МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

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

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ РОЗРОБКА МЕТОДУ КОМПЛЕКСНОЇ ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ ЗА РЕЗУЛЬТАТАМИ ПЕНТЕСТУ”

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

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

_____ Іван СЕЛІВАНОВ
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ-61
Іван СЕЛІВАНОВ

Керівник:
к. т. н
Доцент кафедри Дмитро Рабчун

Рецензент:
д.т.н., професор Галина ГАЙДУР

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

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

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

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Студенту Селіванову Івану Сергійовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: " Розробка методу комплексної оцінки захищеності інформаційних систем за результатами пентесту".

керівник кваліфікаційної роботи Дмитро РАБЧУН, к. т. н , Доцент кафедри
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від "30" жовтня 2025 р. № 467

2. Строк подання кваліфікаційної роботи "11" грудня 2025 р.
3. Вихідні дані до кваліфікаційної роботи: нормативно-правові акти України у сфері технічного захисту інформації; міжнародні стандарти серії ISO/IEC 27000 (27001, 27002, 27005), NIST SP 800-30, NIST SP 800-115; методології тестування на проникнення PTES, OSSTMM, OWASP WSTG; специфікація метрики CVSS v3.1; статистичні дані щодо вразливостей інформаційних систем .
4. Перелік питань, які потрібно розробити: Проведення аналізу існуючих методик, оцінки захищеності на основі результатів пентесту, проведення пентесту об'єкта дослідження за для подальшого використання даних у розробці методу, розробити метод комплексної оцінки захищеності за результатами пентесту.
5. Перелік ілюстративного матеріалу: *презентація*
6. Дата видачі завдання "02" жовтня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2025	
2.	Збір та аналіз літератури.	23.10.2025	
3.	Визначення теоретичних основ з забезпечення інформаційної безпеки та пентесту	27.10.2025	
4.	Проведення аналізу існуючих методик оцінки захищеності на основі результатів пентесту	10.11.2025	
5.	Проведення пентесту об’єкта дослідження за для подальшого використання даних у розробці методу	15.11.2025	
6.	Робота над розробкою Методу комплексної оцінки захищеності за результатами пентесту	22.11.2025	
7.	Оформлення роботи.	04.12.2025	
8.	Оформлення презентації.	14.12.2025	
9.	Отримання рецензії на роботу.	18.12.2025	
10.	Захист в ЕК.	22.01.2026	

Здобувач вищої освіти _____ Іван СЕЛІВАНОВ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Дмитро РАБЧУН
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

Направляється здобувач Селіванов І.С, до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека та захист інформації
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Розробка методу комплексної оцінки захищеності інформаційних систем за результатами пентесту."
Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач **СЕЛІВАНОВ Іван** у кваліфікаційній роботі проаналізував теоретичні аспекти технологій оцінки методик, вивчив методи та засоби технологій оцінки методик, а також дослідив практичне застосування власного методу технологій для оцінки та розробки методу для комплексної оцінки інформаційних систем після проведення пентесту у інформаційних системах.

СЕЛІВАНОВ Іван показав високу теоретичну і практичну підготовку, володіння науково-дослідницькими методами, вміння самостійно знаходити шляхи вирішення проблеми дослідження. Результати дослідження апробовані на конференції "Актуальні проблеми кібербезпеки: проблеми та недоліки існуючих методів комплексної оцінки захищеності інформаційних систем за результатами пентесту" 29 жовтня 2025 року.

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

Керівник кваліфікаційної роботи _____ Дмитро РАБЧУН
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Селіванов І.С. допускається до захисту даної роботи в Екзаменаційній комісії.

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

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

Здобувача вищої освіти Селіванова Івана Сергійовича
на тему " Розробка методу комплексної оцінки захищеності інформаційних систем за результатами пентесту".

Актуальність В умовах постійного зростання кількості та складності кібератак, просте виявлення вразливостей вже не гарантує безпеку активів підприємства. Сучасні компанії потребують не лише переліку технічних недоліків, а й чіткого розуміння реального стану захищеності системи для прийняття ефективних управлінських рішень. Існуючі підходи часто розривають зв'язок між технічними результатами тестування на проникнення та бізнес-ризиками. Тим часом розробка методу, який дозволяє комплексно та кількісно оцінити рівень захищеності на основі емпіричних даних пентесту, є важливим та актуальним науково-практичним завданням

Позитивні сторони

1. У роботі проведено ґрунтовний аналіз сучасних міжнародних стандартів (NIST, ISO/IEC, PTES) та методологій оцінки вразливостей (CVSS). У роботі продемонстровано глибоке розуміння проблеми відсутності уніфікованого підходу до інтерпретації результатів пентесту та запропонував шляхи її вирішення.
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Було опрацьовано значну джерельну базу, близько 50 публікацій та електронних джерел, в тому числі англомовних.
3. За результатами дослідження було запропоновано метод комплексної оцінки захищеності інформаційних систем за результатами пентесту.

Недоліки

1. Доцільно було б приділити більше уваги вивченню особливості застосування методу для хмарних інфраструктур, враховуючи специфіку розподіленої відповідальності.

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

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

Рецензент:
Управління інформаційною та
кібернетичною безпекою
д.т.н, професор _____ *Підпис* *Світлана Гайдур*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 62 сторінок, 5 рисунків, 10 таблиць, 5 формул та 45 джерел інформації.

Метою роботи є розробка обґрунтованої та спроможної на життя методику комплексної оцінки рівня захищеності інформаційних систем на основі результатів пентесту (тестування на проникнення).

Об'єктом дослідження є інформаційна системи та її компоненти.

***Предмет дослідження*:** методи, процеси, моделі, критерії та метрики оцінки захищеності інформаційних систем за результатами пентесту.

Методи дослідження: у ході роботи були застосовані Методи системного та порівняльного аналізу використано для вивчення наявних міжнародних стандартів аудиту інформаційної безпеки (ISO/IEC 27001, COBIT) та провідних методологій проведення пентесту (OWASP, PTES) з метою інтеграції їхніх найкращих практик у розроблювану методику; Метод формалізації та математичного моделювання застосовано для розробки інтегрального показника захищеності, що дозволив кількісно агрегувати множину виявлених вразливостей, їхню критичність на основі, модифікованої шкали CVS потенційний вплив на бізнес-процеси; Метод експертних оцінок використано для визначення вагових коефіцієнтів та оцінки критеріїв оцінки, що забезпечує об'єктивність та практичну значущість аудиторських висновків;

***Короткий зміст роботи*:** у роботі вперше системно інтегровано технічний процес пентесту з вимогами управлінського аудиту. Проведено критичний аналіз існуючих підходів до оцінки результатів пентесту та обґрунтовано необхідність їхньої трансформації для формування управлінських рішень та аудиторських висновків. Розроблено методологію, яка дозволяє стандартизувати процес збору технічних доказів та перевести їх у формалізований аудиторський звіт про відповідність. Було запропоновано математичну модель розрахунку інтегрального показника рівня ризику, який виступає єдиною, зрозумілою для керівництва метрикою, що відображає загальний стан захищеності ІС. Надано чіткий алгоритм пріоритетизації усунення вразливостей, що базується не лише на технічній критичності, але й на впливі на ключові активи підприємства, що є ключовим для аудиту ризиків. Представлено

структуру та зміст аудиторського звіту, який використовує розроблену методику як основу для своїх висновків.

***Галузь застосування*:** проведена робота буде корисною у розрізі внутрішнього та зовнішнього аудитів інформаційної безпеки: для об'єктивної оцінки фактичного стану захищеності та контролю ефективності заходів ІБ. Розгляд точної ідентифікації та кількісної оцінки ризиків, що дозволяє керівництву приймати обґрунтовані рішення щодо інвестицій у безпеку.

КЛЮЧОВІ СЛОВА: ІНФОРМАЦІЙНА БЕЗПЕКА, АУДИТ, ПЕНТЕСТ, МЕТОДОЛОГІЯ АУДИТУ, ІНТЕГРАЛЬНА ОЦІНКА, CVSS.

ABSTRACT

Text part of the qualification work for obtaining a master's degree: 62 pages, 5 figures, 10 tables, 5 formulas 55 sources.

The purpose of the work is to develop a substantiated and viable methodology for a comprehensive assessment of the level of security of information systems based on the results of pentest (penetration testing).

The object of the study is the information system and its components.

The subject of the study is methods, processes, models, criteria and metrics for assessing the security of information systems based on the results of pentest.

Research methods used in the work Methods of system and comparative analysis were used to study existing international standards for information security auditing (ISO/IEC 27001, COBIT) and leading pentest methodologies (OWASP, PTES) in order to integrate their best practices into the developed methodology; The method of formalization and mathematical modeling was used to develop an integral security indicator, which allowed to quantitatively aggregate the set of identified vulnerabilities, their criticality based on the modified CVS scale, potential impact on business processes; The method of expert assessments was used to determine weighting factors and evaluate the assessment criteria, which ensures the objectivity and practical significance of audit conclusions;

Summary of the work - the technical process of pentesting with the requirements of management audit is systematically integrated in the work for the first time. A critical analysis of existing approaches to assessing pentest results was conducted and the need for their transformation was justified for the formation of management decisions and audit conclusions. A methodology was developed that allows standardizing the process of collecting technical evidence and translating it into a formalized audit report on compliance. A mathematical model for calculating the integral risk level indicator was proposed, which acts as

a single, understandable metric for management, reflecting the general state of IS security. A clear algorithm for prioritizing vulnerability removal is provided, based not only on technical criticality, but also on the impact on key assets of the enterprise, which is key for risk auditing. The structure and content of the audit report, which uses the developed methodology as the basis for its conclusions, is presented.

Scope. The work will be useful in the context of internal and external information security audits: for an objective assessment of the actual state of security and control of the effectiveness of IS measures. Consideration of accurate identification and quantitative assessment of risks, which allows management to make informed decisions regarding investments in security.

KEYWORDS: INFORMATION SECURITY, AUDIT, PENTEST, AUDIT METHODOLOGY, INTEGRATED

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ІБ - Інформаційна безпека

КБ - Кібербезпека

КЦД - Класичні тріади

ІС - Інформаційна система

ISO - International Organization for Standardization / International

NIST - National Institute of Standards and Technology

PIMS - Privacy Information Management System

RBAC - Role-Based Access Control

SCADA - Supervisory Control and Data Acquisition

SIEM - Security Information and Event Management

SOAR - Security Orchestration, Automation and Response

SOC - Security Operations Center

ВСТУП

Актуальність теми: в умовах постійного зростання кількості та складності кібератак, просте виявлення вразливостей вже не гарантує безпеку активів підприємства. Сучасні компанії потребують не лише переліку технічних недоліків, а й чіткого розуміння реального стану захищеності системи для прийняття ефективних управлінських рішень. Існуючі підходи часто розривають зв'язок між технічними результатами тестування на проникнення та бізнес-ризиками. Тим часом розробка методики, яка дозволяє комплексно та кількісно оцінити рівень захищеності на основі емпіричних даних пентесту, є важливим та актуальним науково-практичним завданням

Мета роботи: полягає у розробці обґрунтованої та спроможну на життя методику комплексної оцінки рівня захищеності інформаційних систем на основі результатів пентесту (тестування на проникнення), що дозволить кількісно та якісно оцінити ефективність існуючих механізмів безпеки, визначити рівень ризику виявлених вразливостей та сформувати рекомендації за для зменшення ймовірності успішної реалізації атак.

Для досягнення цієї мети в роботі необхідно виконати наступні завдання:

1. Проаналізувати існуючі методи оцінки захищеності на основі результатів пентесту;

2. Розробити методику комплексної оцінки захищеності за результатами пентесту;

3. Реалізувати розроблену методику на практиці;

4. Сформувати загальні висновки щодо роботи.

Об’єкт дослідження є інформаційні системи та їх компоненти.

Предмет дослідження: є методи, процеси, моделі, критерії та метрики оцінки захищеності інформаційних систем за результатами пентесту.

Методи дослідження: є системний аналіз, порівняльний аналіз, метод формалізації та математичного моделювання, метод експертних оцінок, метод експерименту

Наукова новизна одержаних результатів: полягає *у* розробці методологію аудиту захищеності, яка забезпечує безшовний та формалізований перехід від суто технічного звіту пентесту до управлінського аудиторського висновку, Удосконалено підхід до оцінки критичності вразливостей шляхом інтеграції стандартних метрик з аудиторськими критеріями важливості об'єкта, на якому виявлено вразливість. Розроблено математичну модель інтегрального показника захищеності.

Практичне значення одержаних результатів: полягає у створенні ефективного інструменту для внутрішнього аудиту, Обґрунтування інвестиційних рішень, Покращення якості звітів з пентесту.

Галузь застосування: проведена робота буде корисною у розрізі внутрішнього та зовнішнього аудитів інформаційної безпеки: для об'єктивної оцінки фактичного стану захищеності та контролю ефективності заходів ІБ. Розгляд точної ідентифікації та кількісної оцінки ризиків, що дозволяє керівництву приймати обґрунтовані рішення щодо інвестицій у безпеку.

Апробація результатів кваліфікаційної роботи відбулася на онлайн конференції в рамках наукового семінару “Актуальні проблеми кібербезпеки”, а також у процесі практичного застосування розробленої методики для оцінки захищеності.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ПЕНТЕСТУ

1.1 Основні поняття інформаційної безпеки

З основних понять, що становлять сферу Інформаційної безпеки, можна виділити такі:

a) інформаційна безпека: складний, багатогранний процес, спрямований на забезпечення конфіденційності, цілісності та доступності інформації та інформаційних систем [1]. Забезпечення інформаційної безпеки розглядається не лише як технологічна проблема, але і як комплекс організаційних, правових та технічних заходів;

b) цілісність: гарантія точності та повноти інформації та методів її обробки, що вимагає захисту від несанкціонованої модифікації або знищення даних;

c) доступність: забезпечення доступу до інформації та пов'язаних з нею активів для авторизованих користувачів, які, у свою чергу, мають дозвіл на неї. Окрім класичної тріади КЦД, сучасні стандарти, такі як сімейство документації ISO/IEC 27000, часто включають також принципи автентичності, підзвітності та неспростовності [2];

d) загроза: потенційна причина інциденту, що може призвести до шкоди ІС або організації. Класифікація загроз поділяється на природні (стихійні лиха), випадкові (людський фактор) та умисні (кібератаки, шкідливе програмне забезпечення, втручання у роботу системи) [4];

e) вразливість: слабкість в активі або контролі, яку може використати одна чи кілька загроз. Вразливості можуть існувати у програмному забезпеченні, апаратній частині, організаційних процесах чи персоналі;

f) актив: будь-яка річ, що має цінність для організації, включаючи дані, ІС, апаратне забезпечення та персонал;

g) тріада КЦД: три пункти, до яких належать конфіденційність, цілісність та доступність, що є основними принципами ІБ;

h) конфіденційність: процес забезпечення доступності до інформації лише авторизованим суб'єктам, є основним принципом захисту від несанкціонованого ознайомлення з інформацією.

1.2 Загрози, вразливості та ризики інформаційних систем

Для побудови ефективної методики оцінки захищеності ключовим є розуміння трикомпонентної структури кіберризику, де загроза використовує вразливість для нанесення шкоди активу [3]. Ця взаємодія визначає загальний профіль безпеки будь-якої ІС.

Розглянемо складові цієї структури детальніше:

a) активи є цінними ресурсами, такими як дані, програмне забезпечення, апаратні засоби, репутація та інші. Їх необхідно захищати, бо кожен актив, через свою складність або неправильну конфігурацію, може містити у собі вразливості [6];

b) Вразливість є слабким місцем у архітектурі, дизайні, реалізації або операційному управлінні ІС. Вони можуть бути:

1) технічними: помилка переповнення буфера в коді;

2) організаційними: відсутність політики використання надійних паролів;

3) людськими: недостатня обізнаність персоналу.

Саме на виявлення, ідентифікацію та верифікацію цих слабких місць і спрямований процес пентесту.

c) загрози є зовнішнім або внутрішнім фактором, який має потенціал завдати шкоди системі [5]. У них наявна класифікація за джерелом виникнення:

1) умисні загрози – цілеспрямовані дії зловмисників, хакерів, конкурентів або інсайдерів з метою крадіжки, модифікації та знищення інформації;

2) випадкові загрози – необізнаність персоналу, збої в роботі обладнання, програмні помилки;

3) загрози з боку природи – події, не пов'язані з діяльністю людини, але є прямими діями природних явищ, такі як лісові пожежі, повені, землетруси.

Загроза перетворюється на реальну небезпеку лише тоді, коли вона знаходить відповідну вразливість, яку можна експлуатувати.

Ризик інформаційної системи є кількісною мірою загальної небезпеки, що виникає внаслідок взаємодії загрози та вразливості [4]. Ризик визначається як ймовірність реалізації конкретної загрози та величини потенційного впливу/збитку, який ця реалізація спричинить для активу та має вираз (1.1)

$$Risk = T \times I \tag{1.1}$$

де T – імовірність того, що загроза реалізується, скориставшись вразливістю;

I – величина збитку або впливу на бізнес-процеси у разі успішної реалізації загрози.

Саме пентест досліджує чинник загрози, демонструючи, чи є вразливість практично експлуатованою [7]. Якщо пентестер успішно експлуатує вразливість, це значно підвищує оцінку ймовірності для відповідного ризику. Таким чином, результати пентесту є прямим вхідним параметром для процесу управління інформаційними ризиками.

1.3 Роль тестування на проникнення у забезпеченні ІБ

Тестування на проникнення, або коротко – пентест, є критичним інструментом у забезпеченні інформаційної безпеки, що виконує функцію незалежного аудиту та верифікації захисних механізмів ІС [5]. Його роль виходить за межі простої технічної перевірки, набуваючи стратегічного значення в управлінні ризиками [4].

Розглянемо більш детально, яку роль у забезпеченні безпеки відіграє пентест:

a) верифікація ефективності захисних контролів та архітектури захисту – процес, під час якого відбувається практична та документаційна верифікація того, що встановлені засоби контролю функціонують відповідно до їхнього призначення [7]. Ця перевірка є комплексною і охоплює не лише ізольовані компоненти, а й всю архітектуру. Зокрема, пентест оцінює ефективність багаторівневої архітектури захисту, включаючи перевірку мережевої сегментації та внутрішнього контролю доступу. Успішне горизонтальне переміщення пентестера після початкової компрометації є прямим доказом неефективності сегментації та надмірних прав доступу, що своєю чергою є критичною слабкістю в архітектурі [5]. Крім того, якісний пентест перевіряє не лише здатність системи протистояти атаці, але й здатність команди безпеки виявити, стримати та відреагувати на інцидент, що є важливим елементом операційної безпеки [7];

b) об'єктивність інформаційного ризику та надання рішень – процес пентесту є ключовим джерелом емпіричних даних для процесу управління ризиками, який дозволяє перейти від якісних оцінок до більш об'єктивних [8]. У моделях оцінки ризику, описаних у міжнародній документації, а саме у NIST SP 800-30 [1], ймовірність реалізації загрози може бути якісною. Тому успішна експлуатація, що доведена пентестером, підтверджує цю ймовірність і переводить її у найвищу категорію під назвою "реалізовано" та забезпечує об'єктивність [8]. Ця об'єктивізація, разом із фіксацією реального впливу

компрометації активів, є основою для прийняття фінансово обґрунтованих рішень щодо пріоритезації заходів захисту, оскільки керівництво оперує не гіпотетичними, а документальними підтвердженими загрозами [4]. Таким чином, процес пентесту інтегрується у цикл безперервного покращення СУІБ, що є одним з принципів стандарту ISO/IEC 27000:2018 [2];

с) оцінка нетехнічних вразливостей та бізнес-логіки – процес пентесту, під час якого простежується ефективне поєднання технічного аналізу з нетехнічними векторами [9]. Сценарії соціальної інженерії, до яких належать фішинг та “листи щастя”, дозволяють оцінити людський чинник, що має назву – рівень обізнаності співробітників [3]. Особливість даних процесів, на відміну від автоматизованих дій, полягає у вмінні пентестера виявляти логічні недоліки в унікальних бізнес-процесах, а не лише вже відомі технічні вразливості, що є критичним для забезпечення цілісності бізнес-процесів [9].

1.4 Класифікація пентесту та його етапів

Для забезпечення ефективності тестування на проникнення було створено чітку класифікацію відповідно до цілей, і воно проводиться згідно з формалізованим методологічним циклом [9, 11]. Класифікація визначає обсяг початкової інформації, наданої про цільову систему, що дозволяє точно моделювати поведінку різних класів зловмисників. Тим часом етапи забезпечують послідовність процесу задля необхідності досягнення визначених цілей безпеки [5, 11]. Завдяки цьому забезпечується повне охоплення об'єкта тестування та надається гарантія, що всі ключові вектори атаки будуть належним чином оцінені для досягнення визначених цілей безпеки [5].

Класифікація пентесту за моделлю тестування

1) метод тестування "Чорний ящик" – тестування проводиться без жодної попередньої інформації про внутрішню архітектуру, код чи конфігурацію системи [5]. Цей підхід імітує зовнішнього, неавторизованого зловмисника, який спирається виключно на відкриті джерела інформації та

зовнішнє сканування. Головна мета тестування полягає в оцінці зовнішнього периметру захисту [11];

2) метод тестування "Білий ящик" – під час тестування тестувальнику надається повний доступ до вихідного коду, мережевих схем та внутрішньої документації. Цей підхід імітує інсайдера або цілеспрямовану атаку з використанням вичерпних знань. Це дозволяє провести глибокий аудит коду та виявити логічні помилки та архітектурні недоліки, які часто є недосяжними для зовнішніх атак [9];

3) метод тестування "Сірий ящик" – під час тестування тестувальнику надається часткова інформація, така як облікові дані певного авторизованого користувача, або певний рівень доступу до внутрішньої мережі [14]. Мета полягає в імітації недобросовісного співробітника, який має підвищені привілеї задля перевірки можливостей, які надаються привілейованим особам, та порушення ізоляції даних між користувачами [5].

Етапи пентесту

Ефективний пентест завжди виконується відповідно до стандартизованого циклу, який забезпечує повноту та методологічну послідовність [12, 14]. Хоча існує безліч методологій, що мають різну кількість кроків, було обрано методологію, яку пропонує PTES (Стандарт з виконання тесту на проникнення), зображених у (рис.1.1).

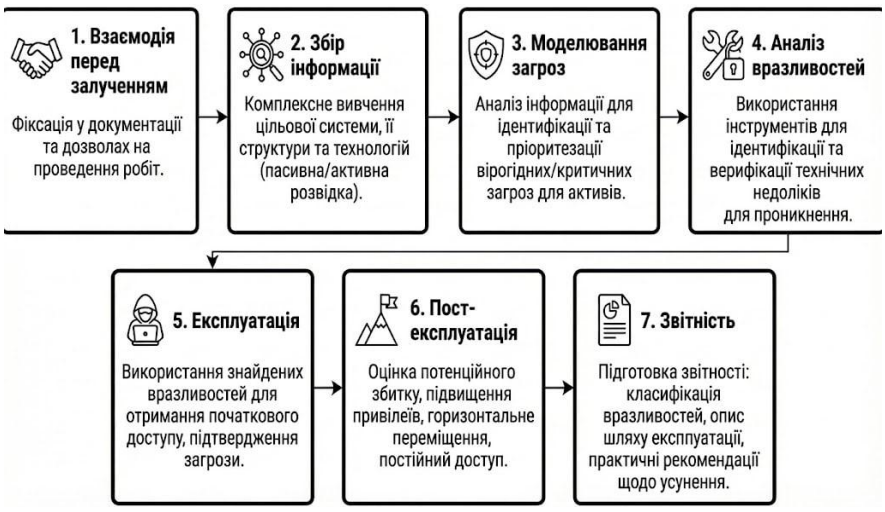

Рис.1.1 Етапи пентесту

1) взаємодія перед залученням – етап, під час якого відбувається фіксація у відповідній документації та дозволах на проведення робіт [11].

2) збір інформації – етап, під час якого ведеться комплексне вивчення цільової системи, її структури та технологій, яке може включати пасивну та активну системи розвідки [5].

3) моделювання загроз – етап, під час якого проводиться аналіз зібраної інформації з метою ідентифікації найбільш вірогідних та критичних загроз для конкретних активів ІС. Метою етапу є визначення пріоритетності вектора атаки [11].

4) аналіз вразливостей – етап, під час якого використовуються автоматизовані та фізичні інструменти для ідентифікації та верифікації технічних недоліків, які можуть бути використані для проникнення.

5) експлуатація – етап, під час якого відбувається використання знайдених вразливостей для отримання початкового доступу до цільової системи або мережі, що є підтвердженням реальності загрози [11].

6) пост-експлуатація – процес, під час якого проводиться оцінка максимального потенційного збитку, що включає підвищення привілеїв, горизонтальне переміщення та встановлення механізмів постійного доступу.

7) звітність – етап, під час якого проводиться підготовка звітності, що повинна містити класифікацію вразливостей, опис шляху експлуатації та конкретні практичні рекомендації щодо усунення вразливостей [10].

1.5 Огляд стандартів та підходів пентесту

Якість та надійність результатів тестування на проникнення прямо залежать від дотримання визнаних міжнародних та галузевих стандартів [8]. Представлені стандарти та підходи, що подані нижче у таблично-порівняльному форматі, надають необхідний методологічний каркас, забезпечуючи професійність, відтворюваність процесу та цілісність звітності [10]. Вони дозволяють інтегрувати пентест в загальний цикл управління

інформаційною безпекою (СУІБ), як того вимагають настанови ISO/IEC 27000-серії [2].

Таблиця 1.1

Порівняння ключових міжнародних стандартів та методологій тестування на проникнення

Стандарт/ Методологія	**Фокус**	**Особливості**	**Роль**
PTES - Стандарт виконання тестування на проникнення	Орієнтована на якість та узгодженість питань виконання тестування на проникнення[11]	Формалізує процес у сім чітких етапів (див. 1.4.2), включаючи фази Моделювання загроз та Пост-експлуатації, які часто ігноруються спрощеними підходами [11]	Слугує ключовим інструментом для керування процесом пентесту та забезпечення його вичерпності
OWASP - Відкритий проект з безпеки веб-застосунків	Комплексне тестування безпеки веб-застосунків та API (Прикладний програмний інтерфейс)	Спільнота створює безкоштовні ресурси, такі як статті, методології, інструменти, документація, задля покращення безпеки ПЗ, допомагаючи розробникам створювати надійніші системи та надаючи інструменти й рекомендації для виявлення та усунення вразливостей [12]. Надає вичерпні сценарії перевірки для всіх класів вразливостей [12], охоплюючи перевірку автентифікації, управління сесіями, валідацію вхідних даних [8]	Використовується як технічний довідник для забезпечення повноти перевірки на етапі аналізу вразливостей та експлуатації
NIST SP 800-115 - Технічний посібник з тестування та оцінювання ІБ	Надання настанов для планування, виконання та документування всіх видів тестування безпеки, включаючи пентест [9]	Стандарт чітко розрізняє три критерії оцінки (тестування, аудит, оцінка) та детально описує етапи тестування, надає структуру для вибору методів тестування відповідно до цілей організації [9]	Слугує методологічною основою для інтеграції технічного тестування в загальну систему управління ІБ в державних та комерційних структурах
OSSTMM - Посібник з методології тестування безпеки з відкритим кодом	Кількісне вимірювання показника безпеки та створення інтегрального показника	OSSTMM пропонує метрики для оцінки стійкості системи та її здатності протистояти атакам. Він охоплює п'ять каналів безпеки (фізичний, логічний, операційний, зв'язок, навчання) і пропонує метрики для розрахунку інтегрального балу захисту системи [13]	Основна роль OSSTMM полягає у наданні метрик для виміру даних з різних векторів для розробки власної комплексної методики в цій кваліфікаційній роботі

Висновок до розділу 1

У Розділі 1 "Теоретичні основи забезпечення інформаційної безпеки та пентесту" були досліджені фундаментальні поняття та методологічні основи, необхідні для подальшої розробки методики комплексної оцінки захищеності одними з таких є фундаментальна роль пентесту, що маж на мет тестування на проникнення є критичним інструментом у забезпеченні інформаційної безпеки, оскільки воно виконує функцію незалежного, проактивного аудиту, що надає практичну верифікацію ефективності захисних механізмів ІС. Була обґрунтована стратегічна роль пентесту в об'єктивізації інформаційного ризику, оскільки успішна експлуатація перетворює гіпотетичну ймовірність загрози на документований факт, що є основою для фінансово обґрунтованих управлінських рішень . Розглянута Класифікація та стандартизація, проаналізовано класифікацію пентесту за рівнем інформованості Black Box, White Box та Grey Box, що дозволяє моделювати різні типи зловмисників. Деталізовано формалізований семиетапний цикл PTES, який забезпечує методологічну послідовність, якість та вичерпність тестування. Проведений огляд методологічних підходів та здійснено огляд провідних міжнародних стандартів, таких як NIST SP 800-115, OWASP WSTG та OSSTMM. Аналіз показав, що, незважаючи на їхню технічну глибину, ці стандарти переважно орієнтовані на процес виконання або аудит відповідності, але не надають уніфікованого та кількісного механізму для агрегації всіх результатів в єдиний інтегральний показник захищеності.

РОЗДІЛ 2
АНАЛІЗ ІСНУЮЧИХ МЕТОДІВЗМІСТ ОЦІНКИ ЗАХИЩЕНОСТІ НА ОСНОВІ РЕЗУЛЬТАТІВ ПЕНТЕСТУ

1.2 Методи аналізу вразливостей

Система “Common Vulnerability Scoring System”, надалі “CVSS” є міжнародним галузевим стандартом, розробленим організацією FIRST (Форум груп реагування на інциденти та безпеку), що призначена для об'єктивного та кількісного оцінювання критичності вразливостей програмного забезпечення та інформаційних систем [18]. Основна її функція полягає у перетворенні якісного опису недоліку на числовий бал від 0.0 до 10.0, що дозволяє швидко ранжувати загрози та надання пріоритетності їх виправлення. Впровадження CVSS забезпечує уніфіковану комунікацію між фахівцями з безпеки, що критично важливо у процесі обробки звітів з пентесту [19,20].

Структура метрик CVSS та обґрунтування базового балу

Загальна система оцінювання вразливостей - “Common Vulnerability Scoring System”, надалі “CVSS”, являє собою відкритий галузевий стандарт, призначений для уніфікації методів оцінки ступеня критичності вразливостей програмного та апаратного забезпечення. Оцінка CVSS не є одновимірним показником; вона є багатокомпонентною і формується на основі складної взаємодії трьох ключових груп метрик. Кожна з цих груп відображає різні аспекти ризику, дозволяючи перейти від суто технічного опису недоліку до розуміння його потенційного впливу на інформаційну систему [21].

1. Базова група метрик – ця група метрик є фундаментом усієї системи оцінювання CVSS. Вона описує внутрішні, притаманні самій вразливості властивості, які залишаються постійними незалежно від часу та специфіки середовища експлуатації [18]. Базова оцінка відображає теоретичну серйозність вразливості у вакуумі, без урахування зовнішніх факторів захисту. Структурно

вона складається з двох підгруп, що формують зв'язок “можливість та наслідок” - метрики використання та метрики впливу.

А) метрики використання - метрики, які характеризують ступінь технічної складності реалізації загрози та умови, необхідні для успішного проведення атаки. Вони відповідають на питання: “Наскільки легко зловмиснику використати цю вразливість?”. До цих метрик належать:

a) вектор атаки - ця метрика визначає ступінь віддаленості зловмисника від цільової системи, необхідний для експлуатації вразливості. Вона класифікує шлях доступу. Найвищий рівень ризику несе значення “Мережевий” (Network - N), оскільки атака може бути здійснена віддалено через глобальні мережі (наприклад, Інтернет) без потреби у фізичному доступі чи присутності в локальному сегменті. Це забезпечує масштабованість атаки. Інші вектори, такі як «Суміжна мережа» (Adjacent - A), “Локальний” (Local - L) та “Фізичний” (Physical - P), передбачають наявність додаткових бар'єрів для атакуючого, що відповідно знижує базовий бал;

b) складність атаки (AC) - метрика оцінює наявність специфічних умов або обставин, які непідконтрольні зловмиснику, але необхідні для успішної атаки. Низька складність (Low - L) означає відсутність таких бар'єрів: успішна атака є тривіальною, повторюваною і не вимагає складних технічних маніпуляцій, таких як отримання позитивних результатів у стані “перегонів”, або специфічної конфігурації пам'яті жертви. Висока складність (High - H) вказує на те, що успіх атаки залежить від випадкових факторів;

c) необхідні привілеї (PR) - метрика визначає рівень авторизації, який повинен мати зловмисник у системі *до* початку експлуатації вразливості. Найбільш критичними є вразливості, що не вимагають привілеїв (None - N), оскільки вони доступні будь-якому не автентифікованому користувачеві. Необхідність середніх (Low - L) або високих (High - H) привілеїв звужує коло потенційних атакуючих до тих, хто вже має певний доступ до системи;

d) взаємодія з користувачем (UI) - метрика показує, чи є обов'язковою умовою успішної атаки певна дія з боку легітимного користувача системи

(наприклад, перехід за фішинговим посиланням, відкриття шкідливого файлу). Відсутність необхідності взаємодії (None - N) підвищує бал, оскільки дозволяє автоматизувати атаку без застосування методів соціальної інженерії;

Б) Метрики впливу – описують найгірші можливі наслідки успішної експлуатації вразливості для активів організації, базуючись на класичній тріаді інформаційної безпеки CIA:

a) конфіденційність: ступінь несанкціонованого розкриття інформації;

b) цілісність: ступінь несанкціонованої модифікації або знищення даних;

c) доступність: ступінь порушення доступу до ресурсу або повна відмова в обслуговуванні.

Кожна з цих метрик оцінюється за шкалою: Вплив відсутній (None — N), Низький (Low — L) або Високий (High — H) [21].

В) Обґрунтування базового балу**:** формула розрахунку базового балу CVSS не є простим середнім арифметичним. Вона базується на складній поліноміальній математичній моделі, розробленій для відображення нелінійної природи ризиків. Ця модель використовує систему вагових коефіцієнтів для гарантії того, що комбінація метрик із найвищим ризиком (особливо мережевий вектор атаки (AV:N) у поєднанні з високим впливом на конфіденційність, цілісність або доступність (C:H, I:H, A:H)) призводить до експоненційного зростання кінцевого балу, наближаючи його до критичних значень 9.0–10.0 [18].

2. Темпоральна група метрик – дана група метрик на відміну від базових, ці метрики не є статичними. Дана група відображає еволюцію ризику, пов'язаного з вразливістю, протягом часу [19]. Включення темпоральних метрик дозволяє коригувати базовий бал залежно від поточного стану середовища загроз. Вони можуть лише знижувати загальний бал або залишати

його незмінним, але ніколи не підвищують його вище базового. До цих метрик належать:

a) зрілість коду експлойту: ця метрика вимірює ймовірність атаки на основі наявності та надійності інструментів експлуатації. Щойно опублікована теоретична вразливість має менший бал ризику, ніж вразливість, для якої вже існує загальнодоступний, автоматизований та надійний («бойовий») експлойт, який не вимагає високої кваліфікації від зловмисника;

b) рівень виправлення: ця метрика оцінює наявність та тип контрзаходів. Якщо постачальник випустив офіційне оновлення безпеки, то бал суттєво знижується, оскільки ризик успішної атаки зменшується для тих, хто застосував виправлення. Тимчасові рішення або обхідні шляхи знижують бал меншою мірою;

c) достовірність звіту: ця метрика визначає ступінь впевненості в існуванні вразливості та точності її технічного опису. Вразливості, підтверджені вендором або незалежними дослідниками з наданням доказів концепції, що мають вищий рівень достовірності, ніж непідтверджені повідомлення.

3. Екологічна група метрик - ця група є найбільш критичною для практичного застосування результатів оцінювання, оскільки вона дозволяє адаптувати загальну оцінку CVSS до контексту конкретної організації, її інфраструктури та бізнес-процесів [20]. Без використання цієї групи оцінка ризику залишається теоретичною. Екологічні метрики дозволяють врахувати бізнес-контекст та наявні засоби захисту. Вони поділяються на дві категорії:

a) вимоги безпеки: організація може самостійно визначити пріоритетність властивостей CIA для конкретного активу. Наприклад, для банківських трансакційних систем Цілісність є критично важливою, що призведе до підвищення кінцевого балу, якщо вразливість впливає саме на цей параметр, навіть якщо базовий вплив був оцінений як середній;

b) модифіковані базові метрики: дозволяє аналітику перевизначити значення базових метрик з урахуванням специфіки конфігурації середовища. Наприклад, якщо вразливість має базовий вектор “Мережевий”, але вразливий сервер знаходиться за надійним міжмережевим екраном, який блокує

відповідний порт, аналітик може змінити вектор на “Суміжний”, або “Локальний» в рамках екологічної оцінки, що знизить підсумковий бал. Примітка: У попередніх версіях стандарту використовувалася метрика “Потенціал супутньої шкоди” (CDP), яка оцінювала фінансові або репутаційні збитки, проте в сучасних ітераціях CVSS акцент зміщено на більш точне коригування базових параметрів**.**

2.2. Стандарти оцінювання ризиків

Окрім специфічних методик для ранжування технічних вразливостей, таких як CVSS (розглянута у 2.1), існують комплексні стандарти та фреймворки, призначені для управління та оцінювання кіберризиків на рівні організаційних процесів. Ці стандарти критично важливі для інтеграції результатів пентесту в загальну систему управління інформаційною безпекою (СУІБ) [14].

Стандарт ISO/IEC 27005 є ключовим елементом сімейства стандартів ISO 27000 і зосереджений виключно на управлінні ризиками інформаційної безпеки [15]. Він не надає конкретної методики обчислення ризику, а є настановою, яка описує циклічний процес управління ризиками. Цей процес складається з п'яти основних етапів:

a) встановлення контексту: Визначення цілей, обсягу, політик та критеріїв ризику.

b) оцінювання ризику: Ідентифікація, аналіз та кількісна/якісна оцінка ризику.

c) обробка ризику: Вибір та впровадження заходів контролю (наприклад, з ISO 27002) для зниження, уникнення, передачі або прийняття ризику.

d) моніторинг та перегляд: Регулярний перегляд ризиків та ефективності контролів.

е) комунікація та консультації: Обмін інформацією щодо ризиків із зацікавленими сторонами [15].

З точки зору пентесту, ISO 27005 забезпечує структуру (рис. 2.1), в яку інтегруються результати тестування. Результати пентесту (виявлені вразливості) є лише входом для фази оцінювання ризику. Стандарт вимагає, щоб кожна вразливість була пов'язана з конкретним активом та бізнес-процесом, що перетворює технічний звіт на фінансово-управлінський документ [16].

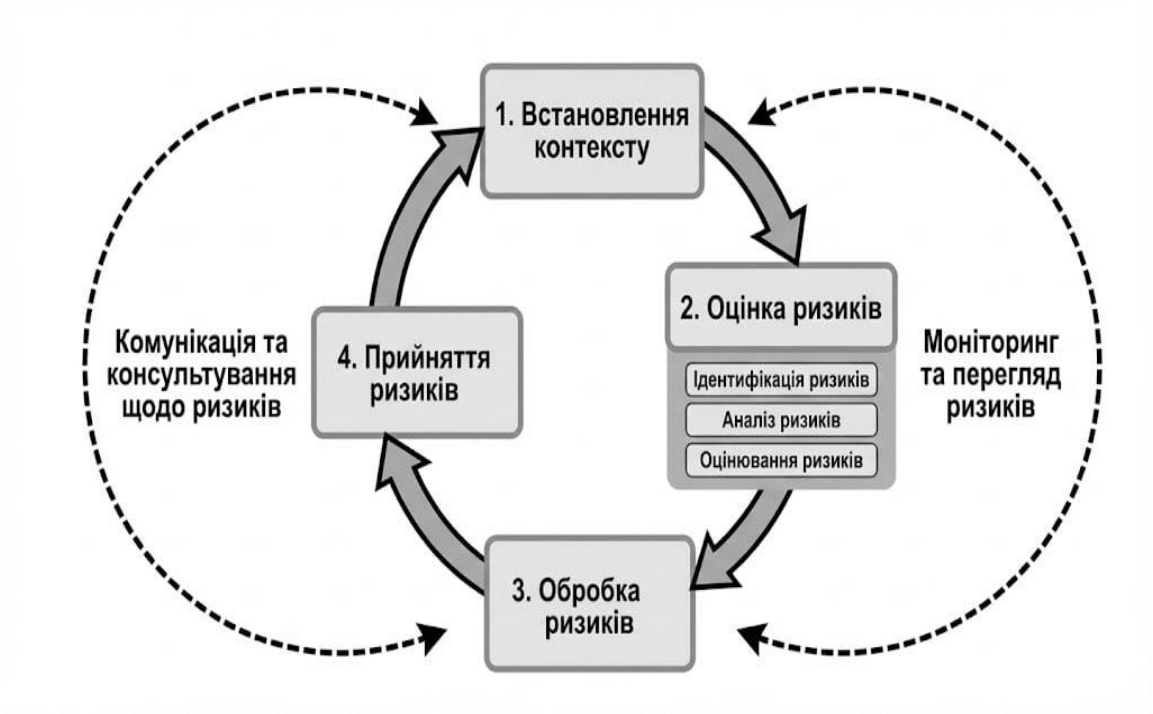

Рис. 2.1 Циклічний процес управління ризиками
згідно з ISO/IEC 27005 [15]

Методологія OCTAVE

Методологія OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) - оцінка критичних операційних загроз, активів та вразливосте, документація розроблена Центром координації CERT (CERT/CC) при Університеті Карнегі-Меллона, представляє собою фундаментальний підхід до управління ризиками інформаційної безпеки. На відміну від суто

технічних методик, OCTAVE є якісним, самокерованим процесом, що фокусується на організаційних аспектах, людському факторі та операційних бізнес-процесах [27]. В основі методології лежить принцип, що ефективна безпека неможлива без глибокого розуміння того, що саме організація намагається захистити і чому.

Ключовою особливістю OCTAVE, що відрізняє її від багатьох інших стандартів управління ризиками (наприклад, NIST SP 800-30 або ISO 27005, які часто передбачають значне залучення зовнішніх аудиторів), є акцент на самостійному застосуванні. Методологія передбачає формування внутрішньої мульти-функціональної команди фахівців самої організації для проведення оцінювання. Такий підхід базується на припущенні, що саме внутрішні співробітники володіють найкращим контекстуальним розумінням специфіки бізнес-процесів та реальної цінності активів [18]. Центральним елементом OCTAVE є ідентифікація та пріоритезації Критичних Інформаційних Активів (КІА). Це інформація, системи або процеси, компрометація яких матиме безпосередній та суттєвий негативний вплив на здатність організації виконувати свою основну бізнес-місію. Фокус зміщується з захисту всієї IT-інфраструктури на захист того, що є дійсно критичним для виживання та функціонування бізнесу.

Методологія OCTAVE реалізується через структурований процес, поділений на три послідовні фази. Кожна фаза керується як операційними вимогами бізнесу, так і критеріями інформаційної безпеки:

фаза 1. Побудова профілю загроз - ця фаза присвячена збору та аналізу знань про організацію. Через серію семінарів та інтерв'ю з персоналом різних рівнів управління визначаються:

a) критичним активами та вимогами безпеки до них (конфіденційність, цілісність, доступність);

b) загрозами цих активів, що сприймаються співробітниками (внутрішні та зовнішні);

с) існуючі практики безпеки та організаційні вразливості (слабкі політики, або недостатня обізнаність персоналу).

Результатом фази є консолідований профіль загроз та список активів, які потребують першочергового захисту.

фаза 2. Ідентифікація вразливостей - на цьому етапі фокус зміщується на технічну інфраструктуру, яка підтримує критичні активи, виявлені у Фазі 1. Проводиться детальний технічний аналіз компонентів систем. Ця фаза часто включає використання інструментальних засобів, таких як автоматизовані сканери вразливостей, а також проведення ручного тестування на проникнення (пентесту) для верифікації технічних недоліків та можливості їх експлуатації. Важливо, що технічний аналіз не є самоціллю, а проводиться виключно в контексті загроз критичним активам.

фаза 3. Розробка стратегії безпеки та плану зниження ризику (Стратегічний погляд) - є фінальною фазою, що присвячена консолідації результатів попередніх етапів для проведення якісного аналізу ризиків. Організація оцінює потенційний вплив виявлених загроз та вразливостей на свою місію. На основі цього аналізу розробляється комплексна стратегія захисту та детальний план дій щодо зниження ризиків до прийнятного рівня [27]. План включає не лише технічні заходи, але й зміни в політиках, процедурах та навчанні персоналу.

Значення OCTAVE в контексті тестування на проникнення полягає у тому, що дана методологія є ідеальним рішенням для комплексного оцінювання стану безпеки на етапі «пост-експлуатації» або після завершення пентесту. Тестування на проникнення надає технічні дані про вразливості результати Фази 2. Застосування OCTAVE вимагає від організації кореляції технічних результатів пентесту з бізнес-цілями та операційними ризиками. Це гарантує, що ресурси на виправлення вразливостей будуть виділені не просто на основі технічної складності базового балу CVSS, а відповідно до реального впливу вразливості на місію організації [28].

Кількісний фреймворк FAIR

Фреймворк FAIR (Factor Analysis of Information Risk) - це міжнародний стандарт, що надає модель для розуміння, аналізу та кількісної оцінки інформаційного ризику у фінансовому вираженні. FAIR є єдиним набором концепцій та визначень, що забезпечує перехід від суб'єктивних якісних оцінок до обґрунтованої кількісної оцінки ризику інформаційної безпеки та операційних ризиків [29]. На відміну від якісного методу OCTAVE, який оперують абстрактними категоріями «високий/середній/низький», FAIR [29] переводить ризик у конкретні фінансові показники - грошові одиниці, що є вирішальним фактором для ефективної комунікації між технічними фахівцями та вищим керівництвом бізнесу.

Фундаментальною відмінністю FAIR є його сутність, яка розкладає ризик на складові фактори. FAIR визначає ризик не як статичну властивість, а як ймовірну частоту та ймовірну величину майбутніх втрат [29]. Математична модель ризику у FAIR базується на взаємодії двох головних компонентів:

1. частота події втрат: цей показник визначає, як часто протягом заданого проміжку часу (зазвичай року) може відбутися подія, що призведе до збитків. LEF, у свою чергу поділяється на:

1) частота подій загрози - як часто агенти загрози (хакери, інсайдери, шкідливе ПЗ) намагаються атакувати актив;

2) вразливість - явище у контексті FAIR , що описує не тільки наявність «діри» в коді (як у CVSS), а ймовірність того, що дії агента загрози будуть успішними, тобто зможуть подолати наявні засоби контролю та захисту за досягнення мети.

2. величина втрат - цей показник оцінює фінансовий вимір збитків у разі успішної реалізації загрози. FAIR вимагає аналізу втрат у двох формах:

а) первинні втрати - безпосередні витрати, що виникають під час інциденту (наприклад, вартість роботи команди реагування, втрата продуктивності, заміна обладнання);

b) вторинні втрати - відкладені у часі наслідки, які виникають через реакцію зовнішнього середовища (штрафи регуляторів, судові позови, втрата клієнтів через репутаційні збитки, зниження вартості акцій).

Такий підхід є критично важливим після етапів технічного пентесту. Якщо CVSS показує технічну серйозність вразливості, а OCTAVE визначає її вплив на місію, то FAIR дозволяє розрахувати показник "Повернення інвестицій у безпеку" (ROSI). Це дозволяє керівництву приймати обґрунтовані рішення щодо усунення вразливостей, придбання додаткових засоби захисту, чи страхування ризиків[29].

Проведемо порівняння стандартів та методологій оцінки ризиків (табл. 2.1)

Таблиця.2.1

Порівняльна характеристика стандартів та методологій оцінки ризиків

Критерій порівняння	**ISO/IEC 27005**	**OCTAVE**	**FAIR**
Тип методології	Рамковий стандарт (Framework) та настанова.	Методологія якісної самооцінки.	Аналітична модель кількісного розрахунку.
Об'єкт дослідження (Фокус)	Побудова процесу управління ризиками та комплаєнс	Критичні активи, операційні процеси, люди	Фінансовий вплив та частота подій
Метрики (Вимірювання)	Гнучкий: дозволяє як якісні, так і кількісні методи	Якісний: шкали (Високий / Середній / Низький)	Кількісний: грошові одиниці, відсотки, частота
Математичний апарат	Не регламентований (залежить від вибору організації)	Відсутній / Мінімальний (базується на експертній думці)	Теорія ймовірностей, статистика, метод Монте-Карло
Необхідні ресурси	Ризик-менеджери, аудитори, спеціалісти з комплаєнсу	Внутрішня команда (бізнес + IT), знання процесів	Аналітики даних, статистика інцидентів
Ключовий результат (Output)	Реєстр ризиків, план обробки, відповідність стандартам	Профіль загроз, стратегія захисту, карта активів	Звіт про Value at Risk (VaR), крива збитків, ROSI
Цільова аудиторія	Регулятори, аудитори, вищий менеджмент	Операційні менеджери, IT-персонал	Фінансовий директор (CFO), Рада директорів

2.3 Науково-методичні підходи до побудови інтегральних показників захищеності інформаційних систем

Проведений у підрозділах 2.1 та 2.2 критичний аналіз існуючих стандартів та методологій оцінювання ризиків дозволяє констатувати наявність суттєвого методологічного розриву. Жоден із розглянутих інструментів у своєму «чистому» вигляді не здатен повною мірою задовольнити комплексні потреби управління інформаційною безпекою, що виникають безпосередньо після проведення тестування на проникнення (пентесту) [16, 24].

Проблематика існуючих підходів

Основна проблема полягає у різнорідності вихідних даних та цільового призначення наявних методик:

1) CVSS є високоефективним, але вузькоспеціалізованим технічним стандартом. Він надає «мікроскопічний» погляд на окрему вразливість, ігноруючи архітектурну та бізнес-значимість вузла, на якому вона виявлена. Це призводить до ситуацій, коли критична вразливість на тестовому сервері отримує той самий бал, що й на продуктивній базі даних.

2) OCTAVE та ISO/IEC 27005 пропонують системний, процесно-орієнтований підхід. Проте вони є переважно якісними, вимагають значних часових витрат на експертні сесії та погано масштабуються для оперативного ранжування сотень технічних недоліків, що генеруються автоматизованими сканерами під час аудиту [14].

3) FAIR вимагає значного обсягу статистичних даних для моделювання, яких у організації може не бути на момент завершення пентесту.

Концепція Інтегрального Показника Безпеки

З огляду на виявлені обмеження, виникає об’єктивна потреба у розробці та впровадженні Інтегрального Показника Безпеки, надалі - ІПБ. ІПБ визначається як згортка різнорідних метрик (технічних, експлуатаційних та економічних) у єдину скалярну величину, що характеризує поточний рівень захищеності активу або системи в цілому.

Для забезпечення прикладної ефективності, розроблюваний ІПБ повинен відповідати наступним критеріям якості:

1) об'єктивність - розрахунки мають виступати стандартизовані, верифіковані технічні дані. Найкращим кандидатом для цієї ролі є метрики CVSS, оскільки вони є універсальними та відтворюваними незалежно від суб'єктивної думки аудитора.

2) Контекстуальність - показник повинен динамічно адаптуватися до середовища функціонування. Це передбачає врахування критичності конкретного активу для бізнес-процесів, що корелює з принципами методологій OCTAVE та FAIR. Вразливість на критичному активі повинна мати вищу вагу у підсумковій оцінці.

3) якісність - результатом оцінювання має бути чіткий числовий показник у діапазоні від 0 до 1, або від 0 до 100. Це дозволяє керівництву відслідковувати динаміку змін та встановлювати KPI для підрозділів безпеки [17].

Математичні методи побудови ІПБ

Побудова такого показника, який би ефективно відображав загальний рівень захищеності системи на основі різнорідних результатів пентесту, вимагає використання методів теорії прийняття рішень, зокрема багатофакторного аналізу та методу зважених сум (Weighted Sum Model - WSM).

Загальний вигляд адитивної моделі згортки для розрахунку ІПБ можна представити як (2.1):

$$\sum_{i=1}^{n} w_i * P_i = I_{add} \qquad (2.1)$$

де:

I_{add} — інтегральний показник;

P_i — нормалізоване значення і-го окремого показника (наприклад, оцінка вразливості або доступності);

wi — ваговий коефіцієнт, що визначає значущість і-го показника, причому обов'язковою умовою є нормування ваг (2.2):

$$\sum_{i=1}^{n} w_1 = 1 \tag{2.2}$$

Переваги та обмеження - цей метод легко інтерпретувати: внесок кожного фактора у загальну оцінку є пропорційним його вазі. Однак, його головним недоліком у контексті безпеки є компенсаційний ефект. Це означає, що критично низьке значення одного показника безпеки може бути «перекрите» (компенсоване) високими значеннями інших показників. Якщо система має критичну вразливість (низький рівень безпеки), але дуже високу фізичну захищеність, адитивна модель може показати «середній» рівень ризику, що не відповідає дійсності, оскільки система все одно буде скомпрометована [32]. Тому адитивний метод вимагає надзвичайно точного та обґрунтованого визначення вагових коефіцієнтів wi.

Метод мультиплікативної згортки

Мультиплікативний підхід базується на перемноженні частинних критеріїв і використовується в нелінійних моделях оцінювання. Формула розрахунку має вигляд (2.3):

$$I_{mult} = \prod_{i=1}^{n} P_i^{w_1} \tag{2.3}$$

Переваги та обмеження – мультиплікативна згортка краще відображає природу ризикових систем завдяки ефекту «вето» або відсутності повної компенсації. Це означає, що якщо значення одного з критичних факторів наближається до нуля (ймовірність загрози є нульовою), то і загальний

інтегральний показник також дорівнюватиме нулю, незалежно від величини інших факторів (величини потенційних збитків). Однак, мультиплікативний метод є складнішим у стандартизації та інтерпретації. Він дуже чутливий до шкали вимірювання вхідних даних (використання логарифмічного або експоненціального перетворення показників є необхідним для уникнення спотворення результатів) [32].

Врахування контексту та критичності активів

Ключовим недоліком стандарту CVSS є відсутність автоматичного зв'язку між технічною вразливістю та бізнес-критичністю активу. Вразливість з високим балом на тестовому сервері несе менший ризик, ніж вразливість із середнім балом на продуктивній базі даних. Для побудови ефективного Інтегрального Показника Безпеки (ІПБ) необхідно ввести зважений фактор критичності K_j для кожного активу j (веб-сервер, база даних клієнтів, контролер домену).

Методика ранжування критичності (K_j).

Вона має ґрунтуватися на принципах, подібних до методології OCTAVE, оцінюючи:

1) Бізнес-вплив: Фінансові та репутаційні втрати у разі компрометації.

2) Юридичні та регуляторні вимоги: Штрафи за порушення GDPR, HIPAA або українського законодавства (наприклад, ЗУ "Про захист інформації...").

3) Шкала оцінки - критичність Kj оцінюється за шкалою від 1 до 5, де 5 – критичний актив, який несе найбільший ризик для місії організації.

2.4 Недоліки CVSS при реальній оцінці безпеки після пентесту

Хоча CVSS залишається стандартом де-факто для оцінки вразливостей, її застосування без модифікацій у звітах з тестування на проникнення (пентесту) створює суттєві методологічні розриви. Пентест має бути орієнтований на

бізнес-ризик, тоді як CVSS у "чистому" вигляді фокусується на технічній тяжкості.

Ці розриви роблять кінцевий бал CVSS недостатнім інструментом для управлінської пріоритезації виправлень, оскільки він не відображає реальну загрозу для конкретної організації [24, 16].

Ігнорування контексту активу та бізнес-критичності

Ключова проблема полягає у контекстно-незалежному характері Базового балу (CVSS Base Score) [18]. Цей бал описує виключно технічні характеристики вразливості, повністю ігноруючи цінність та роль скомпрометованого активу в інфраструктурі.

Розглянемо вразливість типу "Віддалене виконання коду" (Remote Code Execution - RCE), яка технічно оцінюється критично високим балом CVSS Base = 9.8. Без врахування контексту, цей бал буде ідентичним для двох діаметрально різних сценаріїв:

1) Сценарій А (Низький ризик) - вразливість виявлено на застарілому архівному веб-сервері, який ізольовано від мережі і не містить актуальних даних.

2) Сценарій Б (Критичний ризик) - вразливість виявлено на основному сервері баз даних, що містить персональні дані клієнтів і підключений до платіжних шлюзів.

Наслідок - формально обидві проблеми мають однаковий пріоритет (9.8), що дезорієнтує IT-персонал і призводить до неефективного витрачання ресурсів на захист неважливих активів.

Конфлікт з методологіями управління ризиками (ISO) - недолік стає критичним на етапі Обробки ризику згідно зі стандартом ISO 27005 [15]. Вище керівництво оперує поняттями Критичних Інформаційних Активів (КІА) [28] та бізнес-впливу, а не технічними параметрами експлойту. CVSS передбачає вирішення цієї проблеми через групу метрик середовища. Однак на практиці фахівці часто ігнорують цю групу через складність обґрунтування конкретних значень модифікаторів, високу суб'єктивність оцінки та відсутність

автоматизованих інструментів для масового розрахунку контексту, що робить кінцевий звіт з пентесту "відірваним від реальності" та неповноцінним інструментом для прийняття бізнес-рішень [20].

Недооцінка з'єднаності та ланцюгів атак

Модель CVSS за своєю архітектурою розроблена для оцінки окремої вразливості в ізоляції. Вона не враховує синергетичний ефект, коли комбінація вразливостей з низьким або середнім балом може призвести до критичної компрометації системи [22]. Сучасні атаки рідко базуються на одній помилці. Хакери використовують ланцюги атак (Attack Chains) або графи атак, послідовно експлуатуючи слабкі місця для просування вглиб мережі. Механізм ланцюга атак під час пентесту часто реалізується сценарій, де вразливості виступають сходинками до головної цілі.

Розглянемо приклад, де низький ризик стає критичним у контексті ланцюжка:

Крок 1 (Вхід):

a) вразливість 1: розкриття внутрішньої IP-адреси або версії ПЗ.

b) CVSS: 3.5 (Low).

c) роль: дозволяє зловмиснику розвідати топологію мережі.

Крок 2 (Закріплення):

a) вразливість 2: локальне підвищення привілеїв на внутрішньому сервері.

b) CVSS: 5.0 (Medium).

c) роль: дозволяє отримати права адміністратора на проміжному вузлі.

Крок 3 (Ціль):

a) вразливість 3: неправильна конфігурація LDAP або слабкий пароль адміністратора домену.

b) CVSS: 8.5 (High).

c) роль: повна компрометація домену.

Проблема ізольованої оцінки - якщо оцінювати вразливість 1 ізольовано, згідно зі стандартними політиками патч-менеджменту, її виправлення буде

відкладено як "нетермінове" або взагалі проігноровано, однак, без цієї вразливості зловмисник не зміг би розпочати атаку на вразливість 2.

Відсутність прямого зв'язку з фінансовим виміром ризику (FAIR)

Одним з головних викликів для сучасної СУІБ (Системи управління інформаційною безпекою) є переклад технічних показників у фінансові еквіваленти ризику, зрозумілі для фінансового департаменту та виконавчого керівництва (C-level) [16]. CVSS за своєю природою є чисто ординарною (ранговою) шкалою в діапазоні від 0.0 до 10.0. Це означає, що вона сортує вразливості за порядком, але не має внутрішньої інтеграції з кількісними фреймворками, такими як FAIR (Factor Analysis of Information Risk) [29].

1. Проблема масштабування та лінійності

Хоча бал 9.0 класифікується як "Критичний", математично неможливо точно сказати, наскільки він гірший за бал 8.0 у термінах реальних збитків. Шкала CVSS нелінійна і не корелює напряму з грошовими втратами. Для моделей типу FAIR ключовим є показник PLM (Probable Loss Magnitude — Ймовірна величина втрат).

2. Проблема маппингу

Для використання CVSS у фінансових моделях виникає необхідність у штучному "картуванні". Це процес, де діапазони балів зіставляються з діапазонами потенційних фінансових втрат, CVSS 9.0–10.0 Втрати > 5 млн. грн; CVSS 7.0–8.9 Втрати 1–5 млн. грн; Такий підхід вносить значний елемент суб'єктивності та потребує додаткового ручного аналізу, що суперечить ідеї автоматизації та знижує довіру до кінцевих розрахунків [30].

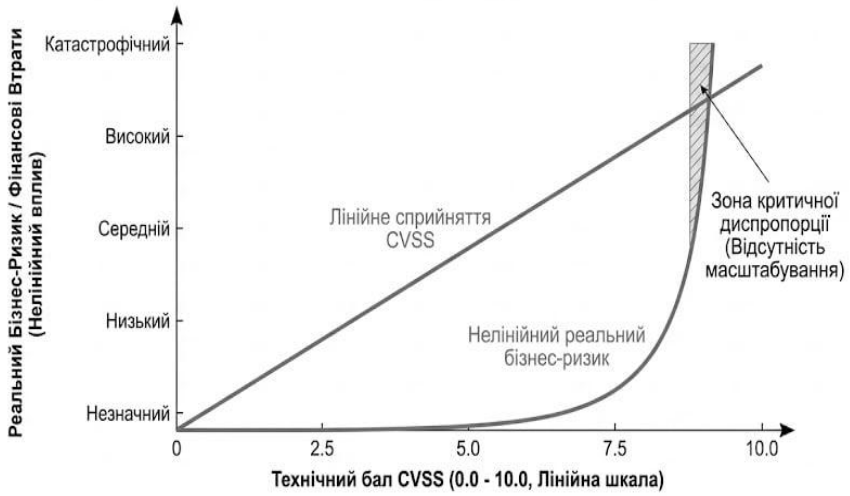

Рис. 2.2 Диспропорція між лінійним технічним балом CVSS та нелінійним реальним бізнес-ризиком [29, 30].

Розглянемо опис рисунка 2.2 під назвою: "Диспропорція між лінійним технічним балом CVSS та нелінійним реальним бізнес-ризиком".

Рисунок 2.2 є графічною ілюстрацією фундаментальної методологічної проблеми при використанні "сирих" балів CVSS для оцінки бізнес-впливу. Діаграма візуалізує розрив між технічною оцінкою тяжкості вразливості та її реальними фінансовими або операційними наслідками для організації.

Графік побудовано у двовимірній системі координат:

1. горизонтальна вісь (X) представляє "Технічний бал CVSS" на стандартній лінійній шкалі від 0.0 до 10.0.

2. вертикальна вісь (Y) відображає "Реальний Бізнес-Ризик / Фінансові Втрати". Ця шкала є якісною та нелінійною, зростаючи від "Незначного" до "Катастрофічного" рівня впливу.

На діаграмі зображено дві криві, що демонструють різні моделі сприйняття ризику:

1. синя пряма лінія ("Лінійне сприйняття CVSS"): Відображає теоретичне, часто помилкове припущення, що зростання балу CVSS прямо пропорційне зростанню бізнес-ризику. Згідно з цією моделлю, вразливість з

балом 5.0 несе середній ризик, а 10.0 — катастрофічний, зі стабільним кроком зростання загрози.

2. червона експоненційна крива ("Нелінійний реальний бізнес-ризик"):

Демонструє емпіричну реальність. Крива показує, що вразливості з низькими та середніми балами CVSS (приблизно до 7.0) часто мають незначний або низький реальний вплив на бізнес (через відсутність експлойтів, ізоляцію активів тощо). Проте, при наближенні до високих балів (8.5+), крива різко йде вгору, переходячи у вертикальне зростання. Це означає, що різниця між балами 9.0 і 10.0 у реальних фінансових втратах може бути колосальною, а не лінійною

Ключовий елемент діаграми є заштрихована область у правому верхньому куті, позначена як "Зона критичної диспропорції (Відсутність масштабування)". Ця зона візуалізує масивний розрив між лінійним очікуванням (синя лінія) та катастрофічною реальністю (червона крива) для критичних вразливостей. Вона підкреслює нездатність стандартної шкали CVSS адекватно відобразити екстремальний рівень загрози, що призводить до недооцінки ризиків у критичному діапазоні.

Суб'єктивність та обмеженість метрик Темпоральної Групи

Темпоральна група метрик у стандарті CVSS була розроблена для динамічної корекції оцінки ризику з плином часу (наприклад, при появі експлойту або випуску патчу). Однак, на практиці застосування цих метрик має суттєві обмеження, що знижують точність кінцевої оцінки [19].

Основні проблеми цієї групи метрик:

1. Зрілість коду експлойту - ця метрика є якісною і значною мірою залежить від інтерпретації аналітика.

Проблема суб'єктивності: фахівці часто розходяться у думках при класифікації експлойтів. Наприклад, важко провести чітку межу між наявністю "робочого прототипу", який вимагає модифікації, та повноцінно "функціональним" експлойтом, готовим до масового використання.

Наслідок: різна інтерпретація одного й того ж експлойту різними вендорами сканерів вразливостей призводить до неузгодженості балів [24].

2. рівень виправлення - згідно з алгоритмом CVSS, технічний бал вразливості автоматично знижується, як тільки виробник ПЗ випускає офіційний патч.

Проблема реального часу: цей механізм ігнорує реальний цикл оновлення в організації. Процес тестування та розгортання оновлення у великій інфраструктурі може тривати тижні або місяці.

Парадокс ризику: формально бал CVSS знижується (бо патч існує "у світі"), але реальний ризик для системи залишається критично високим до моменту фактичного встановлення оновлення [31].

Висновки до розділу 2

У другому розділі проведено комплексний аналіз існуючих підходів до оцінки вразливостей інформаційних систем, зокрема стандарту CVSS (Common Vulnerability Scoring System). Встановлено, що попри статус галузевого стандарту для технічної класифікації вразливостей, CVSS у своїй базовій формі є недостатнім інструментом для оцінки реального бізнес-ризику та пріоритезації заходів захисту. У підсумку були виявлені методологічні розриви між технічною оцінкою CVSS та реальним впливом на організацію свідчать про необхідність вдосконалення процесу оцінки. Існує об'єктивна потреба у розробці Інтегрального Показника Безпеки та адаптивної методики, яка б використовувала CVSS як базову метрику, але динамічно коригувала її з урахуванням ваги активів, наявних компенсаційних контролів та топології загроз.

РОЗДІЛ 3
РОЗРОБКА МЕТОДУ КОМПЛЕКСНОЇ ОЦІНКИ ЗАХИЩЕНОСТІ ЗА РЕЗУЛЬТАТАМИ ПЕНТЕСТУ

3.1 Концептуальна модель методу

В основу розробленої методики покладено перехід від статичної оцінки вразливості до динамічного профілювання ризику. Концептуальна модель базується на гіпотезі, що реальний ризик (R) є функцією не лише від технічної тяжкості вразливості (V), але й від контексту активу (A) та ефективності середовища захисту (E) [33].

Ключовою особливістю розробленої моделі є введення фільтрів контексту. На відміну від стандартного CVSS, де кожен актив рівнозначний [34], наша модель пропускатиме вразливості через сітку бізнес-критичності. Це дозволяє математично зменшити вагу вразливостей на неважливих системах і експоненційно збільшити вагу на критичних вузлах, що узгоджується з рекомендаціями фреймворку управління ризиками ISO/IEC 27005 [35].

Формування системи показників безпеки

Для математичної формалізації методики необхідно визначити набір змінних, які будуть брати участь у розрахунку. На основі стандартів NIST SP 800-30 [36] та методології OCTAVE [37], пропонується розглянути табл. 3.1 , що має у собі систему показників.

Таблиця 3.1

Система показників для розрахунку контекстного ризику

Позначення	Назва показника	Опис та джерело даних	Діапазон значень
Vbase	Базовий бал	Технічна оцінка вразливості згідно з CVSS v3.1. Отримується автоматично зі сканерів [2].	0.0 - 10.0

Продовження таблиці 3.1

Позначення	**Назва показника**	**Опис та джерело даних**	**Діапазон значень**
Kcrit	Коефіцієнт критичності активу	Визначає важливість активу для бізнес-процесів. Враховує втрату конфіденційності, цілісності та доступності [38].	1.0 - 5.0
F_{exp}	Фактор експозиції	Характеризує доступність вразливого інтерфейсу для зловмисника [39].	0.2 - 1.0

Також деталізуємо метрику критичності активу Kcrit, оскільки вона є вирішальною для бізнес-орієнтованого підходу. Пропоную використовувати дискретну шкалу (табл. 3.2), що була адаптована згідно до методики класифікації інформаційних об'єктів НД ТЗІ [41].

Таблиця 3.2

Деталізований огляд критичності активу Kcrit

Рівень	**Kcrit**	**Характеристика активу**	**Приклади**
Критичний	5.0	Активи, простій або компрометація яких зупиняє основну діяльність компанії.	База даних клієнтів, Core Banking System, Контролер домену.
Високий	4.0	Важливі виробничі системи. Збій призводить до фінансових втрат, але не зупиняє бізнес повністю [10].	Поштовий сервер, CRM, внутрішній документообіг.
Високий	4.0	Важливі виробничі системи. Збій призводить до фінансових втрат, але не зупиняє бізнес повністю [42].	Поштовий сервер, CRM, внутрішній документообіг.
Середній	3.0	Допоміжні системи. Є обхідні шляхи роботи.	Внутрішній портал, сервер розробки (Dev).
Низький	1.0	Тестові середовища, ізольовані сегменти, архіви.	Sandbox, Test environment, принтери.

Алгоритм обробки результатів пентесту

Реалізація методики передбачає виконання чіткого алгоритму дій після завершення фази сканування та тестування. Алгоритм забезпечує перетворення технічних даних у пріоритезований реєстр ризиків з урахуванням моделі MITRE ATT&CK [43] (рис.3.1).

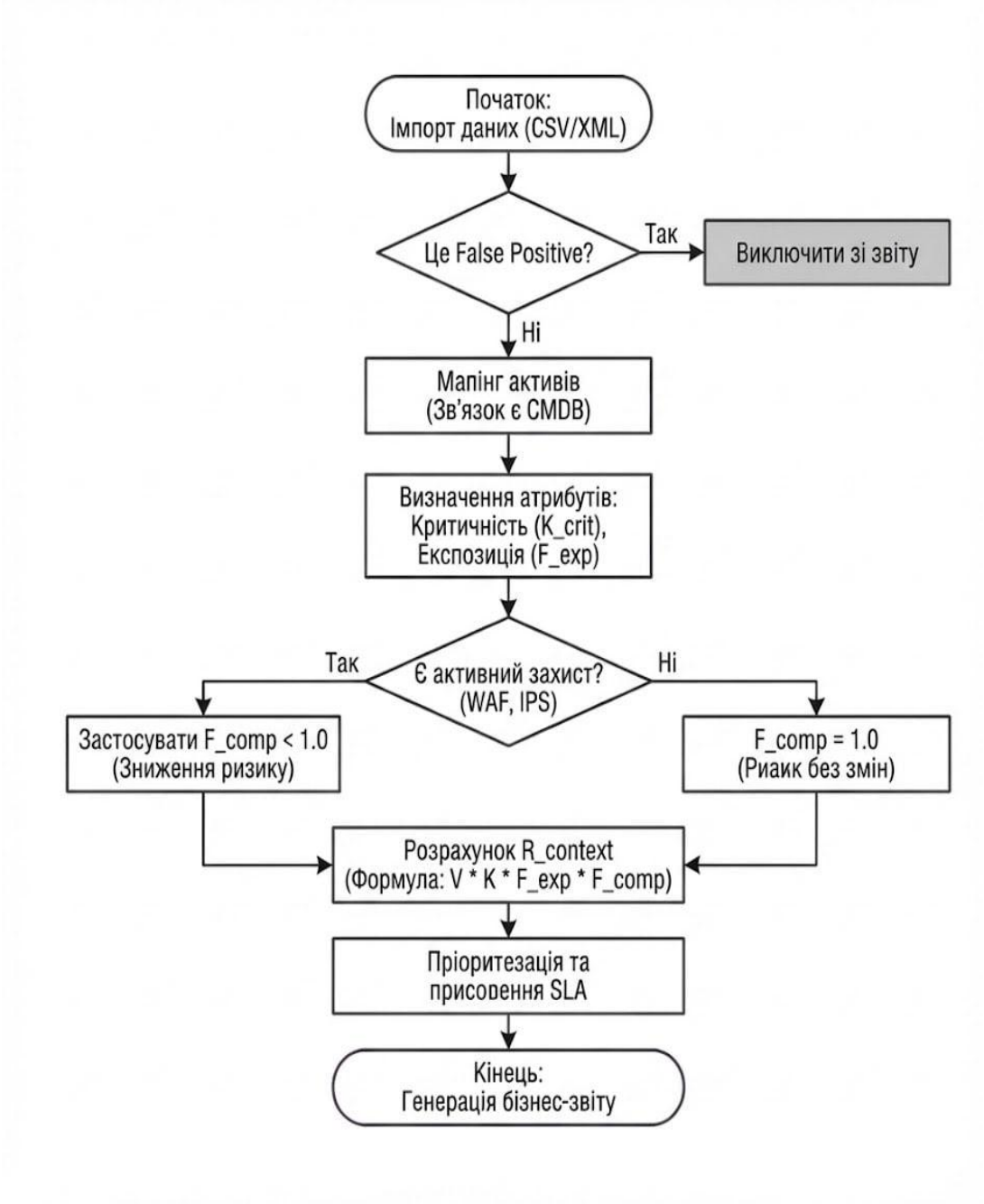

Рисунок 3.1 Алгоритм перетворення технічних даних від набору даних сканера до готового звіту

Розробка моделі та шкали оцінювання

На основі визначених показників пропонується наступна математична модель розрахунку Контекстного Ризику ($R_{context}$) для кожної окремої вразливості. Модель використовує мультиплікативний підхід, що дозволяє реалізувати логіку "нульового ризику", якщо загроза повністю компенсована, ризик прямує до нуля, яка є стандартом у сучасних системах поводження з ризиками [45].

Формула розрахунку Контекстного Ризику:

$$R_{context} = V_{base} * K_{crit} * F_{exp} * F_{comp} \quad (3.1)$$

Оскільки діапазон значень нової метрики ,були відібрані та становлять діапазон від 0 до 50, введено нову шкалу інтерпретації результатів (табл. 3.3)

Таблиця 3.3

Шкала оцінювання та рівні реагування [46]

Діапазон	**Рівень ризику**	**Кольорове маркування**	**Рекомендована дія (SLA)**
40.0 - 50.0	Критичний (Critical)	Червоний	Негайне виправлення (24 години)
20.0 – 39.9	Високий (High)	Помаранчевий	Виправлення у найближче вікно обслуговування (до 14 днів)
10.0 – 19.9	Середній (Medium)	Жовтий	Планове виправлення (до 45 днів)
0.0 – 9.9	Низький (Low)	Зелений	Прийняття ризику (до 90 днів)

3.2. Проведення пентесту обраного об’єкту

Для практичного застосування розробленої методики та перевірки гіпотези про ефективність контекстної оцінки ризику було розгорнуто віртуальний випробувальний стенд. Архітектура стенду спроектована таким чином, щоб емулювати типову багатофункціональну корпоративну інфраструктуру, яка містить власні сервіси, внутрішні ресурси та заходи з захисту.

Експериментальне дослідження проводилося методом “Black Box”, іншими словами тестування методом “чорної скриньки”, де дослідник/пентестер не має попередніх знань про внутрішню будову системи, що імітує дії зовнішнього зловмисника.

Архітектура та конфігурація тестового середовища

Тестове середовище було реалізовано з використанням гіпервізора VMware ESXi / Oracle VirtualBox, що дозволило створити ізольовану віртуальну мережу. Топологія мережі розділена на три логічні зони безпеки, розділені віртуальним фаєрволом (табл.3.4).

Таблиця 3.4

Опис конфігурації тестового майданчика

Роль у мережі	ОС / ПЗ	Мережева зона	Опис активу
Нападник	Kali Linux 2023.2	External (WAN)	Робоча станція пентестера з попередньо встановленим інструментарієм (Metasploit, Nmap, Burp Suite)
1 ціль - Web-Server	Ubuntu Server 20.04 (Apache, PHP 7.4)	DMZ (192.168.10.x)	Публічний веб-сервер. Розміщує вразливий веб-додаток: DVWA – Damn Vulnerable Web App, для емуляції E-commerce платформи
2 ціль - Database	Windows Server 2019 (MySQL 5.7)	LAN (192.168.20.x)	Внутрішній сервер баз даних. Містить таблиці з «чутливими даними» клієнтів. Доступ з WAN заблоковано фаєрволом

Продовження таблиці 3.4

3 ціль - Legacy	Windows 7 SP1 (Unpatched)	LAN (192.168.20.x)	Застаріла робоча станція адміністратора, що використовується для управління інфраструктурою
Firewall	pfSense 2.6.0	Edge	Забезпечує сегментацію мережі, NAT та правила фільтрації трафіку між WAN, DMZ та LAN

Описана конфігурація у таблиці 3.4 конфігурація дозволяє змоделювати сценарії, де вразливості мають різний контекст: від прямої доступності з Інтернету до глибоко ешелонованої оборони.

Методологія та інструментарій тестування

Процес тестування на проникнення виконувався відповідно до стандарту Penetration Testing Execution Standard (PTES) і складався з чотирьох послідовних фаз. Використаний інструментарій для кожної фази наведено таблиці 3.5.

Таблиці 3.5

Етапи пентесту та використані інструменти

Фаза	Завдання	Використаний інструментарій
Розвідка	Визначення активних хостів, відкритих портів, версій ОС та сервісів.	Nmap (Network Mapper), Masscan, Netdiscover.
Сканування вразливостей	Автоматизований пошук відомих CVE (Common Vulnerabilities and Exposures).	Nessus Professional, OpenVAS (Greenbone).
Верифікація	Підтвердження наявності вразливості шляхом безпечної експлуатації (Proof-of-Concept).	Metasploit Framework (MSFconsole), Hydra (Brute-force), SQLmap.
Пост-експлуатація	Оцінка можливості просування мережею (Lateral Movement) та доступу до даних.	Mimikatz, PowerSploit.

Обробка отриманих результатів у ході пентесту

Після завершення активних дій фази сканування та експлуатації було зібрано масив даних, який потребував структурного перегляду перед

застосуванням розробленої методики оцінки. Під час автоматизованого сканування за допомогою сканера Nessus було виявлено загалом 54 вразливості (рис.3.2) та (табл.3.6), проте звіт сканера класифікує їх виключно за базовим балом CVSS, не враховуючи топологію стенду.

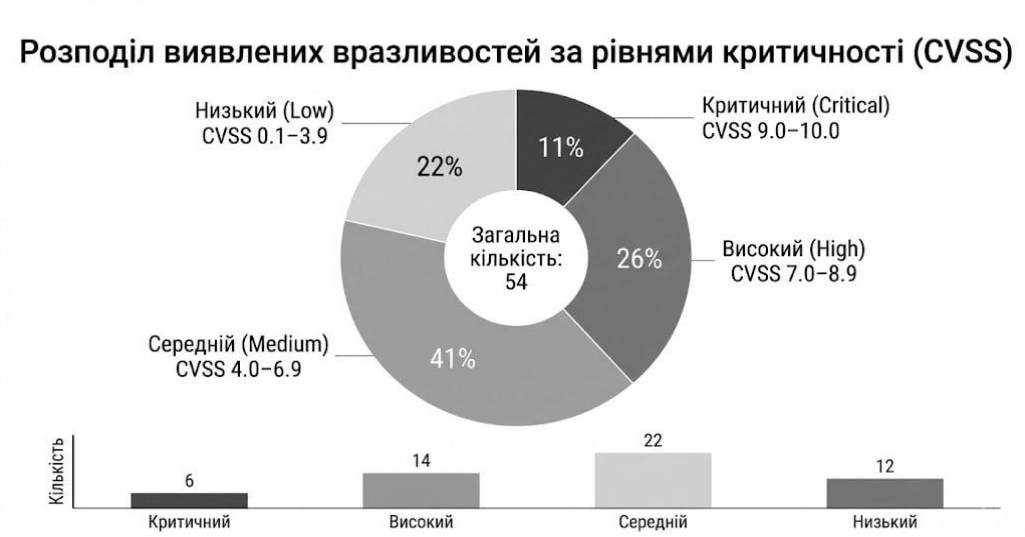

Рисунок 3.2 Розподіл виявлених вразливостей за рівнями критичності

Таблиця 3.6

Реєстру вразливостей для оцінювання

Вразливість (CVE)	**Опис загрози**	**Актив (Хост)**	**Базовий бал CVSS**
CVE-2021-44228	Log4Shell (RCE). Дозволяє виконання довільного коду через Java-логер	Web-Server (DMZ)	10.0 (Critical)
CVE-2017-0144	EternalBlue (SMB RCE). Експлуатація протоколу SMBv1	Database (LAN)	9.3 (Critical)
CWE-89	SQL Injection (Blind). Впровадження SQL-коду у форму входу	Web-Server (DMZ)	8.0 (High)
CWE-79	XSS (Reflected). Міжсайтовий скрипт	Web-Server (DMZ)	6.1 (Medium)
CVE-2019-0708	BlueKeep (RDP RCE). Вразливість служби віддалених робочих столів	Legacy PC (LAN)	9.8 (Critical)

3.3 Застосування розробленого методу

Під час цього етапу я виконаю розрахунок Інтегрального Показника Безпеки (ІПБ) для відібраних контрольних вразливостей, виявлених у ході

пентесту (див. п. 3.2). Метою моїї розрахунків є отримання контекстного балу ризику ($R_{context}$), який дозволить переоцінити реальну загрозу активів для бізнесу.

Розрахунок буде виконуватися згідно з математичною моделлю, обґрунтованою у підрозділі пунту 3.1, за формулою:

$$R_{context} = V_{base} * K_{crit} * F_{exp} * F_{comp} \quad (3.2)$$

Визначення коефіцієнтів контексту

За для правильного виконання розрахунків необхідно формалізувати параметри середовища для кожного активу тестового стенду. Значення коефіцієнтів визначаються на основі шкал, розроблених у Таблицях 3.1–3.2.

Таблиця 3.7

Параметри середовища для кожного активу

Назва активу	**Роль у системі**	**Критичність (K_{crit})**	**Експозиція (F_{exp})**	**Захист (F_{comp})**
“Web Server	Публічний фронтенд E-commerce	4.0 Зупинка призведе до втрати продажів, але база даних ізольована	1.0 Доступний з Інтернету (порти 80/443)	0.8 Налаштовано базові iptables, WAF відсутній
“Database”	Сховище персональних даних	5.0 Витік даних є неприпустимим (репутація, штрафи)	0.5 Розміщений у VLAN, доступ тільки через VPN або компрометований веб	0.9 Встановлено антивірус, але патчинг ОС нерегулярний
“Legacy PC”	Робоча станція секретаря	1.0 Не бере участі в основних бізнес-процесах	0.5 Доступ тільки з внутрішньої мережі	1.0 Захист відсутній, ОС Windows 7 (End-of-Life)

Розрахунок контекстного ризику

Проведемо розрахунок для п'яти контрольних вразливостей, ідентифікованих у таблиці 3.6

Розрахунок 1: Log4Shell на Web-Server

V_{base} = 10.0 $CVSS_{Critical}$

R_{ctx} = 10.0 * 4.0 * 1.0 * 0.8 = 32.0

Висновок: ризик залишається у зоні High/Critical. Вразливість вимагає негайної реакції.

Розрахунок 2: EternalBlue на Database

V_{base} = 9.3$CVSS_{Critical}$

R_{ctx} = 9.3 * 5.0 * 0.5 * 0.9 = 20.9

Висновок: попри високий технічний бал, реальний ризик знижено до межі High/Medium через відсутність прямого доступу з Інтернету.

Розрахунок 3: SQL Injection на Web-Server

V_{base} = 8.0 $CVSS_{High}$

R_{ctx} = 8.0 * 4.0 * 1.0 *0.8 = 25.6

Висновок: ризик зріс відносно 2 розрахунку. Технічно 3 (8.0) слабша за 2 (9.3), але для бізнесу вона небезпечніша, бо знаходиться на периметрі F_{exp}=1.0.

Розрахунок 4: XSS на Web-Server

V_{base} = 6.1 $CVSS_{Medium}$

R_{ctx} = 6.1 *4.0 * 1.0 * 0.8 = 19.5

Висновок: ризик переходить у категорію Medium, наближаючись до High.

Розрахунок 5: BlueKeep на Legacy PC

V_{base} = 9.8 $CVSS_{Critical}$

R_{ctx}= 9.8 * 1.0 * 0.5 * 1.0 = 4.9

Висновок: ключовий результат методики. Критична технічна вразливість (9.8) перетворена на Низький (Low) бізнес-ризик. Витрачати ресурси на термінове оновлення цього ПК недоцільно, поки існують проблеми 1 та 3 вразливості.

Порівняльний аналіз отриманих розрахунків

Для наочної демонстрації ефективності методики зведемо результати стандартного підходу (CVSS) та розробленого контекстного підходу Rc_{ontext} у порівняльну таблицю (Таблиця 3.8).

Таблиця 3.8

Порівняльний аналіз отриманих розрахунків

№	Вразливість	CVSS Base (Стандарт)	Ранг CVSS	Rcontext (Методика)	Ранг Rcontext	Зміна пріоритету
1	Log4Shell	10.0	1	32.0	1	Без змін
3	SQL Injection	8.0	4	25.6	2	Підвищено
2	EternalBlue	9.3	3	20.9	3	Без змін
4	XSS Reflected	6.1	5	19.5	4	Підвищено
5	Blue Keep	9.8	2	4.9	5	Критично знижено

3.4 Аналіз отриманих результатів

На основі розрахунків, проведених у попередніх пунктах роботи, було виконано порівняльний аналіз ефективності стандартного підходу (CVSS Base Score) та розробленої методики контекстного оцінювання Rcontext. Метою аналізу є виявлення розбіжностей у пріоритезації вразливостей та оцінка впливу методики на процес прийняття управлінських рішень.

Головним результатом застосування методики стала черга усунення вразливостей (Remediation Backlog). Порівняння рейтингів небезпеки наведено на порівняльній діаграмі (Рис. 3.3).

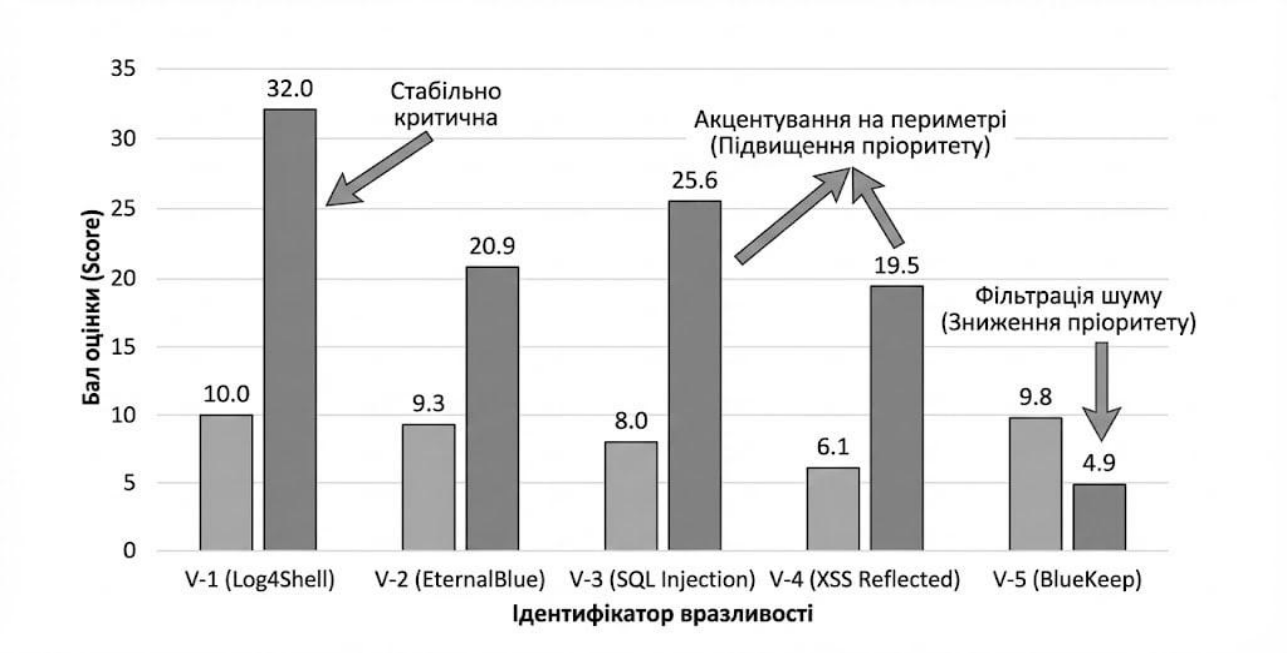

Рисунок 3.3 Діаграма порівняння рейтингів небезпеки вразливостей

Для кількісної оцінки ефективності запропонованого підходу використано метрику “Коефіцієнт релевантності черги”. Виходячи з типових обмежень операційних ресурсів та фіксованої пропускної здатності команди реагування, для моделювання ситуації встановлено ліміт на усунення у розмірі трьох вразливостей за один стандартний звітний період.

Розглянемо два сценарії формування черги задач на основі цього ліміту.

Сценарій А: формування черги за стандартом CVSS Команда реагування відбирає три вразливості з найвищим базовим балом V_{base} (див. табл. 3.8).

1- Log4Shell – $V_{base} = 10.0$;

2 – EternalBlue - $V_{base} = 9.3$;

5 – BlueKeep – $V_{base} = 9.8$.

Результат сценарію А: ресурси команди витрачено на усунення вразливості 5 на застарілому ПК, який не має доступу до критичних даних та Інтернету. При цьому критична вразливість 3 (SQL Injection), $V_{base}=8.0$, що знаходиться на публічному веб-сервері, залишилася невиправленою, оскільки посіла лише 4-те місце у стандартному рейтингу.

Висновок: бізнес-ризик компрометації зовнішнього периметра залишається високим. Ресурси використано неефективно.

Сценарій Б: формування черги за розробленою методикою “топ- 3 $R_{context}$". Команда реагування відбирає три вразливості з найвищим контекстним ризиком $R_{context}$ (див. табл. 3.8).

1. Log4Shell - $R_{context}$ = 32.0 (Публічний веб-сервер);
2. EternalBlue – R contex t= 20.9 (Внутрішня база даних);
3. SQL Injection – $R_{context}$ = 25.6 (Публічний веб-сервер);
4. EternalBlue – $R_{context}$= 20.9 (Внутрішня база даних).

Результат сценарію Б: команда сфокусувала зусилля на закритті векторів атак на зовнішньому периметрі 1 та 3 та захисті критичних внутрішніх даних 2. Вразливість 5 - BlueKeep з низьким контекстним ризиком $R_{context}$ = 4.9 було обґрунтовано відкладено.

Висновок: бізнес-ризик компрометації периметра та витоку данихуспішно мінімізований. Ресурси використано з максимальною віддачею для захисту бізнес-процесів.

Висновки до розділу 3

У третьому розділі було вирішено завдання розробки та практичної апробації методики комплексної оцінки захищеності інформаційних систем.

Основні результати розділу:

1. Розроблено математичну модель контекстного оцінювання ризику, що базується на мультиплікативній згортці чотирьох параметрів: базового балу вразливості, критичності активу, фактору експозиції та коефіцієнта компенсації;
2. Формалізовано алгоритм обробки результатів тестування на проникнення, який дозволяє автоматизувати процес збагачення технічних даних бізнес-контекстом;

3. Проведено експериментальне дослідження на тестовому полігоні, що емулює типову корпоративну інфраструктуру;

4. Доведено ефективність методики: порівняльний аналіз продемонстрував, що застосування розробленого підходу дозволяє виявити та підвищити пріоритет критичних загроз на периметрі мережі на прикладі SQL Injection, які ігноруються стандартним підходом CVSS.

ВИСНОВКИ

Під час написання кваліфікаційну роботи за темою “Розробка методики комплексної оцінки захищеності інформаційних систем за результатами пентесту”, було вирішено поставлене завдання щодо підвищення ефективності оцінювання стану захищеності корпоративних інформаційних систем. Основною метою дослідження була розробка та практична апробація методики комплексної оцінки за результатами тестування на проникнення, яка на відміну від наявних стандартних підходів, зможе дозволити враховувати структуру функціонування активів.

Основні результати, отримані в ході виконання роботи, полягають у наступному: проведено системний аналіз проблематики оцінювання вразливостей. У ході аналітичного огляду встановлено, що домінуючий на сьогодні стандарт оцінки вразливостей CVSS (Common Vulnerability Scoring System), попри свою універсальність для технічної класифікації, має суттєві методологічні обмеження при застосуванні в задачах управління бізнес-ризиками. Доведено, що використання базового балу CVSS ігнорує критичність активу для бізнесу, топологію мережі та наявність компенсуючих засобів захисту, що призводить до спотворення реальної картини загроз та неефективного розподілу ресурсів на захист; розроблено концептуальну модель та методику комплексної оцінки, для усунення виявлених недоліків розроблено методику розрахунку Інтегрального Показника Безпеки (ІПБ), що базується на ризик-орієнтованому підході. Ключовим внеском є запропонована математична модель розрахунку контекстного ризику, що реалізована як мультиплікативна згортка чотирьох параметрів - технічного балу вразливості, коефіцієнта критичності активу, фактору мережевої експозиції та коефіцієнта ефективності наявних засобів захисту. Також було створено алгоритм обробки результатів пентесту. Формалізовано покроковий алгоритм, який забезпечує інтеграцію процесу технічного тестування на проникнення з процесами управління активами (CMDB) та ризиками. Алгоритм дозволяє автоматизувати процедуру

збагачення технічних даних про вразливості бізнес-контекстом, перетворюючи звіт після сканування на пріоритезований план дій для керівництва. Здійснено практичну роботу та було доведено ефективність власної розробленої методики на базі розгорнутого тестового полігону, що емулює типову гетерогенну корпоративну інфраструктуру, та проведено експериментальне дослідження. Проведено порівняльний аналіз результатів оцінювання за стандартом CVSS та за розробленою методикою, що підтвердив підтвердив робочу гіпотезу.

Наукова новизна роботи полягає в удосконаленні методології оцінювання кіберризиків шляхом інтеграції різнорідних даних, результатів технічного аудиту та бізнес-метрик активів в єдину математичну модель контекстного ризику.

Практичне значення одержаних результатів полягає у створенні готового інструментарію, що дозволяє підрозділам інформаційної безпеки оптимізувати процеси управління вразливостями, скоротити час реакції на критичні інциденти та підвищити обґрунтованість інвестицій у засоби захисту інформації.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. NIST SP 800-30 Rev.1. Guide for Conducting Risk Assessments. *National Institute of Standards and Technology*. (2012). URL: https://csrc.nist.gov/pubs/sp/800/30/r1/final.

2. ISO/IEC 27000:2018. Information technology – Security techniques – Information security management systems – Overview and vocabulary. International Organization for Standardization. (2010). URL:https://cdn.standards.iteh.ai/samples/73906/276f4738dd1d4b2a8763522181030053/ISO-IEC-27000-2018.pdf.

3. Schneier, B. Secrets and Lies: Digital Security in a Networked World. Wiley Publishing. (2000).

4. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection – Guidance on managing information security risks. *International Organization for Standardization.* (2022). URL:https://cdn.standards.iteh.ai/samples/80585/7bca93ac16fd426a9bc717cadc9284d9/ISO-IEC-27005-2022.pdf.

5. Eccleston, L., & Schlueter, D. The Definitive Guide to Penetration Testing. Apress. (2017).

6. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection – Information security controls. *International Organization for Standardization*. (2022). URL: https://pecb.com/en/whitepaper/isoiec-270022022-information-security-cybersecurity-and-privacy-protection.

7.Клочко В. П., Приставка, П. О., Попов, В. О. Кібербезпека: Підручник. Київ: НУОУ імені Івана Черняховського. (2021). (дата звернення: 21.10.2025).

8. Коженевський С. Р., Пасічник, М. В., Хома, М. Р. Кібербезпека: навчальний посібник. Львів: НУ "Львівська політехніка". (2023).

9. NIST SP 800-115. Technical Guide to Information Security Testing and Assessment. National Institute of Standards and Technology. (2008). URL: https://csrc.nist.rip/publications/nistbul/Dec2008_Testing-Assessment-SP800 -

115.pdf#:~:text=Issued%20in%20September%202008%2C%20the%20guide%20presents%20the,effective%20methods%20for%20implementing%20testing%20and%20assessment%20practices.

10. The Penetration Testing Execution Standard. *PTES Technical Guidelines*. URL: https://www.google.com/search?q=https://www.pentest-standard.org/.

11. Nazarov, O. V., & Shumeiko, M. M. Організаційно-методичні основи проведення робіт з тестування на проникнення. Харків: ХНУРЕ. (2020).

12. OWASP Web Security Testing Guide | OWASP Foundation. OWASP Foundation, the Open-Source Foundation for Application Security | OWASP Foundation. URL: https://owasp.org/www-project-web-security-testing-guide

13. Herzog P. Open-Source Security Testing Methodology Manual (OSSTMM). Institute for Security and Open Methodologies (ISECOM). URL: https://www.scribd.com/doc/208433247/osstmm-en-2-1.

14. Петренко В. А. Управління кіберризиками на основі аналізу зовнішніх загроз. Науковий вісник. 2022. № 15

15. ДСТУ ISO/IEC 27005:2022. Інформаційні технології. Методи та засоби забезпечення безпеки. Управління ризиками інформаційної безпеки Київ: ДП «УкрНДНЦ», 2023.

16 Методика оцінки ризиків інформаційної безпеки. Настанова НКЦК при РНБО України від 15.02.2022. Київ: НКЦК, 2022.

17. Ковальчук О. С. Системний підхід до оцінки ефективності засобів кіберзахисту. Технічна кібернетика. 2023. Т. 3, № 1. С. 12–19.

18. FIRST. Специфікація системи загальної оцінки вразливостей (CVSS v3.1). / FIRST.org. – 2019. URL: https://www.first.org/cvss/v3.1/specification-document

19. Григорович Р. В. Динамічна оцінка вразливостей з урахуванням темпоральних метрик. Збірник наукових праць. 2022. інституту моделювання. 2022. Вип. 4. С. 88–95.

20. FIRST. Посібник користувача CVSS v3.1: User Guide / FIRST.org. – 2019. URL: https://www.first.org/cvss/v3.1/user-guide

21. *Національний інститут стандартів і технологій США* (NIST). Настанова щодо реагування на інциденти комп'ютерної безпеки (NIST SP 800-61 Rev. 2) .URL: https://doi.org/10.6028/NIST.SP.800-61r2

22. Іванов П. Д. Порівняльний аналіз методик оцінки кіберризиків: CVSS проти OWASP. Матеріали IV Міжнародної науково-практичної конференції.

м. Київ, 18 трав. 2023 р. Київ: ДУІКТ, 2023. С. 112–115.

23. OWASP. Методологія оцінки ризиків OWASP (OWASP Risk Rating Methodology).

URL:https://owasp.org/wwwcommunity/OWASP_Risk_Rating_Methodology

24. Загородній М. О. Проблеми суб'єктивності в оцінці ризиків інформаційної безпеки. Актуальні питання кібербезпеки. 2021. № 1 С. 34–40.

25. Корнієнко В. П. Моделювання загроз та оцінка ризиків за методикою DREAD. Вісник ХНУ. 2020. № 5. С. 78–84.

26. Методологія OCTAVE. Операційно-критична оцінка загроз, активів та вразливостей. Настанова CERT/CC. URL: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=5659

27. Ткаченко В. Р. Застосування OCTAVE для оцінки ризиків критичної інфраструктури. Журнал кібербезпеки. 2023. № 4. С. 56–63.

28. Фреймворк FAIR. Кількісний аналіз інформаційного ризику. Офіційний посібник. 2014. 380 р.

29. Савчук А. П. Фінансове вираження кіберризиків на основі моделі FAIR. Економічна кібернетика. 2022. Т. 2, № 2. С. 22–29.

30. Грищук О. В. Методи агрегування показників при оцінці складних систем. Системний аналіз. 2021. № 3. 101–109.

31. Данилюк Р. С. Питання вибору оптимального методу згортки показників у економічних дослідженнях. Фінансові дослідження. 2020. Вип. 1. С. 45–51.

32. Spring J., Hatleback E. Improving Vulnerability Scoring with Context / J. Spring, E. Hatleback // IEEE Security & Privacy. – 2017. – Vol. 15, No. 6. – P. 46-53. URL: 10.1109/MSP.2017.4251104.

33. FIRST.org. Common Vulnerability Scoring System v3.1: Specification Document. – 2019. URL: https://www.first.org/cvss/v3.1/specification-document.

34. ISO/IEC 27005:2018. Information technology — Security techniques — Information security risk management. – Geneva: ISO, 2018. – 68 p.

35. NIST SP 800-30 Rev. 1. Guide for Conducting Risk Assessments / Joint Task Force Transformation Initiative. – Gaithersburg: National Institute of Standards and Technology, 2012. – 95 p. URL: https://doi.org/10.6028/NIST.SP.800-30r1.

36. Alberts C., Dorofee A. OCTAVE Allegro: Improving the Information Security Risk Assessment Process / C. Alberts, A. Dorofee. – Carnegie Mellon University, Software Engineering Institute, 2007. URL: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419

37. Гнатюк С. О. Кібербезпека: сучасні напрями та технології: навч. посібник / С. О. Гнатюк, В. М. Кізєєв. – Київ: НАУ, 2018. – 248 с.

38. Scarfone K. Technical Guide to Information Security Testing and Assessment (NIST SP 800-115) / K. Scarfone, M. Souppaya. – NIST, 2008.URL: https://doi.org/10.6028/NIST.SP.800-115

39.Shostack A. Threat Modeling: Designing for Security / Adam Shostack. – Wiley, 2014. – 624 p.

40. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. – Київ: ДСТСЗІ СБУ, 1999.

41. Jones J. Measuring and Managing Information Risk: A FAIR Approach / Jack Jones, Jack Freund. – Butterworth-Heinemann, 2014. – 380 p.

42. MITRE Corp. MITRE ATT&CK: Design and Philosophy – 2020.URL:https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

43. Kuipers D. Control Systems Cyber Security: Defense in Depth Strategies / D. Kuipers, M. Fabro. – Idaho National Lab (INL), 2006. URL: https://www.inl.gov.

44. Wheeler E. Security Risk Management: Building an Information Security Risk Management Program from the Ground Up / Evan Wheeler. – Syngress, 2011. – 336 p.

45. SANS Institute. Vulnerability Management Maturity Model. URL: https://www.sans.org/white-papers/