possible	Moderate	Significant
OpenSSH Multiple Vulns	Possible	Moderate	Significant
OpenSSL Multiple Vulns	Very Likely	Moderate	High
MS17-010 (EternalBlue)	Possible	Severe	High
OpenSSL Heartbleed	Very Likely	Moderate	High
IPMI v2.0 Hash Disclosure	Very Likely	Moderate	High
SMB NULL Session	Very Likely	Moderate	High
SSH v1 Key Retrieval	Possible	Moderate	Significant
TLS 1.0 Detection	Possible	Major	High
TLS 1.1 Detection	Possible	Major	High
Unencrypted Telnet	Possible	Severe	High
JQuery XSS	Likely	Moderate	Medium
SSH Terrapin Weakness	Possible	Moderate	Significant
SMB Signing not required	Very Likely	Insignificant	Medium
SSH Weak Key Exchange Algs	Possible	Insignificant	Low
SSL/TLS DH ≤ 1024 Bits (Logjam)	Possible	Insignificant	Low
SSLv3 Padding Oracle (POODLE)	Possible	Insignificant	Low

Рисунок 3.6 – Порівняння результатів експертного та алгоритмічного аналізу з виділеними розбіжностями

Порівняння цих підходів свідчить, що алгоритм має низку переваг, зокрема стандартизованість та прозорість у розрахунках. Експертний підхід дозволяє враховувати специфіку кожного конкретного випадку, але може бути суб'єктивним. Оптимальним рішенням є поєднання цих двох методів. Алгоритмічні оцінки можуть бути використані як базова основа для стандартизації аналізу, а експертна оцінка – для врахування унікальних характеристик інфраструктури та конфігурації. Такий підхід дозволяє досягти балансу між точністю, адаптивністю та стандартизованістю оцінювання ризиків.

3.5. Висновки та рекомендації

Практичне впровадження алгоритму є обґрунтованим у контексті використання комбінованого підходу для забезпечення оптимізації процесу. Коли алгоритм стандартизує процедуру оцінювання, тим самим дозволяє швидко визначати базовий рівень початкового ризику, тоді як експертний аналіз додає необхідний контекст і враховує специфіку бізнесу, підвищуючи точність та практичність для оцінки залишкових ризиків.

Попереднє оцінювання здійснюється через застосування алгоритму, який нормалізує та масштабує значення впливу та ймовірності, приводячи їх до значень для інтеграції в матрицю ризиків. Ця процедура забезпечує структуровану первинну пріоритизацію, дозволяючи оперативно виявляти найбільш критичні загрози та визначати їх потенційну небезпеку для організації.

Експертний аналіз спрямований на уточнення результатів автоматичного оцінювання. У процесі аналізу враховуються такі аспекти, як доступність вразливості в мережевому середовищі організації, наявність компенсувальних механізмів захисту та потенційний вплив на ключові бізнес-процеси. Такий підхід дозволяє мінімізувати кількість помилкових спрацювань, забезпечуючи більш реалістичне оцінювання початкових ризиків для подальшого опрацювання.

Методика є найбільш ефективною для середніх та великих організацій із значним обсягом вразливостей, які мають високий рівень автоматизації кіберзахисту та потребують стандартизованих звітів для ухвалення рішень. Водночас, цей підхід менш доцільний для малих і середніх компаній без формалізованих процесів безпеки, а також для галузей із критичними бізнес-процесами, які вимагають більш деталізованого аналізу.

Алгоритм не може функціонувати як самостійний метод оцінки ризиків, оскільки він не адаптований до специфіки окремих організацій і не враховує контекст використання систем. Відсутність врахування критичності активів, бізнес-процесів чи взаємозв'язків між системами може призводити до ситуацій, коли вразливість на малокритичному ресурсі отримує високу оцінку, і навпаки. Також ігнорується наявність компенсувальних засобів захисту, таких як брандмауери, WAF, IDS/IPS або сегментація мережі, що здатне завищити оцінку ризику, оскільки доступність вразливості не є абсолютною.

Для забезпечення точності результатів необхідна експертна перевірка, яка додає релевантний контекст, зменшує ймовірність хибних висновків і підвищує достовірність оцінки. Поєднання алгоритму та експертного аналізу дозволяє інтегрувати отримані дані в матрицю для залишкових ризиків, враховуючи специфіку організації та забезпечуючи надійнішу основу для ухвалення рішень.

Варто зазначити, що алгоритм було інтегровано у матрицю початкових ризиків формату 5×5 із п'ятьма рівнями ризику. Оскільки тестування проводилося лише в межах цієї конфігурації, ефективність та коректність роботи алгоритму в інших форматах (наприклад, матриці 4×4 або 6×6 із відмінними рівнями ризику) залишаються невідомими. Водночас, масштабування та застосування методики в інших форматах матриць не становить труднощів, а результати, отримані під час даного дослідження, можуть слугувати основою для подальших досліджень її ефективності та коректності в ширшому спектрі сценаріїв.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

При виконанні кваліфікаційної роботи основні дослідження проводились у програмному середовищі з використанням комп’ютерної техніки та спеціалізованого програмного забезпечення. Робота виконувалась у лабораторних умовах, що вимагали дотримання встановлених норм і правил з охорони праці, електробезпеки, пожежної безпеки, а також санітарно-гігієнічних вимог.

Під час роботи з екранними пристроями, відповідно до чинного законодавства та нормативно-правових актів України, було забезпечено ергономічну організацію робочого місця та належний мікроклімат. Зокрема, виконувались вимоги Закону України "Про затвердження Вимог щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями" та НПАОП 0.00-7.15-18 [24]. Такі заходи сприяли зменшенню негативного впливу на зір, опорно-руховий апарат, а також мінімізували ризик розвитку втоми та стресових ситуацій.

– Ергономіка робочого місця дотримувалась за такими критеріями: Положення монітора: верхній край екрана знаходився на рівні або трохи нижче рівня очей користувача, а відстань до очей становила приблизно 50-70 см. Це запобігало перенапруженню зору.
– Освітлення: у приміщенні забезпечувався достатній рівень природного та штучного освітлення відповідно до ДБН В.2.5-28-2018. Використовувалися люмінесцентні або світлодіодні лампи з нейтральним світлом, що дозволяло уникнути блиску на екрані та зайвого напруження очей [25].
– Режим праці та відпочинку: через кожні 1-2 години роботи за комп’ютером робились короткі перерви, під час яких виконувались вправи для очей та

легка розминка. Такий підхід сприяв профілактиці втоми та перенапруження м’язів шиї, спини, кистей.

Електробезпека робочого місця забезпечувалась відповідно до вимог «Правил безпечної експлуатації електроустановок споживачів» (НПАОП 40.1-1.21-98). Комп’ютерна техніка та периферійне обладнання підключалися до електромережі через справні розетки із заземленням. Електромережа була обладнана пристроями захисного відключення, що мінімізувало ризик ураження електричним струмом. Проводка й подовжувачі використовувались з негорючими ізоляційними матеріалами.

Для забезпечення пожежної безпеки дотримувались вимог «Правил пожежної безпеки в Україні». У приміщенні, де проводились дослідження, були наявні первинні засоби пожежогасіння (вогнегасник відповідного типу). Дотримання рекомендованого розташування обладнання, відсутність перевантаження розеток і застосування лише справних подовжувачів знижували ризик виникнення займання. На випадок надзвичайної ситуації існував чіткий алгоритм дій та належні засоби евакуації.

Санітарно-гігієнічні умови включали дотримання температурного режиму та вологості повітря згідно з чинними санітарними нормами. Забезпечувались оптимальні параметри мікроклімату для комфортної роботи, зокрема належна вентиляція та регулярне провітрювання приміщення. Відсутність надмірного шуму сприяла підвищенню концентрації та зменшенню психофізіологічного навантаження.

Під час виконання роботи було унеможливлено будь-які небезпечні маніпуляції з обладнанням: не проводилося втручання у внутрішню конструкцію комп’ютерної техніки, не застосовувались несправні пристрої або матеріали. Уся діяльність обмежувалася програмними операціями та аналітичними дослідженнями, що знижувало ризики травматизму до мінімуму.

Загалом дотримання вимог охорони праці, електробезпеки, пожежної безпеки, ергономіки та санітарно-гігієнічних норм забезпечило безпечні та комфортні умови для проведення досліджень.

4.2 Здоровий спосіб життя людини та його вплив на професійну діяльність

Здоровий спосіб життя є ключовим чинником, який забезпечує якість життя та високу ефективність професійної діяльності людини. Він об'єднує кілька важливих аспектів: фізичну активність, збалансоване харчування, психоемоційну рівновагу, якісний сон та відмову від шкідливих звичок. Виконання цих принципів сприяє зміцненню здоров'я, підвищенню енергійності та стійкості до стресів, що є особливо важливим у сучасному ритмі професійного життя.

Фізична активність є одним із найважливіших компонентів здорового способу життя, оскільки вона сприяє підтримці загального здоров'я та підвищенню якості життя. Вона позитивно впливає на серцево-судинну систему, зміцнює м'язи і суглоби, а також сприяє покращенню загального тонусу організму. Регулярні фізичні вправи дозволяють значно знизити ризик розвитку серйозних захворювань, таких як гіпертонія, діабет або ожиріння, що часто виникають через малорухливий спосіб життя. Крім того, фізична активність активізує виділення ендорфінів – гормонів щастя, які сприяють покращенню настрою, підвищенню рівня енергії та концентрації.

Всесвітня організація охорони здоров'я рекомендує виконувати вправи помірної інтенсивності тривалістю не менше 150 хвилин на тиждень, що допомагає забезпечити необхідний рівень фізичної активності для підтримки здоров'я. У сучасному професійному середовищі інтеграція фізичної активності у щоденний графік може включати такі заходи:

- Прогулянки під час обідньої перерви.
- Використання сходів замість ліфта для підвищення рухливості.
- Заняття короткими руханками протягом робочого дня.
- Регулярні тренування після роботи, такі як заняття у спортзалі або йога.

Крім того, роботодавці можуть відігравати важливу роль у популяризації фізичної активності серед працівників, організовуючи корпоративні заходи, наприклад спортивні дні або програми заохочення до здорового способу життя.

Такі ініціативи не лише сприяють покращенню фізичного стану працівників, але й підвищують їх мотивацію та загальну задоволеність роботою.

Харчування є одним із фундаментальних елементів здорового способу життя, оскільки воно забезпечує організм необхідними поживними речовинами та енергією для підтримання фізичної активності та розумової працездатності. Збалансоване споживання білків, жирів, вуглеводів, вітамінів і мінералів сприяє підтриманню здоров’я на належному рівні, запобігає розвитку захворювань і забезпечує стабільну роботу всіх систем організму. Особливо важливим аспектом є споживання достатньої кількості води, яка відіграє ключову роль у регуляції обмінних процесів, підтримці терморегуляції та забезпеченні нормальної діяльності органів і тканин.

Недотримання принципів раціонального харчування, зокрема надмірне вживання солі, цукру та продуктів із високим вмістом трансжирів, може призводити до розвитку хронічних захворювань, таких як серцево-судинні патології, ожиріння або діабет. Водночас здорове харчування допомагає підтримувати стабільний рівень енергії протягом дня, що особливо важливо для працівників, чия діяльність вимагає високої концентрації та тривалої продуктивності. Для цього рекомендується включати до раціону свіжі фрукти, овочі, нежирне м’ясо, рибу, а також продукти, багаті на клітковину.

На робочих місцях доцільно створювати умови, які сприяють дотриманню раціонального харчування. Наприклад, роботодавці можуть забезпечувати доступ до здорових перекусів, таких як фрукти, горіхи, йогурти, або організовувати корпоративні програми харчування, які пропонують збалансовані обіди. Заохочення до здорового способу життя також може включати інформаційні кампанії, присвячені перевагам раціонального харчування, або проведення лекцій із залученням дієтологів. Упровадження таких ініціатив сприяє не лише підвищенню продуктивності працівників, а й зміцненню їхнього загального здоров’я та зменшенню ризику виникнення професійного вигорання.

Психоемоційна рівновага є ключовим чинником, що впливає на здатність ефективно виконувати професійні обов'язки, оскільки саме від неї залежить стійкість працівника до стресу та його емоційна стабільність. Постійний стрес і емоційне вигоряння можуть значно знизити продуктивність, спричинити втрату мотивації та розвиток психосоматичних розладів, таких як порушення сну, тривожність або депресія. З метою запобігання таким негативним наслідкам особливу увагу слід приділяти практикам, які сприяють зниженню рівня стресу.

Одним із ефективних способів підтримки психоемоційного здоров'я є регулярне виконання медитацій, дихальних вправ та технік релаксації, які дозволяють відновлювати емоційну рівновагу навіть у стресових ситуаціях. Крім цього, регулярні перерви у роботі та створення дружньої атмосфери у колективі можуть значно покращити загальний стан здоров'я працівників. Підтримка колег та доброзичливі відносини всередині команди відіграють важливу роль у зниженні емоційного напруження та створенні комфортного середовища для ефективної діяльності.

У сучасному корпоративному світі компанії все частіше включають у свої соціальні пакети додаткові програми для підтримки психоемоційного здоров'я. До них належать тренінги з управління стресом, консультації з психологами, створення зон для відпочинку, а також організація майстер-класів із розвитку емоційного інтелекту. Деякі роботодавці також впроваджують програми гнучкого графіка, які дозволяють працівникам краще балансувати між роботою та особистим життям, що є важливим фактором для запобігання емоційному вигоранню. Такий підхід не лише покращує добробут співробітників, але й позитивно впливає на їхню продуктивність, знижує плинність кадрів і підвищує загальну ефективність компанії.

Якісний сон є критично важливим для відновлення організму після фізичних і психічних навантажень. Сон тривалістю 7-8 годин на добу дозволяє відновити працездатність, покращити когнітивні функції та зміцнити імунну систему. Хронічний дефіцит сну призводить до зниження продуктивності, підвищення дратівливості та порушення обміну речовин, що може стати

причиною серйозних проблем зі здоров'ям. Щоб покращити якість сну, важливо дотримуватися режиму дня, уникати використання електронних пристроїв перед сном та створювати комфортні умови для відпочинку. На професійному рівні це може включати гнучкий графік роботи або організацію зон для відпочинку в офісі.

Шкідливі звички, такі як куріння, зловживання алкоголем або наркотичними речовинами, негативно впливають на здоров’я та знижують ефективність професійної діяльності. Відмова від цих звичок сприяє покращенню фізичного стану, підвищенню рівня енергії та стійкості до стресів. Корпоративні програми, спрямовані на підтримку здорового способу життя, можуть включати консультації зі спеціалістами, підтримувальні групи або програми заохочення до здорових звичок.

Ефективне управління часом є надзвичайно важливим компонентом здорового способу життя, оскільки воно безпосередньо впливає на рівень професійної продуктивності, емоційного благополуччя та загального стану здоров'я. Грамотне планування робочого та особистого часу дозволяє уникнути перенавантаження, зберегти баланс між професійними обов'язками та відпочинком, а також забезпечити необхідний рівень фізичного й емоційного відновлення. Відсутність цього балансу може призводити до перевтоми, зниження мотивації та підвищення рівня стресу, що, своєю чергою, негативно впливає на якість виконання завдань.

Ключовими принципами ефективного управління часом є створення чіткого розподілу завдань, правильне делегування обов'язків, а також уникнення багатозадачності, яка часто знижує концентрацію та уповільнює виконання роботи. Крім того, важливим є використання сучасних цифрових інструментів, таких як планувальники, трекери завдань і додатки для моніторингу часу, які дозволяють оптимізувати робочі процеси. Такі інструменти сприяють не лише організації роботи, але й зменшенню ризику перевтоми, завдяки чіткій структурі дня.

На корпоративному рівні багато компаній активно впроваджують програми, які допомагають працівникам ефективно розподіляти свій час. Наприклад, роботодавці можуть організовувати тренінги з тайм-менеджменту, запроваджувати гнучкі графіки роботи або забезпечувати доступ до технологій, які полегшують планування робочого процесу. У деяких випадках у соціальний пакет включають консультації з фахівцями з тайм-менеджменту, що дозволяє співробітникам краще адаптуватися до робочого навантаження та знаходити час для відпочинку.

Щоб забезпечити максимальну продуктивність і мінімізувати стрес, рекомендується дотримуватися таких практик:

- Встановлення пріоритетів: визначення найважливіших завдань на день.
- Планування перерв для фізичної активності або релаксації.
- Чітке розмежування робочого та особистого часу, щоб уникнути емоційного вигоряння.
- Аналіз витрат часу для виявлення неефективних практик.

Таким чином, ефективне управління часом є основою для досягнення гармонії між роботою та життям, що сприяє покращенню фізичного й емоційного здоров'я, а також підвищенню загальної ефективності.

Сучасні компанії все частіше інтегрують у свої стратегії програми, спрямовані на заохочення працівників до здорового способу життя. Це включає організацію тренінгів, присвячених управлінню стресом, консультації з дієтологами або психологами, а також забезпечення доступу до спортивних програм, таких як фітнес-зали або корпоративні абонементи у спортивні клуби. У деяких компаніях до соціального пакета включають регулярні медичні огляди, майстер-класи з кулінарії здорового харчування або лекції про підтримання фізичної активності. Це сприяє формуванню усвідомленого підходу до власного здоров’я серед працівників.

Такі ініціативи мають значний вплив не лише на фізичний стан працівників, але й на їхню мотивацію та задоволеність роботою. Співробітники, які відчувають підтримку з боку роботодавця, краще адаптуються до стресових

ситуацій, рідше хворіють і демонструють вищий рівень продуктивності. Впровадження програм, спрямованих на популяризацію здорового способу життя, допомагає також знизити рівень плинності кадрів і створити в компанії позитивну репутацію як роботодавця. Таким чином, підтримка здорового способу життя на робочих місцях стає інвестицією, яка забезпечує довгострокові вигоди як для працівників, так і для бізнесу загалом.

ВИСНОВКИ

Проведене дослідження підтвердило доцільність та ефективність інтеграції показників CVSS 3.0 (Exploitability, Impact) у формат корпоративної матриці ризиків 5×5 для спрощення процесу оцінювання вразливостей. Запропонований алгоритм нормалізації та масштабування вхідних даних із подальшою їх адаптацією до стандартної матриці початкових ризиків дає змогу зменшити обсяг рутинної роботи експертів із безпеки.

Аналіз практичних результатів засвідчив, що автоматизований розрахунок ризиків на основі базових показників CVSS може бути ефективно поєднаний із наступним експертним аналізом, який враховує контекст конкретної організації: критичність активів, специфіку бізнес-процесів, а також наявність компенсувальних механізмів захисту.

На основі проведеного аналізу можна припустити, що найбільша ефективність запропонованого методу може бути досягнута у середніх та великих організаціях із розвиненими системами кіберзахисту. Стандартизована система звітності та швидке формування пріоритетів дозволяють оптимізувати розподіл ресурсів і, у підсумку, підвищувати загальну стійкість інформаційної інфраструктури. Натомість для невеликих організацій із відсутніми або неформалізованими процесами безпеки ефективність цього методу може бути зниженою, оскільки визначення початкових ризиків потребує додаткового опрацювання.

Обмеженням розробленого алгоритму є його початкова орієнтація на матрицю ризиків 5×5 із п’ятьма рівнями критичності. Хоча результати дослідження демонструють відсутність труднощів у масштабуванні та перенесенні методики на інші формати, наразі відсутні емпіричні дані щодо точності та придатності цього алгоритму в таких сценаріях.

Таким чином, запропонована методика розширює існуючі інструменти управління початковими ризиками, надаючи гнучкий і водночас стандартизований підхід. Її застосування дає змогу скоротити час, необхідний на

оцінювання початкових ризиків, оптимізувати розподіл ресурсів та формувати релевантні звіти. Надалі перспективи дослідження полягають у масштабуванні методу на інші формати матриць і поглибленому вивченні особливостей його використання в організаціях із різними рівнями зрілості процесів кіберзахисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. WIVSS: A New Methodology for Scoring Information Systems Vulnerabilities. ResearchGate. [Електронний ресурс] Режим доступа: https://www.researchgate.net/publication/262241114_WIVSS_A_new_methodology_for_scoring_information_systems_vulnerabilities. (дата звернення: 03.10.2024).
2. CVSS (Common Vulnerability Scoring System): Definition and Overview. TechTarget. [Електронний ресурс]. Режим доступу: https://www.techtarget.com/searchsecurity/definition/CVSS-Common-Vulnerability-Scoring-System. (дата звернення: 03.10.2024).
3. CWSS Version 1.0.1. MITRE. [Електронний ресурс]. Режим доступу: https://cwe.mitre.org/cwss/cwss_v1.0.1.html. (дата звернення: 04.10.2024).
4. Threat Modeling with Microsoft DREAD. Satori Cyber. [Електронний ресурс]. Режим доступу: https://satoricyber.com/glossary/threat-modeling-with-microsoft-dread/. (дата звернення: 04.10.2024).
5. CVSS Version 4.0. FIRST Organization. [Електронний ресурс]. Режим доступу: https://www.first.org/cvss/v4-0/. (дата звернення: 26.12.2024).
6. Derkach, M., Skarga-Bandurova, I., Matiuk, D., & Zagorodna, N. (2022, December). Autonomous quadrotor flight stabilisation based on a complementary filter and a PID controller. In 2022 12th International Conference on Dependable Systems, Services and Technologies (DESSERT) (pp. 1-7). IEEE.
7. Understanding Inherent Risks in Cybersecurity. Computers & Security, Volume 123, 2023. p. 35–50.
8. ISO 27001: A Comprehensive Approach to Residual Risk Management. International Journal of Information Security and Policy, Volume 20, Issue 4, 2023. p. 275–290.

9. Mishko, O., Matiuk, D., & Derkach, M. (2024). Security of remote iot system management by integrating firewall configuration into tunneled traffic. Вісник Тернопільського національного технічного університету, 115(3), 122-129.
10. What is a Risk Assessment Matrix? AuditBoard. [Електронний ресурс]. Режим доступу: https://www.auditboard.com/blog/what-is-a-risk-assessment-matrix/. (дата звернення: 11.10.2024).
11. Lechachenko, T., Gancarczyk, T., Lobur, T., & Postoliuk, A. (2023). Cybersecurity Assessments Based on Combining TODIM Method and STRIDE Model for Learning Management Systems. In CITI (pp. 250-256).
12. Quantitative Risk Analysis in Cybersecurity: Methods and Models. IEEE Transactions on Risk Management, Volume 25, Issue 3, 2023. p. 350–370.
13. Tymoshchuk, D., Yasniy, O., Mytnyk, M., Zagorodna, N., Tymoshchuk, V., (2024). Detection and classification of DDoS flooding attacks by machine learning methods. CEUR Workshop Proceedings, 3842, pp. 184 - 195.
14. ТИМОЩУК, Д., & ЯЦКІВ, В. (2024). USING HYPERVISORS TO CREATE A CYBER POLYGON. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (3), 52-56.
15. CVSS Version 3.0 Specification Document. FIRST Organization. [Електронний ресурс]. Режим доступу: https://www.first.org/cvss/v3.0/specification-document. (дата звернення: 20.10.2024).
16. Tymoshchuk, D., & Yatskiv, V. (2024). Slowloris ddos detection and prevention in real-time. Collection of scientific papers «ΛΌГОΣ», (August 16, 2024; Oxford, UK), 171-176.
17. Yesin, V., Karpinski, M., Yesina, M., Vilihura, V., Kozak, R., & Shevchuk, R. (2023). Technique for Searching Data in a Cryptographically Protected SQL Database. Applied Sciences, 13(20), 11525.
18. IEEE FiCloud. "Normalization Framework for Vulnerability Risk Management in Cloud". Presented at the International Conference on Internet of Things and Cloud Technologies (FiCloud).

19. Lypa, B., Horyn, I., Zagorodna, N., Tymoshchuk, D., Lechachenko T., (2024). Comparison of feature extraction tools for network traffic data. CEUR Workshop Proceedings, 3896, pp. 1-11.
20. Tymoshchuk, V., Pakhoda, V., Dolinskyi, A., Karnaukhov, A., & Tymoshchuk, D. (2024). MODELLING CYBER THREATS AND EVALUATING THE PERFORMANCE OF INTRUSION DETECTION SYSTEMS. Grail of Science, (46), 636–641. https://doi.org/10.36074/grail-of-science.29.11.2024.081
21. Information Security Risk Assessment. ResearchGate. [Електронний ресурс]. Режим доступу: https://www.researchgate.net/publication/353436973_Information_Security_Risk_Assessment. (дата звернення: 04.11.2024).
22. ТИМОЩУК, Д., ЯЦКІВ, В., ТИМОЩУК, В., & ЯЦКІВ, Н. (2024). INTERACTIVE CYBERSECURITY TRAINING SYSTEM BASED ON SIMULATION ENVIRONMENTS. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (4), 215-220.
23. Lupenko, S., Orobchuk, O., Osukhivska, H., Xu, M., & Pomazkina, T. (2019, July). Methods and means of knowledge elicitation in Chinese Image Medicine for achieving the tasks of its ontological modeling. In 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON) (pp. 855-858). IEEE.
24. Порядок організації захисту інформації в інформаційно-телекомунікаційних системах. Законодавство України. [Електронний ресурс] Режим доступа: https://zakon.rada.gov.ua/laws/show/z0508-18#Text. (дата звернення: 20.11.2024).
25. НПАОП 0.00-7.15-18 Вимоги щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями. Київ. 2018.
26. Вовк Ю. Я. Охорона праці в галузі. Навчальний посібник / Ю. Я. Вовк, І. П. Вовк – Тернопіль: ФОП Паляниця В.А. – 2015. – 172 с.

Додаток А – Публікація

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
імені ІВАНА ПУЛЮЯ
НАУКОВЕ ТОВАРИСТВО ім. ШЕВЧЕНКА

М А Т Е Р І А Л И

XII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

18-19 грудня 2024 року

ТЕРНОПІЛЬ
2024

УДК 001
М34

ПРОГРАМНИЙ КОМІТЕТ

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

М34 Матеріали XII науково-технічної конфції «Інформаційні моделі, системи та технології» Тернопільського національного технічного університету імені Івана Пулюя, (Тернопіль, 18–19 грудня 2024 р.). – Тернопіль : Тернопільський національний технічний університет імені Івана Пулюя, 2024.

Адреса оргкомітету: ТНТУ ім. І. Пулюя, м. Тернопіль, вул. Руська, 56, 46001,
тел. (0352) 52-41-33, факс (0352) 25-49-83.
E-mail: conffis2024@gmail.com
Редагування, оформлення та верстка: Надія Крива

СЕКЦІЇ КОНФЕРЕНЦІЇ, ЯКІ ПРЕДСТВЛЕНІ В ЗБІРНИКУ

- Математичне моделювання
- Інформаційні системи та технології, кібербезпека
- Комп'ютерні системи та мережі
- Програмна інженерія та моделювання складних розподілених систем
- Новітні фізико-технічні та освітні технології

В збірнику надруковано тези доповідей XII науково-технічної конференції «Інформаційні моделі, системи та технології» (Тернопіль, 18–19 грудня 2024 р.) за такими науковими напрямками: математичне моделювання; інформаційні системи та технології, кібербезпека; комп'ютерні системи та мережі; програмна інженерія та моделювання складних розподілених систем; новітні фізико-технічні та освітні технології.

Розрахований на науковців, викладачів та студентів вузів.

За зміст тез та дотримання норм академічної доброчесності відповідальність несе автор.

УДК 004.7:8

Ревура Дмитро, студент гр.СБм-61, Руслан Козак, к.т.н, доцент
(Тернопільський національний технічний університет імені Івана Пулюя)

ІНТЕРПРЕТАЦІЯ СИСТЕМИ ОЦІНКИ ВРАЗЛИВОСТЕЙ, ЯК МЕТОДУ ДЛЯ ОЦІНКИ РИЗИКІВ

Dmytro Revura, student of gr. СБм-61, Ruslan Kozak, Ph.D.

INTERPRETATION OF A VULNERABILITY ASSESSMENT SYSTEM AS A METHOD FOR RISK EVALUATION

У сучасному кіберсередовищі стрімко зростає кількість вразливостей та загроз, що створює потребу в простих і доступних методах оцінювання ризиків. Одним із ключових інструментів для оцінювання вразливостей є система CVSS (Common Vulnerability Scoring System). CVSS широко використовується в різних організаціях для визначення пріоритетності усунення вразливостей, але її потенціал для оцінки ризиків залишається недостатньо розкритим [1].

Метою роботи є дослідження можливості застосування характеристик системи оцінки вразливостей CVSS для оптимізації процесу оцінювання ризиків, використовуючи наявні в CVSS показники впливу та ймовірності. Для досягнення мети виконано наступні завдання:

- Проаналізовано систему CVSS 3.0, включаючи формули, їхню специфіку, визначення та обґрунтування коефіцієнтів.
- Проаналізовано наукові дослідження, присвячені вдосконаленню процесів оцінки та управління ризиками за допомогою нормалізації CVSS для стандартизації оцінок ризиків, а також методології OWASP, яка забезпечує структуровану класифікацію ризиків та прозорість у їх інтерпретації
- Досліджено методології нормалізації даних, що використовуються для аналізу ризиків.
- Розроблено алгоритм оцінки ризиків на основі CVSS та побудувано блок-схему для його впровадження.

Аналіз літератури охоплює наукові праці, присвячені вдосконаленню процесів управління ризиками [2], а також OWASP Risk Rating Methodology. Було досліджено математичні підходи до нормалізації даних для полегшення інтерпретації метрик CVSS. Результати аналізу показали, що нормалізація може бути ефективним інструментом для автоматизації процесу оцінювання ризиків.

На основі отриманих даних запропоновано інтерпретацію CVSS методом нормалізації на прикладі вразливостей компаній малого бізнесу, що дозволяє адаптувати підхід до їхніх потреб і обмежених ресурсів.

Результати дослідження демонструють, що інтеграція CVSS у процеси оцінки ризиків дає змогу створити системний підхід для управління безпекою. Нормалізація даних підвищує точність інтерпретації, а автоматизований алгоритм оцінки зменшує потребу в залученні експертів. Запропонована методологія є перспективним напрямом у розвитку підходів з управління ризиками кібербезпеки та може бути адаптована до умов малого та середнього бізнесу.

Література

1. SAM'11. "Defining and Assessing Quantitative Security Risk Measures Using Vulnerability Lifecycle and CVSS Metrics". Presented at the International Conference on Security Assessment and Management.

2. IEEE FiCloud. "Normalization Framework for Vulnerability Risk Management in Cloud". Presented at the International Conference on Internet of Things and Cloud Technologies (FiCloud).