

ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет кораблебудування імені адмірала Макарова
Навчально-науковий інститут автоматики і електротехніки
Кафедра комп'ютерних технологій та інформаційної безпеки

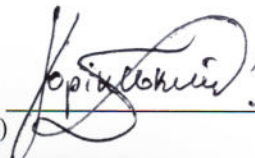
«ДОПУЩЕНИЙ ДО ЗАХИСТУ»
Завідувач кафедри комп'ютерних
технологій та інформаційної
безпеки, к.т.н., доцент
 С.М. Нужний
« 17 » 06 2026р.

КВАЛІФІКАЦІЙНА РОБОТА
на здобуття ступеня вищої освіти «бакалавр»

**РОЗРОБКА ІНФОРМАЦІЙНОЇ МОДЕЛІ ОЦІНКИ ЗАЛЕЖНОСТІ
ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ ВІД ВПЛИВУ ФАКТОРІВ
ВРАЗЛИВОСТЕЙ**

Галузь знань: 12 «Інформаційні технології»
Спеціальність: 125 «Кібербезпека»
Освітньо-професійна програма: «Системи технічного захисту інформації,
автоматизація її обробки»

Виконав: студент 4381 групи
Горінський Дмитро Миколайович
(прізвище та ініціали)

(підпис) 

Керівник роботи: ст. викладач кафедри комп'ютерних технологій та
інформаційної безпеки

Трибулькевич С.Л.
(прізвище та ініціали)

 (підпис)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова

Навчально-науковий інститут автоматики та електротехніки

Кафедра комп'ютерних технологій та інформаційної безпеки

Спеціальність 125«Кібербезпека»

Освітня програма «Системи технічного захисту інформації, автоматизація її обробки»

ЗАТВЕРДЖУЮ

Гарант освітньої програми, к.т.н.,
доцент, доцент кафедри КТІБ

 С.М. Нужний
« 10 » 02 2026р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ на здобуття ступеня вищої освіти «бакалавр»

Студенту Горінському Дмитру Миколайовичу

(Прізвище, ім'я, по батькові)

1. Тема роботи: Розробка інформаційної моделі оцінки залежності захисту комп'ютерних мереж від впливу факторів вразливостей.

Керівник роботи ст. викладач кафедри комп'ютерних технологій та інформаційної безпеки, Трибулькевич Сергій Леонідович

Затверджені наказом ректора д36-42 від 22.04.2026

2. Термін подання роботи: 5.06.2026
3. Вихідні дані по роботі: Математичний апарат на базі теорії ймовірностей. Технічний інструментарій: ізольоване віртуальне середовище на базі Oracle VM VirtualBox; характеристики цільового вузла (Ubuntu Server 26.04 LTS) та атакуючого вузла (Kali Linux); параметри засобів захисту Fail2ban та інструментарію імітації атак Hydra 9.5..
4. Перелік питань, що належать до розробки (найменування розділів):
 1. Аналіз останніх досліджень і публікацій.
 2. Теоретичні основи та методи оцінки захищеності комп'ютерних мереж.
 3. Розробка та верифікація інформаційної моделі оцінки залежності захисту від факторів вразливостей.
 4. Розробка та верифікація інформаційної моделі оцінки залежності захисту від факторів вразливостей.
5. Перелік презентаційних матеріалів:.. слайди в якості результатів дослідження у відповідності до переліку питань, що належать до розробки.

6. Консультант - внутрішній рецензент роботи

Прізвище, ініціали та посада	Дата подання роботи на рецензію	Дата отримання рецензії	Підпис
Передерій В.І., професор, д.т.н.	2.06.26	5.06.26	

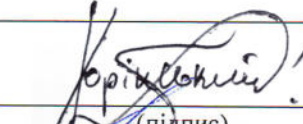
7. Дата видачі завдання 10.02.2026

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання	Примітка
1	Вибір теми, визначення мети, завдань, об'єкта та предмета дослідження	10.02.2026	
2	Попередній варіант оглядових розділів, підбір і опрацювання списку використаних джерел	20.03.2026	
3	Попередній варіант повної КР	15.04.2026	
4	Складання ЄДКІ зі спеціальності на ступінь «бакалавра»	16.04.2026 14.05.2026	
5	Попередній варіант презентації	29.05.2026	
6	Подання на кафедру КТІБ тексту остаточного варіанту роботи, підписаного її керівником в електронному форматі разом із заявами щодо самостійності виконання роботи та ідентичності друкованої та електронної версій роботи (Додатки 1 і 2 «Порядку здійснення заходів з перевірки робіт на наявність текстових збігів/ідентичності/схожості із використанням програмно-технічних засобів», який введений в дію наказом ректора НУК за №20 від 20.01.2020) Отримання внутрішньої рецензії	05.06.2026	не пізніше, ніж за 14 діб до захисту
7	Отримання висновку керівника; Отримання висновку кафедри щодо наявності / відсутності плагіату в роботі Попередній захист роботи на засіданні кафедри КТІБ Висновок кафедри про КР, допуск до захисту	10.06.2026	
8	Отримання зовнішньої рецензії	15.06.2026	
9	Підготовка презентації та доповіді	17.06.2026	
10	Подання на кафедру КТІБ: – друкованого і зшитого варіанту пояснювальної записки до кваліфікаційної роботи та/або (за рішенням кафедри) електронного варіанту в форматі *.pdf – друкованого варіанту презентації (в 5-ти екземплярах в разі захисту оф-лайн, в одному екземплярі в разі захисту он-лайн (за рішенням кафедри)) та електронного варіанту презентації; – зовнішньої рецензії; – документів щодо відсутності плагіату і передачі авторських прав; – файлу-опису кваліфікаційної роботи (згідно Додатку до наказу ректора НУК за №287-уч від 19.05.2020 р.).	22.06.2026	
11	Захист кваліфікаційної роботи	24 - 25.06.2026	

Студент

Керівник роботи


(підпис)


(підпис)

Д.М. Горінський
(ПІБ)С.Л. Трибулькевич
(ПІБ)

АНОТАЦІЯ

Горінський Д.М. Розробка інформаційної моделі оцінки залежності захисту комп'ютерних мереж від впливу факторів вразливостей

Кваліфікаційна робота на здобуття ступеня вищої освіти «бакалавр» за спеціальністю 125 «Кібербезпека та захист інформації» галузі знань 12 «Інформаційні технології». – Національний університет кораблебудування імені адмірала Макарова, Миколаїв, 2026.

Пояснювальна записка: 72 с., 28 рис., 4 таблиці, 43 посилань.

У бакалаврській роботі виконується розробка інформаційної моделі оцінки залежності захисту комп'ютерних мереж від впливу факторів вразливостей.

Кваліфікаційна робота присвячена актуальній темі – забезпечення стійкості комп'ютерних мереж потребує переходу від статичного оцінювання вразливостей до динамічного моделювання ризиків. Реактивні засоби захисту (зокрема Fail2ban) через аналіз логів мають часову латентність (затримку реакції). Під час високошвидкісних Brute-force атак на SSH виникає «вікно вразливості», у межах якого злоумисник здійснює сотні спроб підбору паролів до моменту блокування. Метою роботи є розробка інформаційної моделі оцінки залежності захисту комп'ютерних мереж від впливу факторів вразливостей.

Очікуваним результатом роботи є математичного обґрунтована модель оцінки захищеності з урахуванням динамічного фактора латентності. Функціональний тестовий стенд для моделювання кібератак та оцінки ефективності систем безпеки. Кількісні дані та порівняльний аналіз стійкості систем при реактивному (Fail2ban) та превентивному (Ed25519) підходах. Комплекс практичних рекомендацій для захисту віддаленого доступу.

Ключові слова: кібербезпека, інформаційна модель, фактори вразливості, SSH, Brute-force, Fail2ban, латентність захисту, вікно вразливості, ключі ED25519, превентивна безпека, Zero trust.

ANNOTATION

Horinskyi D.M. Development of an Information Model for Assessing the Dependence of Computer Network Protection on the Influence of Vulnerability Factors

Thesis for the degree of Bachelor of Science in the specialty 125 “Cybersecurity and Information Protection” in the field of knowledge 12 “Information Technologies.”
– Admiral Makarov National University of Shipbuilding, Mykolaiv, 2026.

Explanatory note: 72 p., 28 figures., 4 tables, 43 references.

This bachelor’s thesis develops an information model for assessing the dependence of computer network security on the impact of vulnerability factors.

The thesis addresses a timely topic: ensuring the resilience of computer networks requires a shift from static vulnerability assessment to dynamic risk modeling. Reactive protection measures (in particular, Fail2ban), which rely on log analysis, have a time latency (response delay). During high-speed brute-force attacks on SSH, a “window of vulnerability” arises, within which an attacker makes hundreds of password guessing attempts before being blocked. The aim of this work is to develop an information model for assessing the dependence of computer network security on vulnerability factors.

The expected outcome of this work is a mathematically sound security assessment model that accounts for the dynamic latency factor. A functional test bench for modeling cyberattacks and evaluating the effectiveness of security systems. Quantitative data and a comparative analysis of system resilience under reactive (Fail2ban) and preventive (Ed25519) approaches. A set of practical recommendations for protecting remote access.

Keywords: cybersecurity, information model, vulnerability factors, SSH, Brute-force, Fail2ban, protection latency, vulnerability window, ED25519 keys, preventive security, Zero trust.

ЗМІСТ

АНОТАЦІЯ.....	2
ЗМІСТ	3
Перелік СКОРОЧЕНЬ.....	5
ВСТУП	7
1 Аналіз останніх досліджень і публікацій.....	10
1.1 Законодавча та нормативна база України у сфері кібербезпеки.....	10
1.2 Міжнародні стандарти та регламенти: NIST CSF, ISO/IEC, директиви (NIS2), рекомендації ENISA	12
1.3 Еволюція підходів до оцінки захищеності мереж у міжнародних фахових виданнях	14
1.4 Критичний аналіз щодо моделювання вразливостей та факторів ризику	16
1.5 Аналіз ролі протоколу SSH та стандартних портів як практичного об'єкта дослідження. Обґрунтування наукової проблеми.....	18
2 ТЕОРЕТИЧНІ ОСНОВИ ТА МЕТОДИ ОЦІНКИ ЗАХИЩЕНОСТІ КОМП'ЮТЕРНИХ МЕРЕЖ	20
2.1 Огляд математичних моделей оцінки ризиків і захищеності: теорія ймовірностей, теорія черг, марківські процеси	20
2.2 Теоретичне обґрунтування концепції «вікна вразливості» для реактивних систем захисту	23
2.3 Формалізація задачі: вихідні дані, змінні стану, крайові умови та обмеження моделі	24
2.4 Вибір та обґрунтування метрик ефективності захисту: час до бану, ймовірність компрометації, кількість спроб	26
2.5 Перспективний напрямок дослідження: порівняння реактивного та превентивного підходів. Очікувані результати	27
3 РОЗРОБКА ТА ВЕРИФІКАЦІЯ ІНФОРМАЦІЙНОЇ МОДЕЛІ ОЦІНКИ ЗАЛЕЖНОСТІ ЗАХИСТУ ВІД ФАКТОРІВ ВРАЗЛИВОСТЕЙ.....	29

3.1 Математична модель імовірності компрометації системи при різних сценаріях атак	29
3.2 Архітектура та параметри тестового стенду як дослідної установки .	30
3.3 Базовий сценарій: тестування SSH без засобів захисту та кількісна оцінка параметрів атаки	38
3.4 Реактивний сценарій: тестування ефективності Fail2ban та вимірювання латентності захисту Lf2b	40
3.5 Превентивний сценарій: автентифікація за ключовою парою Ed25519 як контрольний сценарій верифікації	43
3.6 Порівняльний аналіз отриманих результатів та верифікація моделі ..	49
4 РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ МОДЕЛІ ТА РЕКОМЕНДАЦІЇ ЩОДО БЕЗПАРОЛЬНОЇ АРХІТЕКТУРИ В КОРПОРАТИВНОМУ СЕРЕДОВИЩІ ...	54
4.1 Практичне застосування моделі: рекомендації щодо безпарольної архітектури в корпоративному середовищі	54
4.2 Аналіз ризиків і переваг Open Source рішень у світлі отриманих результатів	55
4.3 Організаційно-економічна ефективність запропонованих заходів	55
4.4 Напрямки подальших досліджень: розширення моделі, нові фактори вразливостей, автоматизація оцінки	57
ВИСНОВКИ.....	59
ПЕРЕЛІК ПОСИЛАНЬ	63
ДОДАТОК А.....	68
ДОДАТОК Б	69

ПЕРЕЛІК СКОРОЧЕНЬ

ALE (Annualized Loss Expectancy) – очікувані річні збитки

ASCII (American Standard Code for Information Interchange) – базовий комп'ютерний стандарт кодування

CIA (Confidentiality, Integrity, Availability) – конфіденційність, цілісність та доступність

CLI (Command Line Interface) – інтерфейс командного рядка

CVE (Common Vulnerabilities and Exposures) – Міжнародна система та база даних загальновідомих вразливостей і дефектів безпеки в інформаційних системах

CVSS (Common Vulnerability Scoring System) – відкритий галузевий стандарт для оцінки серйозності вразливостей у програмному забезпеченні

DoS (Denial of Service) – відмова в обслуговуванні

EAL (Evaluation Assurance Level) – рівень гарантії оцінки; шкала від 1 до 7, визначена стандартом ISO/IEC 15408

FAIR (Factor Analysis of Information Risk) – факторний аналіз інформаційних ризиків

FIA (Identification and Authentication) – «Ідентифікація та автентифікація»

FIA_UAU (User authentication) – безпосередньо механізми перевірки автентичності користувачів перед наданням доступу за ISO/IEC 15408

Firewall – міжмережевий екран

FTP (File Transfer Protocol) – протокол передавання файлів

IEC (International Electrotechnical Commission) – міжнародна електротехнічна комісія

IP (Internet Protocol) – протокол міжмережевої взаємодії

IP-адреса – унікальний мережевий адрес пристрою у мережі TCP/IP

ISO (International Organization for Standardization) – Міжнародна організація зі стандартизації

ISO/IEC – спільні міжнародні стандарти, розроблені спільно Міжнародною організацією зі стандартизації та Міжнародною електротехнічною комісією IEC (International Electrotechnical Commission) – локальна обчислювальна мережа

MAC-адреса – унікальний ідентифікатор мережевого інтерфейсу пристрою

MITRE ATT&CK – база тактик і технік кіберзагроз

MTTD (Mean Time To Detect) – середній час виявлення

MTTR (Mean Time To Repair/Respond) – середній час відновлення/реагування

RDP (Remote Desktop Protocol) – протокол віддаленого робочого столу

SIEM (Security Information and Event Management) – управління інформацією та подіями безпеки

SOAR (Security Orchestration, Automation, and Response) – платформа для автоматизації процесів моніторингу та швидкого реагування на кіберінциденти

SOC (Security Operations Center) – центр управління безпекою

SSH (Secure Shell) – захищене з'єднання

TOE (Target of Evaluation) – об'єкт оцінювання

Zero day – вразливості нульового дня

Zero Trust – архітектура «нульової довіри»

ІБ – інформаційна безпека

ІТ – інформаційні технології

КСЗІ – комплексні системи захисту інформації

НД ТЗІ – нормативний документ з технічного захисту інформації

НСД – несанкціонований доступ

ОС – операційна система

ПБ – політика безпеки

ПЗ – програмне забезпечення

СМО – системи масового обслуговування

СУІБ – системи управління інформаційною безпекою

ВСТУП

Розвиток сучасних інформаційних технологій супроводжується стрімким збільшенням кількості та складності комп'ютерних мереж, які визначають функціонування державних органів, підприємств, організацій критичної інфраструктури та збройних сил. Водночас, зростання рівня цифровізації в суспільстві загострює проблему кіберзагроз та несанкціонованого доступу до інформаційних ресурсів. У 2023 році кількість виявлених кіберзагроз зросла на 40% порівняно з попереднім роком, і ця тенденція прогнозується на наступні роки [1]. У 2024 році кількість кіберінцидентів в Україні зросла майже на 70% порівняно з попереднім роком, досягнувши 4315 випадків, при цьому характер зловмисників змінився з деструктивних атак на шпигунські операції та розвідку [2,3]. Це питання найбільш гостро стоїть під час бойових дій. У 2023 році Системою виявлення та реагування на вразливості при кіберінцидентах та кібератак було опрацьовано приблизно 18 мільярдів подій, виявлено 133 мільйони підозрілих подій інформаційної безпеки та опрацьовано 148 тисяч критичних подій [4]. Ключовим чинником успішності кібератак є використання вразливостей програмного та апаратного забезпечення мереж. Аналіз показує, що зловмисники постійно використовують відомі вразливості програмного забезпечення, деяким з яких понад 10 років, а організації, що продовжують спиратися на стару інфраструктуру з відомими вразливостями, надають зловмисникам основні точки входу до мережі [5]. Станом на 2024 рік у базі даних CVE (Common Vulnerabilities and Exposures) налічується понад 237 725 задокументованих вразливостей різного роду [6]. Для систематизованої оцінки вразливостей міжнародним співтовариством розроблено спеціалізовані стандарти та методики. Загальна система оцінки вразливостей (CVSS) визначає базові, темпоральні метрики та метрики середовища [7]. Стандарти серії ISO/IEC 27001 та NIST SP 800-53 встановлюють вимоги до систем управління безпекою. Окреме місце серед міжнародних стандартів посідає ISO/IEC 15408 («Common Criteria») – трирівнева система оцінки захищеності інформаційних технологій, що визначає функціональні вимоги безпеки (зокрема клас FIA щодо

автентифікації) та рівні гарантій EAL 1–7. Саме цей стандарт формує критеріальну основу для формалізованої оцінки відповідності механізмів захисту встановленим вимогам [29].

Незважаючи на наявність зазначених стандартів, практика засвідчує суттєву прогалину між загальними методиками оцінювання вразливостей та конкретними механізмами визначення залежності між факторами вразливостей і реальним рівнем захисту мережі. Методика оцінки рівня захищеності мережі, що містить у собі систему CVSS, дає змогу користуватися актуальними коефіцієнтами для розрахунку вразливостей та мати перелік основних вразливостей, пов'язаних із сучасними програмними продуктами, що використовуються в автоматизованих системах [8]. Однак побудова формалізованої інформаційної моделі, яка б відображала залежність рівня захисту мережі від комплексного впливу різних факторів вразливостей, залишається актуальним науково-практичним завданням [10, 17]. Актуальність теми дипломної роботи зумовлена необхідністю розробки інструментарію для кількісного оцінювання впливу факторів вразливостей на стан захищеності комп'ютерних мереж з метою своєчасного виявлення критичних залежностей та прийняття обґрунтованих рішень щодо підвищення рівня кібербезпеки. Метою даного дослідження є розробка інформаційної моделі оцінки залежності захисту комп'ютерних мереж від впливу факторів вразливостей та рівня захищеності. Для досягнення поставленої мети необхідно вирішити такі задачі:

- провести аналіз нормативної бази та існуючих підходів до оцінки вразливостей;
- визначити та систематизувати фактори вразливостей комп'ютерних мереж;
- розробити математичну модель залежності захисту від цих факторів;
- верифікувати модель на тестовому стенді та порівняти з відомими результатами;

– сформулювати практичні рекомендації щодо застосування моделі.

Об'єктом дослідження є процес забезпечення захисту комп'ютерних мереж від кіберзагроз. Предметом дослідження є залежність рівня захищеності комп'ютерних мереж від впливу факторів вразливостей. У роботі використовуються: методи системного аналізу та синтезу – для дослідження структури вразливостей та їх впливу на захист мережі; методи математичного моделювання – для формалізації залежностей між факторами; теорія ризиків – для оцінки критичності вразливостей; порівняльний аналіз стандартів кібербезпеки; метод експертних оцінок – для верифікації отриманих результатів. Наукова новизна одержаних результатів полягає у розробці інформаційної моделі, яка на відміну від існуючих підходів: забезпечує комплексне врахування взаємного впливу різнорідних факторів вразливостей у їх сукупності; формалізує залежності між параметрами вразливостей і рівнем захищеності мережі у вигляді структурованої інформаційної моделі; дозволяє динамічно оновлювати оцінки при зміні конфігурації мережі або появі нових вразливостей, дозволяє оцінювати відповідність конфігурації захисту вимогам функціональних класів стандарту ISO/IEC 15408-2 (зокрема FIA_UAU щодо стійкості механізму автентифікації) та динамічно оновлювати оцінки при зміні конфігурації мережі або появі нових вразливостей. Практичне значення отриманих результатів: розроблена модель може застосовуватися при проведенні аудиту інформаційної безпеки комп'ютерних мереж, у системах управління інформаційною безпекою (ISMS) організацій, а також у навчальному процесі при підготовці фахівців у галузі кібербезпеки та захисту інформації. Робота складається зі вступу, чотирьох розділів, висновків та переліку посилань. У першому розділі проведено аналіз нормативної бази та критичний огляд існуючих методів захисту. Другий розділ присвячено теоретичним основам та вибору математичного апарату. У третьому розділі розроблено та верифіковано інформаційну модель. Четвертий розділ містить результати дослідження та рекомендації щодо практичного застосування.

1 АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

1.1 Законодавча та нормативна база України у сфері кібербезпеки

Формування цілісної системи кіберзахисту в Україні регулюється ієрархічною структурою нормативно-правових актів, що включає закони України, постанови Кабінету Міністрів та нормативні документи з технічного захисту інформації (НД ТЗІ).

Правовий фундамент кіберзахисту в Україні базується на системі законів, які пройшли значну модернізацію у 2024-2025 роках для адаптації в умовах воєнного стану та євроінтеграційних вимог. Основним документом є закон України «Про основні засади забезпечення кібербезпеки України» (зі змінами від 27.03.2025 згідно із Законом № 4336-IX) [19]. Цей закон визначає об'єкти кіберзахисту, до яких належать інформаційно-комунікаційні системи (ІКС) усіх форм власності, де обробляються національні інформаційні ресурси. Оновлена редакція закону 2025 року впроваджує критично важливі терміни [19]:

- «Кризова ситуація у сфері кібербезпеки» – порушення режиму функціонування ІКС, що може мати значні негативні наслідки для національної безпеки;
- «Реагування на кіберінциденти» — структурований процес виявлення, аналізу та мінімізації шкоди від атак;
- «Активна протидія агресії у кіберпросторі» – дії, спрямовані на нейтралізацію систем і мереж держави-агресора, що використовуються для завдання шкоди Україні.

Також паралельно діє Закон України «Про захист інформації в інформаційно-комунікаційних системах»[20], який станом на березень 2025 року зазнав суттєвої реформи. Головною новацією став перехід від виключно жорсткої сертифікації до поняття «авторизації з безпеки». Це рішення щодо можливості експлуатації системи на основі її відповідності національним стандартам та

профілям безпеки. Закон чітко покладає відповідальність за захист інформації на власника або розпорядника системи.

Особлива увага в аналізі нормативної бази приділяється об'єктам критичної інфраструктури, оскільки саме для них встановлено гранично суворі вимоги до фільтрації портів та стійкості автентифікації. Це дозволяє використовувати ці нормативи як базові параметри для розроблюваної інформаційної моделі оцінки мереж [2].

Постанова КМУ № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» (з оновленнями 2022-2025 рр.). Вона встановлює обов'язкові технічні заходи для захисту ІКС [2, 10]:

- Сегментація мережі: обов'язковий розподіл на фізичному або логічному рівні з використанням міжмережевих екранів;
- Захист від атак «нульового дня»: виявлення та блокування зловмисного коду, для якого ще немає сигнатур;
- Фільтрація трафіку: обмеження доступу за критеріями дозволених портів, протоколів та сервісів;
- Заборона вразливих технологій: на об'єктах критичної інформаційної інфраструктури (ОКІІ) заборонено використання Wi-Fi та Bluetooth для передачі критичних даних.

Практична реалізація КСЗІ базується на стандартах серії 2.5, які класифікують вимоги залежно від типу системи:

1. НД ТЗІ 2.5-004-99 [35] визначає критерії оцінки захищеності інформації та рівні гарантій (Г-1 – Г-7).

2. НД ТЗІ 2.5-008-2002 [36] встановлює вимоги для автоматизованих систем класу 2, вимагаючи реалізації послуг автентифікації (НИ-2), реєстрації подій (НР-2) та цілісності КЗЗ (НЦ-2). Загальні підходи до оцінювання ризиків за цими стандартами також розглядаються у фахових дослідженнях [9].

Згідно з аналітичним звітом за 2025 рік, рівень виконання Стратегії кібербезпеки України сягнув 86% [24]. Держава перейшла до ризик-орієнтованого підходу, що передбачає адаптацію політик до реальних загроз воєнного часу та

гармонізацію із директивою ЄС NIS2. Важливим аспектом є впровадження NIST CSF 2.0 як орієнтира для національної системи кіберготовності [10, 24].

1.2 Міжнародні стандарти та регламенти: NIST CSF, ISO/IEC, директиви (NIS2), рекомендації ENISA

Міжнародна стандартизація є фундаментом для побудови надійних систем захисту, забезпечуючи уніфікацію термінології, методів оцінки та заходів контролю. Для України впровадження міжнародних практик є стратегічним пріоритетом, закріпленим у планах реалізації Стратегії кібербезпеки [25]. В умовах сучасних кіберзагроз, використання уніфікованих стандартів дозволяє не лише гармонізувати українське законодавство з європейським, а й отримати верифіковані метрики для побудови імовірнісних моделей захисту [26].

Основним інструментом для побудови СУІБ є серія стандартів ISO/IEC 27000. Зокрема ISO/IEC 27001 (ДСТУ ISO/IEC 27001:2015) [37] визначає вимоги до створення, впровадження та постійного вдосконалення СУІБ, використовуючи ризик-орієнтований підхід. У контексті дослідження критично важливим є розділ 6.1.2, який регламентує процес оцінювання ризиків та визначення рівнів ризику на основі конфіденційності, цілісності та доступності [26]. Більш детальні технічні орієнтири надає ISO/IEC 27002:2022 [38], який класифікує заходи контролю за атрибутами (превентивні, детективні, корегувальні). Для дослідження ключовими є:

- Захід 8.5 (Secure Authentication): вимагає впровадження стійких методів автентифікації, що безпосередньо обґрунтовує вибір між паролем та ключовим методами;
- Захід 8.8 (Management of Technical Vulnerabilities): встановлює необхідність оперативного отримання інформації про вразливості та оцінки ризиків їх експлуатації;

– Заходи 5.25 та 5.26: регламентують оцінку подій безпеки та реагування на інциденти, що є нормативним підґрунтям для дослідження латентності систем захисту

Міжнародний стандарт ISO/IEC 15408 є ключовим для дослідження, оскільки він запроваджує поняття "Об'єкт оцінювання" (TOE – Target of Evaluation) та ієрархію рівнів довіри/гарантій (від Г-1 до Г-7 або EAL1–EAL7) [29].

Інформаційна модель фактично є формалізованим описом «функцій захисту», стійкість яких (Strength of Function) оцінюється через імовірність їхнього подолання зловмисником. Стандарт вимагає, щоб для імовірнісних механізмів (таких як паролі) проводився аналіз ентропії E_{str} , що повністю збігається із математичним апаратом роботи [8, 29].

Оновлена модель NIST CSF 2.0 пропонує п'ять основних функцій (Identify, Protect, Detect, Respond, Recover), які формують замкнений цикл кіберзахисту. У межах кваліфікаційної роботи:

- Функція Detect (Виявлення) корелює з моніторингом спроб brute-force атаки.
- Функція Respond (Реагування) визначає ефективність дій системи (наприклад, блокування через Fail2ban).

Особливе значення має стандарт NIST SP 800-207, який описує архітектуру «нульової довіри» (Zero Trust). Вона базується на принципі «нікому не довіряй за замовчуванням», що вимагає безперервної верифікації кожного запиту до SSH-порту [23].

У 2025 році критичним стає виконання вимог Регламенту DORA (Digital Operational Resilience Act). Він впроваджує термін «операційна стійкість» і вимагає від організацій доведення здатності відновлюватися після атак. П'ять «стовпів» DORA включають управління ризиками ІКТ та регулярне тестування стійкості. Модель в дослідженні дозволяє виконати вимогу DORA щодо «сценарного аналізу», оцінюючи ризик компрометації при різних рівнях інтенсивності атак λ [10].

Директива NIS2 та рекомендації ENISA доповнюють цей перелік вимогами до транскордонної координації та створення мереж CSIRT. Вони акцентують увагу на «швидкості нульової секунди» – необхідності автоматизованого реагування на III-загрози, що робить аналіз затримок реактивного захисту надзвичайно актуальним [3, 33].

Регламент GDPR вимагає впровадження принципу «Privacy by Design», що передбачає використання таких технологій, як шифрування (AES, RSA) та багатфакторна автентифікація для захисту персональних даних. Модель підтримує ці вимоги, обґрунтовуючи перехід до безпарольних архітектур як метод мінімізації ризиків витоку даних [26].

Аналіз міжнародних регламентів (ISO 27002, DORA, NIST CSF) підтверджує, що сучасний захист мереж перейшов від пасивного спостереження до проактивної стійкості. Це легітимізує розробку динамічної інформаційної моделі, де рівень захисту залежить не лише від наявності засобу, а й від його здатності нейтралізувати атаку протягом критично малого «вікна вразливості» [26, 28].

1.3 Еволюція підходів до оцінки захищеності мереж у міжнародних фахових виданнях

Аналіз наукових публікацій та звітів провідних аналістичних центрів дозволяє простежити трансформацію методів оцінки захищеності комп'ютерних мереж від статичних перевірок до динамічних адаптивних систем, що здатні самостійно еволюціонувати в умовах кіберпростору 2026 року [26].

Історично оцінка захищеності базувалася на методології функціональних профілів, закріплених у стандартах серії ISO/IEC 15408 та національних НД ТЗІ 2.5-004-99 і 2.5-005-99. Основним підходом на цьому етапі був статичний аналіз: відповідність системи заданому рівню гарантій (Г-1 – Г-7) та наявність обов'язкових послуг безпеки. Проте дослідження показали, що формальне виконання вимог не враховує динаміку виникнення нових вразливостей, кількість яких у 2026 році демонструє стрімке зростання. Зі зростанням складності мережевих

архітектур фокус досліджень змістився до імовірнісних методів оцінки. Були впроваджені методології FAIR (Factor Analysis of Information Risk) та ALE (Annualized Loss Expectancy), які дозволили перетворити технічні вразливості у кількісні показники ймовірних збитків. Централізація моніторингу в центрах SOC (Security Operations Center) з використанням систем SIEM та SOAR дозволила автоматизувати життєвий цикл інциденту. Ключовими метриками ефективності стали середній час виявлення (MTTD) та середній час реагування (MTTR) [8, 26].

Сучасні дослідження проголошують повну відмову від концепції «захищеного периметра» на користь Zero Trust Architecture. Принципи Zero Trust – «нікому не довіряй, перевіряй завжди», які вимагають безперервної верифікації кожного SSH-запиту на основі контексту та поведінкових факторів [26]. У міжнародних виданнях наголошується, що захищеність мережі тепер залежить не від «підрахунку вразливостей», а від доведення ризику (Proving Risk) в умовах реальної експлуатації [28].

Найновішим трендом 2026 року є перехід до Agentic Security (Агентної безпеки), де автономні ШІ-агенти (наприклад, від Microsoft, Google та CrowdStrike) виконують до 80% рутинної роботи з моніторингу та самовідновлення систем [27]. Це зумовлено появою Adversarial AI (змагального ШІ), здатного проводити атаки на «швидкості нульової секунди»

В Україні еволюція підходів відбувається синхронно зі світовими трендами. Згідно зі звітами CERT-UA за 2025 рік, інтенсивність атак зросла, причому критичним фактором залишається компрометація облікових даних [18]. Реалізація Стратегії кібербезпеки України наприкінці 2025 року сягнула 86%, що підтверджує успішний перехід до активної протидії та ризик-орієнтованого моделювання на об'єктах критичної інфраструктури [24].

Огляд попередніх досліджень свідчить, що сучасна оцінка захищеності мереж має бути динамічною та імовірнісною. Перехід від сигнатурних методів до поведінкового аналізу та ШІ-агентів обґрунтовує необхідність розробки

інформаційної моделі, яка б кількісно оцінювала вразливість SSH-протоколу через призму часу реакції системи та ентропії факторів автентифікації [26, 27].

1.4 Критичний аналіз щодо моделювання вразливостей та факторів ризику

Сучасний етап розвитку засобів мережевого захисту виявляє обмеження традиційних підходів до управління вразливостями [15]. Багаторічним фундаментом аналізу загроз була Національна база вразливостей (NVD) від NIST, проте станом на 2026 рік вона зіткнулася з критичним перевантаженням: беклог некла-сифікованих записів перевищив 27000 CVE, що фактично паралізувало оперативне оновлення інформації про нові загрози [12, 15]. Це унеможливило використання простого кількісного «підрахунку вразливостей» як адекватного критерію захищеності системи [28]. У зв'язку з цим, наукова спільнота та провідні аналітичні центри проголошують перехід до парадигми «доведення ризику» (Proving Risk) [28]. Замість статичного аналізу всіх наявних CVE, акцент зміщується на пріоритезацію на основі експлуатації (Exploitation-weighted prioritization), головним фактором стає імовірність реального використання вразливості зловмисниками в конкретній мережевій архітектурі [26, 28]. Для кількісної оцінки ризиків частіше застосовуються складні математичні моделі, такі як FAIR (Factor Analysis of Information Risk) та Bayesian Analysis, які дозволяють трансформувати технічні параметри вразливостей у імовірнісні показники потенційних збитків [26]. Аналіз факторів ризику для таких протоколів, як SSH, вимагає використання методологій моделювання загроз, зокрема STRIDE та PASTA [26]. Ці підходи дозволяють виявити вразливості не лише в коді, а й у логіці автентифікації та конфігурації портів, що є критичним для дослідження [11, 26]. Важливим фактором ризику, згідно з міжнародними стандартами, є латентність реагування, оскільки затримка між виявленням аномалії та її блокуванням створює «вікно вразливості», достатнє для успішної brute-force атаки [26, 37].

Сканери вразливостей (Nessus, OpenVAS, Qualys) є поширеними інструментами. Вони виявляють відомі вразливості CVE шляхом зіставлення

конфігурації системи з базами знань NVD/Mitre [11, 12]. Основним недоліком є те, що результат сканування береться як «знімок» стану системи на момент сканування [8]. Сканер може відзначити наявність патча чи ні, чи відкритий порт, версію служби тощо, але він не може оцінити ймовірність успішного використання атаки, враховуючи довільну інтенсивність атаки зломисника та час реакції захисної системи; для ілюстрації, Nessus може показати, що SSH-сервер вразливий, але не говорить, наскільки ймовірно, що його буде успішно використано протягом наступних 60 секунд під час атаки з інтенсивністю 300 спроб/сек [26].

Система оцінювання вразливостей Common Vulnerability Scoring System (CVSS) надає числову оцінку критичності від 0 до 10 на основі базових, часових та екологічних метрик. Базова метрика включає вектор атаки, складність, привілеї та вплив на тріаду CIA [7]. Часова метрика частково враховує динаміку – доступність виправлень та рівень перевірки. CVSS має системне обмеження: вона оцінює вразливості як окремі сутності, не враховуючи взаємодію між параметрами захисту [7, 28].

Найбільш дестабілізуючим фактором у 2026 році визнано Adversarial AI (змагальний ШІ). Зломисники використовують ШІ-агенти для автоматизованого пошуку дір у захисті та генерації експлойтів на швидкості «нульової секунди», що робить людський фактор у моніторингу занадто повільним [27]. Відповіддю на це стає впровадження Agentic Security – автономних систем захисту, які здатні самостійно моделювати вектори атак та адаптувати конфігурації мережі у реальному часі для мінімізації ризику компрометації [26, 27].

Для об'єктів критичної інфраструктури та корпоративних мереж в Україні нормативні вимоги (зокрема Постанова КМУ № 518) зобов'язують враховувати ці фактори через впровадження багатофакторної автентифікації та обов'язкову реєстрацію всіх подій безпеки [2, 10]. Це підтверджує наукову обґрунтованість інформаційної моделі, яка базується на залежності захисту від ентропії автентифікаційних даних та часових затримок реактивних засобів, таких як Fail2ban [2, 10, 26].

1.5 Аналіз ролі протоколу SSH та стандартних портів як практичного об'єкта дослідження. Обґрунтування наукової проблеми

Протокол SSH у 2026 році залишається де-факто стандартом для захищеного дистанційного управління серверами у корпоративних та хмарних середовищах [26]. Проте, попри вбудоване шифрування, SSH є одним з найбільш атакованих сервісів через використання стандартного порту TCP/22 [26]. Згідно з методологією MITRE ATT&CK, експлуатація SSH-доступу є ключовою технікою для отримання початкового доступу та подальшого горизонтального переміщення зломисників всередині мережі [39].

Техніка T1110 (Brute Force) за класифікацією MITRE ATT&CK, є одним з найпростіших і найрозповсюдженіших методів отримання доступу (Initial Access) [37]. На відміну від складних Zero day вразливостей, атака перебором не потребує спеціальних знань чи навичок і повністю автоматизована такими інструментами як Hydra, Medusa або Ncrack. Статистика CERT-UA за 2024 рік підтверджує, що компрометація облікових даних залишається основним початковим вектором атак на українські організації [18].

Наукова проблема полягає в тому, що традиційні реактивні засоби захисту, зокрема Fail2ban, є де факто широко використовуваним стандартом для захисту SSH, але їхня ефективність ніколи не була формально кількісно оцінена в функції від параметрів атаки. Адміністратори налаштовують `maxretry=3`, `findtime=600`, `bantime=3600` на основі евристики та досвіду, не маючи математичного обґрунтування того, чи є ці параметри достатніми для конкретної комбінації ентропії пароля та очікуваної інтенсивності атаки.

Обґрунтування вибору SSH як об'єкта дослідження визначається такими чинниками: масовість використання (кожен Linux-сервер у корпоративній мережі), простота відтворення атаки на тестовому стенді (відсутність потреби у спеціальному обладнанні), наявність детальних лог-файлів (`/var/log/auth.log`) для точного вимірювання часових параметрів, а також наявність відкритих інструментів для обох сторін (OpenSSH з боку захисту, Hydra з боку атаки).

Таким чином, SSH-протокол на стандартному порті 22 є оптимальним полігоном для верифікації інформаційної моделі: він поєднує реальну практичну значущість з можливістю точного кількісного вимірювання всіх параметрів моделі в контрольованому середовищі тестового стенду.

2 ТЕОРЕТИЧНІ ОСНОВИ ТА МЕТОДИ ОЦІНКИ ЗАХИЩЕНОСТІ КОМП'ЮТЕРНИХ МЕРЕЖ

2.1 Огляд математичних моделей оцінки ризиків і захищеності: теорія ймовірностей, теорія черг, марківські процеси

Математичне моделювання є фундаментальним інструментом кількісної оцінки захищеності комп'ютерних мереж. На відміну від якісної методики CVSS, математичні моделі дозволяють встановити детерміновані та ймовірнісні залежності між параметрами атаки і параметрами захисту, отримуючи числовий прогноз рівня ризику.

Теорія ймовірностей є базовим апаратом для опису невизначеності в кібербезпеці. Для моделювання атак перебором (Brute Force) необхідно спочатку визначити розмір ключового простору. Ключовий простір це – множина всіх можливих паролів довжиною n із алфавіту потужністю A [43]. Його розмір визначається комбінаторною формулою (2.1). Проте, на практиці атаки Brute Force часто реалізуються як атаки за словником. Тому, у випадку використання словника, потужність ключового простору $|K|$ дорівнює не A^n , а кількості записів у словнику D .

$$|K| = A^n \quad (2.1)$$

де n – довжина пароля (кількість символів);

A – потужність використаного алфавіту.

Ентропія пароля розраховується за формулою (2.2), що є окремим випадком ентропії Шеннона для рівноймовірного розподілу символів [42]:

$$E_{str} = \log_2(|K|) = n \cdot \log_2(A) \quad (2.2)$$

де n – довжина пароля;

A – потужність використаного алфавіту;

Для різних класів паролів: лише малі літери – $A = 26$, буквено-цифровий алфавіт – $A = 62$, повний ASCII-алфавіт – $A = 95$. Для ключової пари Ed25519 ентропія приватного ключа становить $E_{str} = 256$ біт [31], що дає $|K| = 2^{256} \approx 1.16 \cdot 10^{77}$

Ймовірність успіху однієї спроби автентифікації при рівномірному розподілі по ключовому простору обчислюється за формулою (2.3):

$$p = \frac{1}{|K|} = \frac{1}{2^{E_{str}}} \quad (2.3)$$

де $|K|$ – потужність ключового простору.

Ймовірність хоча б одного успіху за N незалежних спроб, коли ймовірність успіху визначається виразом (2.4) описується формулою Бернуллі [34]:

$$p(\text{злам} | N) = 1 - \left(1 - \frac{1}{|K|}\right)^N \approx 1 - e^{-\frac{N}{|K|}} \quad (2.4)$$

Наближення через показникову функцію справедливе при $|K| \gg 1$ та $N \ll |K|$. Саме формула (2.4) є основою для оцінки ймовірності компрометації в даній роботі. У повній моделі в розділі 3 кількість спроб N замінюється на N_{window} – кількість спроб у вікні вразливості Fail2ban.

Теорія черг (СМО – системи масового обслуговування) застосовується для аналізу мережевого трафіку і навантаження на захисні механізми [40]. Потік спроб автентифікації від зловмисника моделюється як пуасонівський потік λ (спроб/сек). Сервер Ubuntu є одноканальною СМО з інтенсивністю обслуговування μ . При умові $\lambda > \mu$ система входить у стан перевантаження, що є окремим вектором атаки DoS.

Для дослідження важливою є не сама черга, а число спроб (2.5), що надходять за проміжок часу t .

$$N(t) = \lambda \cdot t \quad (2.5)$$

де t – вікно вразливості L_{f2b} до спрацювання Fail2ban.

Марківські процеси з дискретним простором станів надають формальний апарат для опису динаміки зміни стану захищеності системи. У Марківській моделі система в кожний момент часу знаходиться в одному з кінцевої множини станів $S = \{S0, S1, S2, S3\}$:

- $S0$ – захищений стан системи: Fail2ban активний, атака на IP-адресу відсутня;
- $S1$ – стан вікна вразливості: атаку розпочато, але захисний механізм Fail2ban ще не спрацював;
- $S2$ – стан блокування: IP-адресу зловмисника заблоковано, атаку призупинена;
- $S3$ – стан компрометації: пароль успішно підібрано зловмисником під час перебування системи у стані $S1$.

Матриця переходів P описує ймовірності переходів між станами за одиницю часу. Стан $S3$ є поглинаючим – вихід з нього неможливий без ручного втручання (зміна пароля, відновлення системи). Час перебування в стані $S1$ є критичним параметром – саме він відповідає поняттю «вікна вразливості», що є центральним об'єктом дослідження даної роботи.

Порівняно з Марківськими моделями, запропонована в роботі модель є більш практично орієнтованою: вона зосереджується на кількісному вимірюванні тривалості стану $S1$ (L_{f2b}) та числа спроб (2.6) що відбуваються в цьому стані. Такий підхід дозволяє безпосередньо пов'язати архітектурні параметри конфігурації (тип автентифікації, латентність Fail2ban) з ймовірністю компрометації.

$$N_{window} = \lambda \cdot L_{f2b} \quad (2.6)$$

де λ – інтенсивність атаки (спроб/с);

L_{f2b} – «вікно вразливості» Fail2ban.

2.2 Теоретичне обґрунтування концепції «вікна вразливості» для реактивних систем захисту

Будь-яка система захисту, що базується на аналізі подій після їх виникнення, є реактивною за своєю природою. Fail2ban – типовий представник такого класу систем. Алгоритм його роботи принципово включає затримку між подією (спробою автентифікації) та реакцією на неї (блокуванням IP-адреси в *iptables*) [30]. Латентність Fail2ban «вікно вразливості» обчислюється за формулою (2.7):

$$L_{f2b} = t_{ban} - t_0 \quad (2.7)$$

де t_{ban} – час коли Fail2ban реально заблокував IP-адресу,

t_0 – перша спроба невдалого входу

Розглянемо часову діаграму атаки. Нехай t_0 – момент початку атаки (перша невдала спроба входу). Fail2ban зчитує файл */var/log/auth.log* з певним інтервалом опитування δ (за замовчуванням близько 1 секунди) [30]. Після виявлення $maxretry = 3$ невдалих спроб протягом $findtime = 600$ секунд, Fail2ban викликає команду *iptables -A INPUT -s <IP> -j DROP*. Час між t_0 та моментом реального блокування і є латентністю захисту.

Протягом цього інтервалу $[t_0, t_{ban}]$ атакуючий продовжує здійснювати спроби автентифікацію зі швидкістю λ (спроб/с). Кількість запитів, що встигають пройти через систему до моменту її повного блокування, за формулою (2.6). Збільшення інтенсивності атаки λ лінійно збільшує N_{window} , тоді як L_{f2b}

залишається відносно фіксованим – він визначається апаратними характеристиками сервера та налаштування Fail2ban.

Для превентивних систем (SSH-ключова пара) поняття «вікна вразливості» втрачає сенс: атака перебором приватного ключа є обчислювально нездійсненою за сучасних технічних можливостей. Розрив з'єднання відбувається на рівні протоколу SSH ще до будь-якого аналізу логів. Це є принциповою архітектурною відмінністю між реактивним і превентивним підходами.

2.3 Формалізація задачі: вихідні дані, змінні стану, крайові умови та обмеження моделі

Для побудови формальної моделі необхідно чітко визначити вхідні параметри, змінні стану та область допустимих значень.

Вектор стану системи S (2.8) – повний набір параметрів конфігурації, що однозначно визначає ймовірність компрометації:

$$S = \langle V_{port}, V_{auth}, L_{f2b}, E_{str}, \lambda \rangle \quad (2.8)$$

де V_{port} – ознака стандартного порту;

V_{auth} – тип автентифікації;

L_{f2b} – латентність Fail2ban;

E_{str} – ентропія пароля.

λ – інтенсивність атаки.

Фізичний зміст кожного параметра, одиниці вимірювання та допустимі діапазони значень наведені в таблиці 2.1. Параметри протоколу SSH визначені відповідно до специфікації [22, 23]. Діапазон інтенсивності атаки λ відповідає реальним можливостям інструменту Hydra [41].

Таблиця 2.1 – Параметри вектору стану системи SSH

Параметр	Фізичний вміст	Одиниці	Діапазон
V_{port}	Ознака стандартного порту SSH	Бінарна	0 – нестандартний, 1 – порт 22
V_{auth}	Тип автентифікації	Бінарна	2^{256} – ключова пара, 1 – пароль
L_{f2b}	Латентність Fail2ban	Секунди	0.5 – 10 с (вимірюється)
E_{str}	Ентропія пароля	Біти	0 – 256 біт
λ	Інтенсивність атаки	Спроб/с	1 – 500 (Hydra, 1 – 200 потоків)

Зв'язок між параметрами E_{str} та $|K|$ встановлено формулами (2.1)-(2.2). Для зручності наведемо числові значення для характерних класів паролів та ключів у таблиці 2.2.

Таблиця 2.2 – Числові значення для характерних класів паролів

Конфігурація	N	A	E_{str} , біт	$ K $
Пароль <i>123</i>	3	10	9.97	1000
Пароль <i>admin</i>	5	26	23.5	$\sim 1.19 \cdot 10^7$
Пароль (буквенно-цифр.,)	8	62	47.6	$\sim 2.18 \cdot 10^{42}$
Пароль ASCII	12	95	78.8	$\sim 5.40 \cdot 10^{72}$
Ключ Ed25519	–	–	256	$\approx 1.16 \cdot 10^{77}$

Крайові умови та обмеження моделі визначають область її коректного застосування:

- Модель коректна для одиночного джерела атаки (одна IP-адреса). При розподіленій атаці (botnet) Fail2ban блокує кожен IP окремо, а загальний N_{window} є сумою по всіх джерелах;
- Модель описує словниковий та повний перебір. Цільові атаки з відомою частиною пароля вимагають корекції E_{str} ;
- Передбачається, що зломисник не знає пароля апіорі (рівномірний розподіл по ключовому простору);
- Модель не враховує вразливостей на прикладному рівні та соціальну інженерію.

2.4 Вибір та обґрунтування метрик ефективності захисту: час до бану, ймовірність компрометації, кількість спроб

Для кількісної оцінки ефективності досліджуваних конфігурацій захисту в роботі використовується система з трьох взаємопов'язаних метрик.

Метрика 1: Латентність захисту (L_{f2b}). Час у секундах між першою зафіксованою спробою входу та моментом додавання атакуючої IP-адреси до блокуючого правила *iptables*. Вимірюється безпосередньо на стенді шляхом порівняння міток часу у */var/log/auth.log* та виводі *journalctl -u fail2ban*. Менше значення – кращий захист.

Метрика 2: Кількість спроб у вікні вразливості (N_{window}). Похідна від L_{f2b} та λ , дає абсолютне число спроб автентифікації, що пройшли через систему до блокування. Безпосередньо рахується з лог-файлу: *grep 'Failed password' /var/log/auth.log | wc -l* за інтервал атаки.

Метрика 3: Ймовірність компрометації (P). Розраховується на основі формули, що пов'язує N_{window} з ентропією пароля. Є узагальнюючим показником, що зводить конфігурацію системи захисту до єдиного числа в діапазоні $[0, 1]$.

Порівняння трьох конфігурацій за даними метриками дозволяє кількісно підтвердити або спростувати гіпотезу роботи: ймовірність компрометації при ключовій автентифікації прямує до нуля незалежно від решти параметрів.

2.5 Перспективний напрямок дослідження: порівняння реактивного та превентивного підходів. Очікувані результати

Центральна гіпотеза роботи формулюється наступним чином: для класу атак Brute Force на SSH-протокол перехід від реактивного захисту (Fail2ban) до превентивного (ключова автентифікація) є не кількісним покращенням одного показника, а якісною зміною архітектурного класу рішення, що проявляється в принципово іншій залежності ймовірності компрометації від параметрів атаки.

Ймовірність компрометації захисті при реактивному захисті визначається за формулою (2.9):

$$P = 1 - \left(1 - \frac{1}{|K|}\right)^{L_{f2b} \cdot \lambda_{att}} \quad (2.9)$$

де $|K| = 2^{E_{str}}$ потужність ключового простору, що визначається через ентропію пароля E_{str} ;

L_{f2b} – час реакції Fail2ban до блокування IP-адреси в секундах;

λ_{att} – інтенсивність потоку запитів зловмисника (спрос/с).

При превентивному захисті парольна автентифікація повністю вимкнена, тому зловмисник позбавлений вектору атаки. Ймовірність компрометації тотожно дорівнює нулю незалежно від інтенсивності атаки λ : $P = 0$.

Очікувані результати дослідження:

– Виміряти реальне значення L_{f2b} для тестового стенду та порівняти з теоретичним мінімумом.

– Кількісно підтвердити, що ймовірність компрометації при ключовій парі Ed25519 є практично нульовою через надзвичайно високий розмір ключового простору 2^{256} .

Теоретичне дослідження (теорія ймовірностей, теорія черг, Марківські процеси) надають математичне підґрунтя для побудови моделі залежності захищеності від факторів вразливості. Концепція «вікна вразливості» формалізує головний недолік реактивного захисту. Визначені метрики (L_{f2b}, N_{window}, P) дозволяють кількісно порівнювати різні конфігурації системи захисту, що є необхідною умовою для верифікації моделі у розділі 3.

3 РОЗРОБКА ТА ВЕРИФІКАЦІЯ ІНФОРМАЦІЙНОЇ МОДЕЛІ ОЦІНКИ ЗАЛЕЖНОСТІ ЗАХИСТУ ВІД ФАКТОРІВ ВРАЗЛИВОСТЕЙ

3.1 Математична модель імовірності компрометації системи при різних сценаріях атак

Для формалізації оцінки захищеності SSH від атак типу Brute-force у цьому розділі розроблено математичну модель, що дозволяє кількісно оцінити ймовірність компрометації системи при трьох архітектурних сценаріях: без засобів захисту, з реактивним захистом Fail2ban та превентивним захистом – ключова пара Ed25519.

Модель є функцією відображення вектору стану системи S у значення ймовірності компрометації P .

Основна функція моделі (3.1):

$$P(S) = (V_{auth} \cdot V_{port}) \cdot \left(1 - \left(1 - \frac{1}{|K|} \right)^{L_{f2b} \cdot \lambda_{att}} \right) \quad (3.1)$$

де, V_{port} – коефіцієнт вразливості порту (1 – відкритий, 0 – закритий)

V_{auth} – коефіцієнт вразливості автентифікації (1 – пароль, 0 автентифікація виконана (Ed25519 режим));

$|K|$ – потужність ключового простору (для пароля це $2^{E_{str}}$, а для ключа Ed25519 це 2^{256});

L_{f2b} – латентність Fail2ban;

λ_{att} – інтенсивність потоку запитів зломисника (спроб/с).

Для ключа Ed25519 розмір ключового простору настільки великий що математичне очікування успішного підбору буде наближатись до нуля.

Ця модель дозволяє провести порівняльний аналіз трьох станів системи:

1. Базовий сценарій без активного захисту: при $V_{port} = 1$ та $V_{auth} = 1$, за відсутності механізмів блокування, параметр латентності L_{f2b} стає довільним часом $t \rightarrow \infty$. Це призводить до того, що $P(S) \rightarrow 1$, підтверджуючи неминучість зламу при достатньому часі атаки.

2. Реактивний сценарій (Fail2ban): Система захисту обмежує час успішної атаки значенням L_{f2b} . Кількість спроб, які встигає зробити зловмисник до моменту спрацювання блокування за формулою (2.6). Саме це значення ми будемо експериментально визначати для різної інтенсивності атаки λ .

3. Превентивний сценарій Ed25519: при використанні ключової автентифікації.

3.2 Архітектура та параметри тестового стенду як дослідної установки

Для експериментальної верифікації розробленої інформаційної моделі оцінки захищеності було розгорнуто ізольоване віртуальне тестове середовище у системі віртуалізації Oracle VM VirtualBox 7.2.6 [32].

Характеристики віртуальних машин наведені в таблиці 3.1.

Таблиця 3.1 – Характеристики віртуальних машин тестового стенду

Параметр	Цільовий вузол	Атакуючий вузол
ОС	Ubuntu Server 26.04 LTS	Kali Linux
CPU	2 vCPU (Ryzen 5 5600H)	2 vCPU (Ryzen 5 5600H)
RAM	2 ГБ	4 ГБ
Мережа	Internal Network 192.168.56.10/24	Internal Network 192.168.56.20/24
Ключові пакети	OpenSSH, Fail2ban	Hydra 9.5
SSH-порт	22 (стандартний)	—

Віртуальні машини об'єднані в ізольовану мережу типу Internal Network з назвою DiplomNet. Така архітектура забезпечує повну ізоляцію тестового стенду від зовнішніх мереж та дозволяє безпечно моделювати brute-force атаки.

Для фіксації стану системи на різних етапах дослідження буде використуватись функція Snapshots (знімки стану віртуальних машин). Це дозволить оперативно відновлювати попередні конфігурації після проведення атак.

Заходи безпеки тестового середовища:

- Використання Internal Network;
- Вимкнення Shared Folders, Drag & Drop та Clipboard Sharing;
- Увімкнення Promiscuous Mode;

Всі налаштування виконувались відповідно до рекомендацій офіційної документації Oracle VM VirtualBox [32].

Віртуальні машини об'єднані в ізольовану мережу типу Internal Network з назвою DiplomNet. Налаштування мережевого адаптера віртуальної машини Target показано на рисунку 3.1.

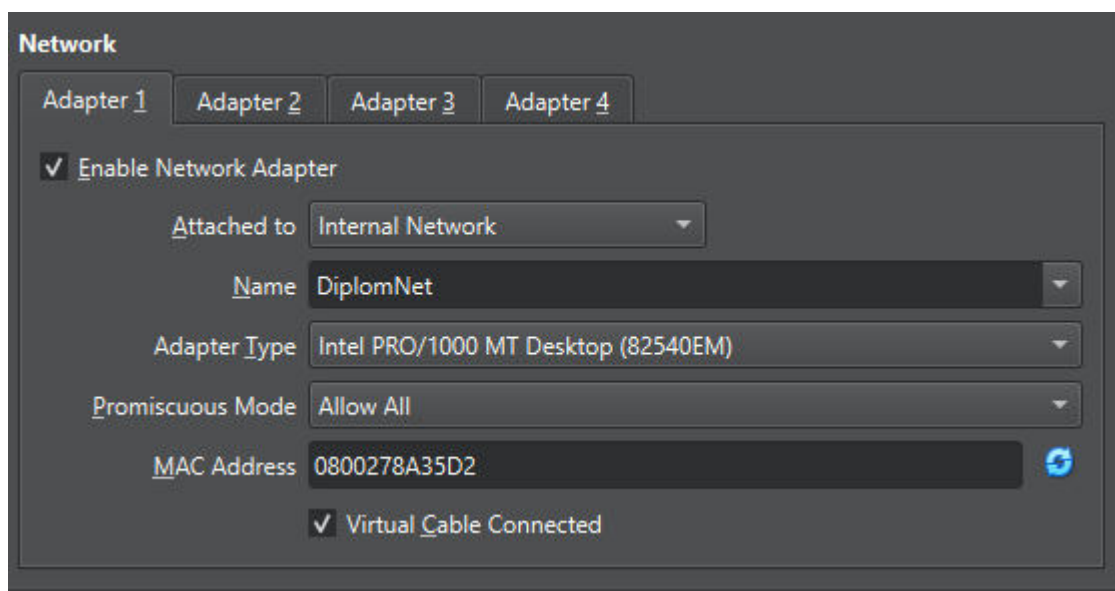


Рисунок 3.1 – Налаштування мережевого адаптера Internal Network «DiplomNet» віртуальної машини Target

Для забезпечення безпеки тестового середовища було вимкнено обмін даними між хостовою та гостьовою системами (Shared Clipboard та Drag-and-Drop), що унеможливило випадковий витік даних поза межі стенду. Налаштування параметрів безпеки показано на рисунку 3.2.



Рисунок 3.2 – Налаштування параметрів безпеки Shared Clipboard та Drag-and-Drop віртуальної машини Target

Налаштування віртуальної машини Kali Linux, яка буде атакувати машину Target зображено на рисунках 3.3 – 3.4.

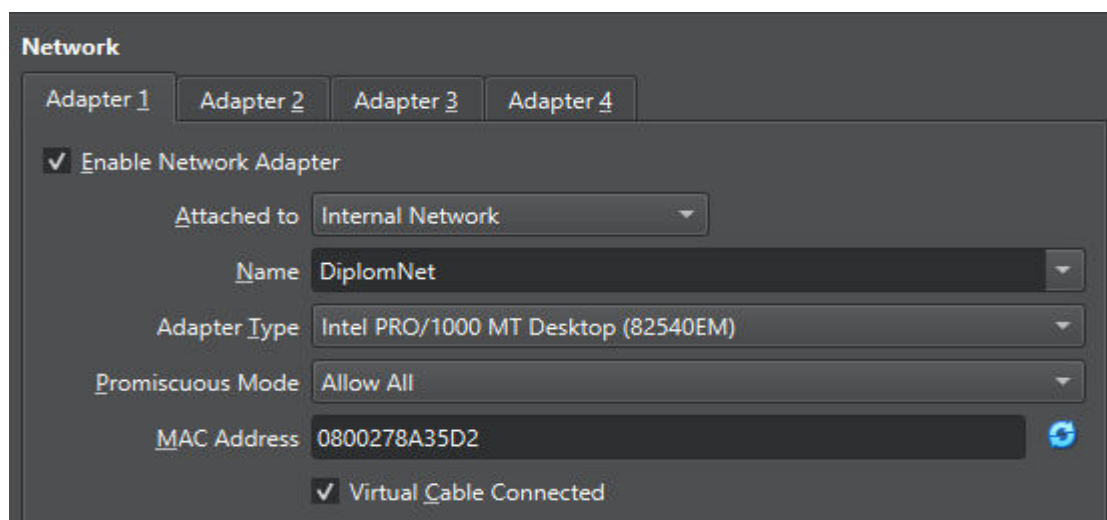
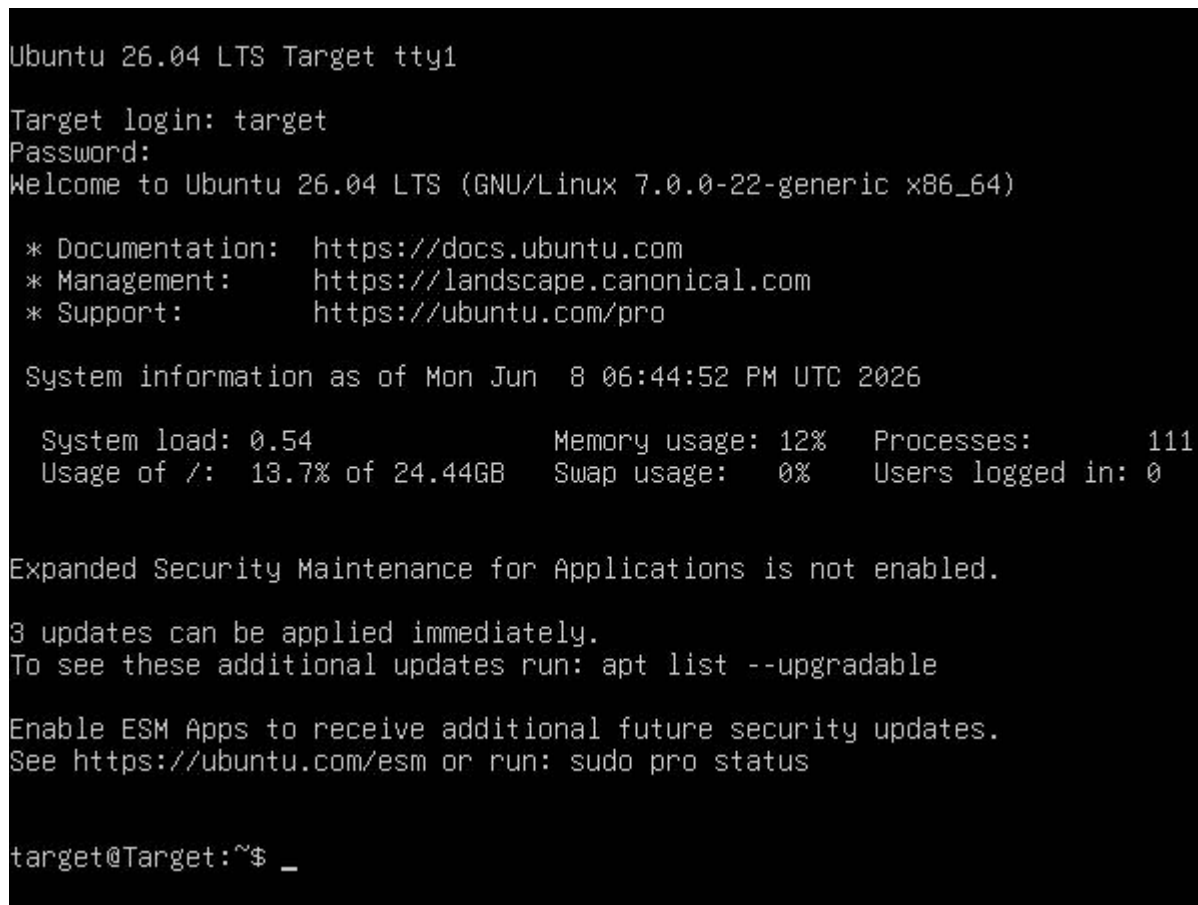


Рисунок 3.3 – Налаштування мережевого адаптера Internal Network «DiplomNet» атакуючої машини Kali



Рисунок 3.4 – Налаштування параметрів безпеки Shared Clipboard та Drag-and-Drop віртуальної атакуючої машини Kali

Після запуску віртуальної машини target маємо такий головний екран, дана ОС має лише CLI, для мінімізації навантаження на систему зображено на рисунку 3.5.



```
Ubuntu 26.04 LTS Target tty1
Target login: target
Password:
Welcome to Ubuntu 26.04 LTS (GNU/Linux 7.0.0-22-generic x86_64)

* Documentation:  https://docs.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/pro

System information as of Mon Jun  8 06:44:52 PM UTC 2026

System load: 0.54           Memory usage: 12%   Processes:      111
Usage of /:  13.7% of 24.44GB Swap usage:   0%    Users logged in: 0

Expanded Security Maintenance for Applications is not enabled.

3 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

target@Target:~$ _
```

Рисунок 3.5 – Головне вікно при ввімкненні сервера

Для налаштування підключення в мережі Internal Network «DiplomNet» треба змінити базові налаштування IP-адрес. Для віртуальної машини Target мережеві налаштування виконуються за допомогою команд:

```
sudo nano /etc/netplan/00-installer-config.yaml
sudo netplan apply
```

Перша команда відкриває конфігураційний файл, а друга застосовує його до всієї системи.

В самому конфігураційному файлі написаний код, який зображено на рисунку 3.6:

```
GNU nano 8.7.1
# This is the network config written by 'subiquity'
network:
  ethernet:
    enp0s3:
      dhcp4: no
      addresses:
        - 192.168.56.10/24
```

Рисунок 3.6 – Код конфігураційного файлу віртуальної машини Target

Перевіряємо чи застосувались зміни наступною командою

ip a

На рисунку 3.7 зображено, що IP-адреса була змінена:

```
target@Target:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:96:a2:9e brd ff:ff:ff:ff:ff:ff
    altname enx08002796a29e
    inet 192.168.56.10/24 brd 192.168.56.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fd17:625c:f037:2:a00:27ff:fe96:a29e/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 86391sec preferred_lft 14391sec
    inet6 fe80::a00:27ff:fe96:a29e/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
```

Рисунок 3.7 – Виконання команди *ip a* для перевірки зміни IP-адреси

Для віртуальної машини Kali прописуємо такі команду для зміни IP-адреси:

```
sudo nmcli con mod "Wired connection 1" ipv4.address 192.168.56.20/24
                                ipv4.method manual
```

Ця команда налаштовує статичну IP-адресу для мережевого підключення. Для того щоб зміни вступили в силу треба прописати наступну команду:

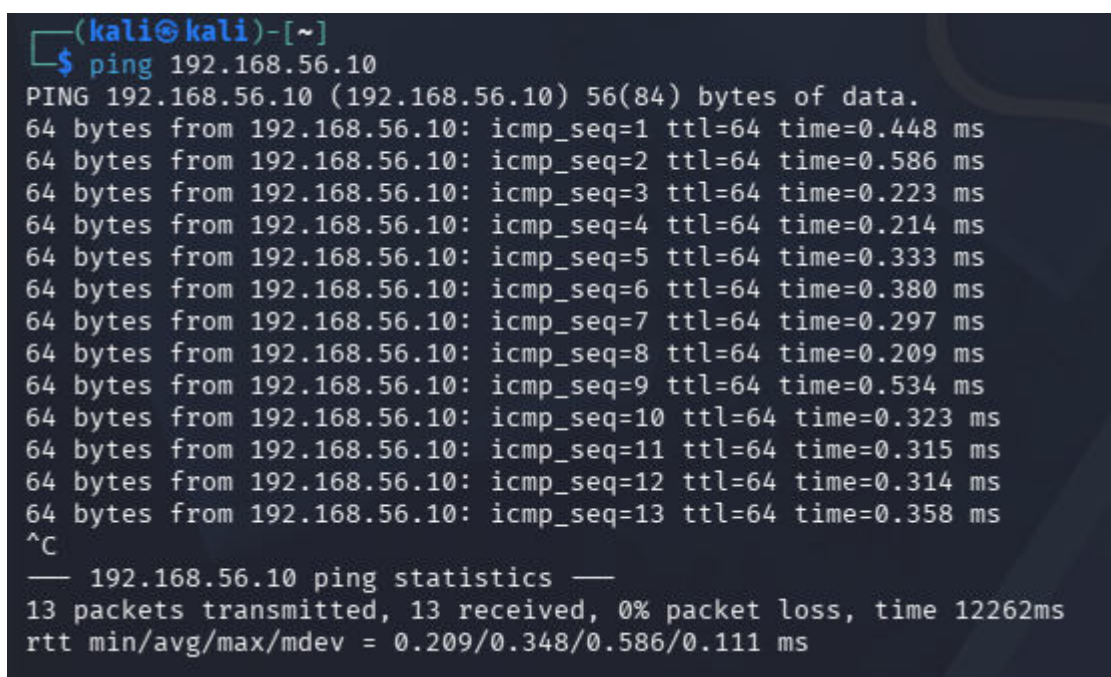
sudo nmcli con up "Wired connection 1"

Команда застосовує зміни, які були прийняті минулою командою.

Перевіряємо чи встановлено з'єднання з іншою машиною:

ping 192.168.56.10

Результат виконання команди зображено на рисунку 3.8, на ньому видно, що пакети відправляються на іншу віртуальну машину, отже з'єднання успішно встановлене.



```
(kali㉿kali)-[~]  
$ ping 192.168.56.10  
PING 192.168.56.10 (192.168.56.10) 56(84) bytes of data.  
64 bytes from 192.168.56.10: icmp_seq=1 ttl=64 time=0.448 ms  
64 bytes from 192.168.56.10: icmp_seq=2 ttl=64 time=0.586 ms  
64 bytes from 192.168.56.10: icmp_seq=3 ttl=64 time=0.223 ms  
64 bytes from 192.168.56.10: icmp_seq=4 ttl=64 time=0.214 ms  
64 bytes from 192.168.56.10: icmp_seq=5 ttl=64 time=0.333 ms  
64 bytes from 192.168.56.10: icmp_seq=6 ttl=64 time=0.380 ms  
64 bytes from 192.168.56.10: icmp_seq=7 ttl=64 time=0.297 ms  
64 bytes from 192.168.56.10: icmp_seq=8 ttl=64 time=0.209 ms  
64 bytes from 192.168.56.10: icmp_seq=9 ttl=64 time=0.534 ms  
64 bytes from 192.168.56.10: icmp_seq=10 ttl=64 time=0.323 ms  
64 bytes from 192.168.56.10: icmp_seq=11 ttl=64 time=0.315 ms  
64 bytes from 192.168.56.10: icmp_seq=12 ttl=64 time=0.314 ms  
64 bytes from 192.168.56.10: icmp_seq=13 ttl=64 time=0.358 ms  
^C  
— 192.168.56.10 ping statistics —  
13 packets transmitted, 13 received, 0% packet loss, time 12262ms  
rtt min/avg/max/mdev = 0.209/0.348/0.586/0.111 ms
```

Рисунок 3.8 – Результат встановлення з'єднання

Перевіряємо чи працює на сервері SSH прописавши команду:

sudo systemctl status ssh

```

target@Target:~$ sudo systemctl status ssh
• ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: enabled)
   Active: active (running) since Mon 2026-06-08 20:25:40 UTC; 3s ago
     Invocation: 17f1708ba41c478cb685caf782c5ba2d
   TriggeredBy: • ssh.socket
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 1962 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 1964 (sshd)
     Tasks: 1 (limit: 1888)
    Memory: 1.9M (peak: 2.3M)
       CPU: 53ms
    CGroup: /system.slice/ssh.service
            └─1964 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Jun 08 20:25:40 Target systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Jun 08 20:25:40 Target sshd[1964]: Server listening on 0.0.0.0 port 22.
Jun 08 20:25:40 Target sshd[1964]: Server listening on :: port 22.
Jun 08 20:25:40 Target systemd[1]: Started ssh.service - OpenBSD Secure Shell server.

```

Рисунок 3.9 – Результат виконання команди *sudo sysmtemctl status ssh*

За результатами виконання команди підтверджено активний стан сервісу SSH, результат зображено на рисунку 3.9. Для налаштування відкриваємо конфігураційний файл командою::

sudo nano /etc/ssh/sshd_config

Ставимо наступні параметри, *Port 22*, *MaxAuthTries 100*, *PasswordAuthentication yes*, *PermitEmptyPasswords yes*. Ці налаштування вказують, що SSH знаходиться на 22 порту, та обмеження кількості спроб в одній SSH сесії 100 (для ефективного захисту ставлять 3-6, але в контексті роботи взято більше, щоб при використанні з'єднання не розривалось), та ввімкнено парольну автентифікацію. На рисунках 3.10-3.11 зображено текст з конфігураційного файлу, де вказано налаштування.

```

Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
MaxAuthTries 100
#MaxSessions 10

```

Рисунок 3.10 – Налаштування конфігураційного файлу

```

# To disable tunneled clear text passwords, change to "no" here!
PasswordAuthentication yes
PermitEmptyPasswords yes

```

Рисунок 3.11 – Налаштування конфігураційного файлу

Щоб налаштування були прийняті застосовуємо команду:

sudo systemctl restart ssh

Створюємо простий словник паролів, зображено на рисунку 3.12, щоб зменшити час на тестування моделі для першого сценарію.

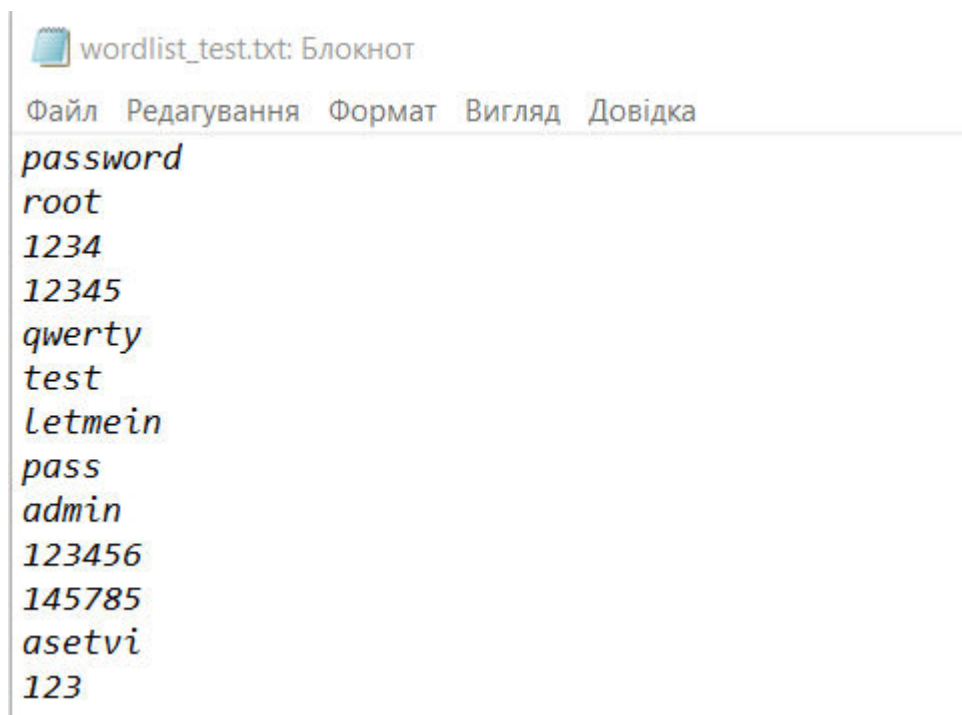


Рисунок 3.12 – Словник паролів тестового стенду

Конфігурацію Fail2ban на цільовому вузлі налаштовано зі стандартними параметрами: `maxretry = 3`, `findtime 600` секунд, `bantime = 3600` секунд. Саме ці значення є базовими для вимірювання латентності захисту у підрозділі 3.3. Файл конфігурації `/etc/fail2ban/jail.local` показано на рисунку 3.13.

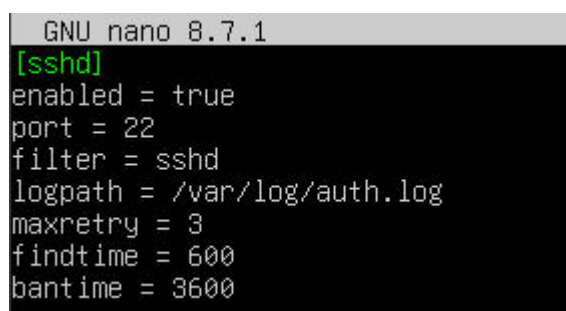


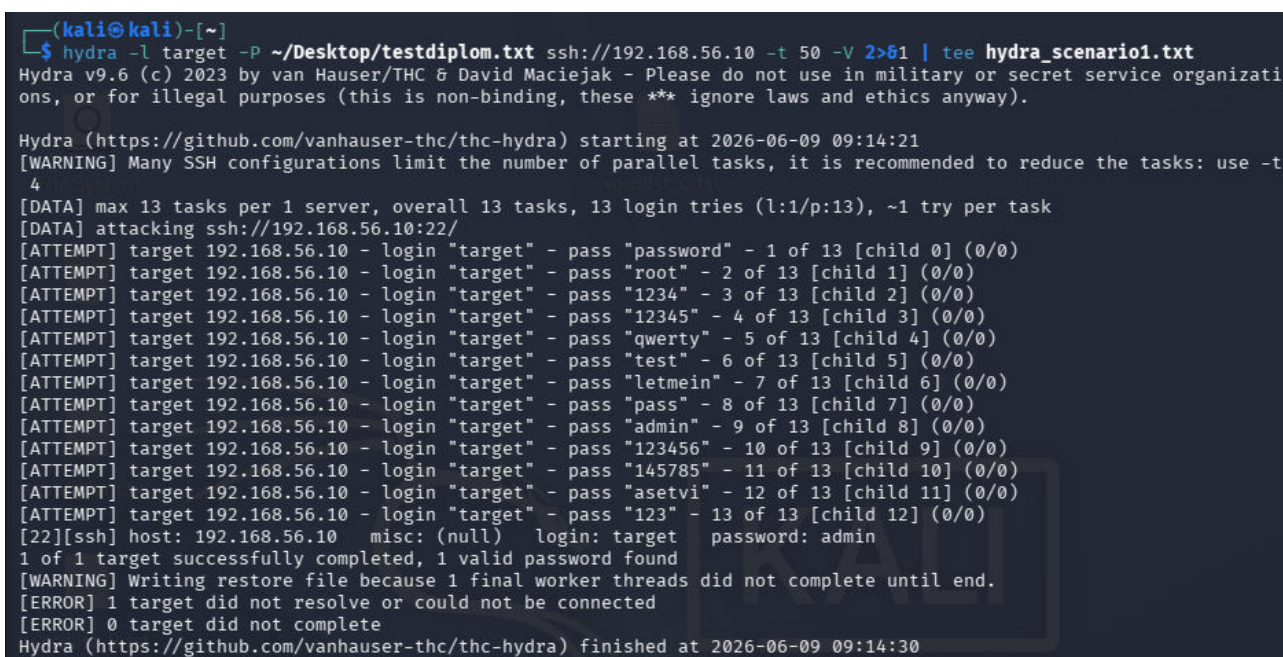
Рисунок 3.13 – Конфігурація Fail2ban

3.3 Базовий сценарій: тестування SSH без засобів захисту та кількісна оцінка параметрів атаки

Запускаємо атаку на атакуючій машині вводимо команду:


```
hydra -l target -P /usr/share/wordlists/testdiplom.txt ssh://192.168.56.10 -t 50 -V
2>&1 | tee hydra_scenario1.txt
```

Результат атаки зображено на рисунках 3.14-3.15



```
(kali@kali)-[~]
$ hydra -l target -P ~/Desktop/testdiplom.txt ssh://192.168.56.10 -t 50 -V 2>&1 | tee hydra_scenario1.txt
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-06-09 09:14:21
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 13 tasks per 1 server, overall 13 tasks, 13 login tries (l:1/p:13), ~1 try per task
[DATA] attacking ssh://192.168.56.10:22/
[ATTEMPT] target 192.168.56.10 - login "target" - pass "password" - 1 of 13 [child 0] (0/0)
[ATTEMPT] target 192.168.56.10 - login "target" - pass "root" - 2 of 13 [child 1] (0/0)
[ATTEMPT] target 192.168.56.10 - login "target" - pass "1234" - 3 of 13 [child 2] (0/0)
[ATTEMPT] target 192.168.56.10 - login "target" - pass "12345" - 4 of 13 [child 3] (0/0)
[ATTEMPT] target 192.168.56.10 - login "target" - pass "qwerty" - 5 of 13 [child 4] (0/0)
[ATTEMPT] target 192.168.56.10 - login "target" - pass "test" - 6 of 13 [child 5] (0/0)
[ATTEMPT] target 192.168.56.10 - login "target" - pass "letmein" - 7 of 13 [child 6] (0/0)
[ATTEMPT] target 192.168.56.10 - login "target" - pass "pass" - 8 of 13 [child 7] (0/0)
[ATTEMPT] target 192.168.56.10 - login "target" - pass "admin" - 9 of 13 [child 8] (0/0)
[ATTEMPT] target 192.168.56.10 - login "target" - pass "123456" - 10 of 13 [child 9] (0/0)
[ATTEMPT] target 192.168.56.10 - login "target" - pass "145785" - 11 of 13 [child 10] (0/0)
[ATTEMPT] target 192.168.56.10 - login "target" - pass "asetvi" - 12 of 13 [child 11] (0/0)
[ATTEMPT] target 192.168.56.10 - login "target" - pass "123" - 13 of 13 [child 12] (0/0)
[22][ssh] host: 192.168.56.10 misc: (null) login: target password: admin
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-06-09 09:14:30
```

Рисунок 3.14 – Результат атаки підбором з атакуючої віртуальної машини

Для перевірки логів було використано наступні команди:

```
grep "Failed password" /var/log/auth.log | head -1
grep "Accepted password" /var/log/auth.log
grep "Failed password" /var/log/auth.log | wc -l
```

Перша виводить лише перший знайдений рядок, щоб побачити час коли почалась атака. Друга команда рахує скільки було невдалих спроб входу.

```

root@Target:/home/target# grep "Accepted password" /var/log/auth.log
2026-06-09T04:42:23.855178+00:00 Target sshd-session[6767]: Accepted password for target from 192.168.56.20 port 47698 ssh2
root@Target:/home/target# grep "Failed password" /var/log/auth.log
2026-06-09T04:42:24.799319+00:00 Target sshd-session[6766]: Failed password for target from 192.168.56.20 port 47692 ssh2
2026-06-09T04:42:24.934446+00:00 Target sshd-session[6763]: Failed password for target from 192.168.56.20 port 47664 ssh2
2026-06-09T04:42:25.203892+00:00 Target sshd-session[6773]: Failed password for target from 192.168.56.20 port 47724 ssh2
2026-06-09T04:42:25.226175+00:00 Target sshd-session[6759]: Failed password for target from 192.168.56.20 port 47656 ssh2
2026-06-09T04:42:25.254257+00:00 Target sshd-session[6764]: Failed password for target from 192.168.56.20 port 47676 ssh2
2026-06-09T04:42:25.332281+00:00 Target sshd-session[6757]: Failed password for target from 192.168.56.20 port 47646 ssh2
2026-06-09T04:42:25.358188+00:00 Target sshd-session[6755]: Failed password for target from 192.168.56.20 port 47618 ssh2
2026-06-09T04:42:25.506958+00:00 Target sshd-session[6776]: Failed password for target from 192.168.56.20 port 47750 ssh2
2026-06-09T04:42:25.575714+00:00 Target sshd-session[6760]: Failed password for target from 192.168.56.20 port 47662 ssh2
2026-06-09T04:42:25.719983+00:00 Target sshd-session[6756]: Failed password for target from 192.168.56.20 port 47634 ssh2
2026-06-09T04:42:26.060397+00:00 Target sshd-session[6770]: Failed password for target from 192.168.56.20 port 47708 ssh2
root@Target:/home/target# grep "Accepted password" /var/log/auth.log | tail -1
2026-06-09T04:42:23.855178+00:00 Target sshd-session[6767]: Accepted password for target from 192.168.56.20 port 47698 ssh2
root@Target:/home/target# _

```

Рисунок 3.15 – Результат атаки з цільової віртуальної машини

Можна побачити, що злам відбувся за 1.26 секунди, що відповідає 10 спробам в секунду (10.72). А сам вхід відбувся на 0.94 секунди раніше ніж це зафіксувала система.

3.4 Реактивний сценарій: тестування ефективності Fail2ban та вимірювання латентності захисту L_{f2b}

Запускаємо сервіс Fail2ban та перевіряємо його статус командами:

```

sudo systemctl start fail2ban
sudo systemctl status fail2ban

```

Результат виконання команд зображено на рисунку 3.16.

```

root@target:/home/target# sudo systemctl start fail2ban
root@Target:/home/target# sudo systemctl status fail2ban
• fail2ban.service - Fail2Ban Service
   Loaded: loaded (/usr/lib/systemd/system/fail2ban.service; enabled; preset: enabled)
   Active: active (running) since Tue 2026-06-09 07:07:24 UTC; 12min ago
   Invocation: 7724d728bad84e6398b0f3b65743f798
     Docs: man:fail2ban(1)
   Main PID: 1000 (fail2ban-server)
     Tasks: 5 (limit: 1888)
    Memory: 45.2M (peak: 45.2M)
       CPU: 636ms
    CGroup: /system.slice/fail2ban.service
            └─1000 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Jun 09 07:07:24 Target systemd[1]: Started fail2ban.service - Fail2Ban Service.
Jun 09 07:07:26 Target fail2ban-server[1000]: Server ready

```

Рисунок 3.16 – Ввімкнення та перевірка працездатності Fail2ban

Запускаємо нову атаку і використовуємо аналогічну команду для цього використано словник з паролями який наведено в ДОДАТКУ Б.

```
hydra -l target -P ~/Desktop/wordlist_A.txt ssh://192.168.56.10 -t 50 -V 2>&1  
| tee hydra_scenario2.txt
```

Перше, що було перевірено, чи потрапила атакуюча машина до списку заблокованих за IP-адресою, зображено на рисунку 3.17, команда для перевірки:

```
sudo fail2ban-client status sshd
```



```
root@Target:/home/target# sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|   |- Currently failed: 1
|   |- Total failed:      39
|   \- Journal matches:  _SYSTEMD_UNIT=ssh.service + _COMM=sshd
|- Actions
|   |- Currently banned: 1
|   |- Total banned:      1
|   \- Banned IP list:   192.168.56.20
```

Рисунок 3.17 – Список заблокованих IP-адрес

Бачимо, що атакуюча машина була заблокована, перевіряємо логи, щоб побачити, чи був підібраний пароль, скільки спроб перевірки реально було це зображено на рисунку 3.18.



```
root@Target:/home/target# sudo grep "Accepted password" /var/log/auth.log
2026-06-09T19:21:03.042715+00:00 Target sshd-session[1705]: Accepted password for target from 192.168.56.20 port 43756 ssh2
2026-06-09T19:44:59.748576+00:00 Target sudo: root : TTY=/dev/pts/1 ; PWD=/home/target ; USER=root ; COMMAND=/usr/bin/grep Accep
2026-06-09T19:46:44.567295+00:00 Target sudo: root : TTY=/dev/pts/0 ; PWD=/home/target ; USER=root ; COMMAND=/usr/bin/grep Accep
2026-06-09T19:57:54.751152+00:00 Target sudo: root : TTY=/dev/pts/0 ; PWD=/home/target ; USER=root ; COMMAND=/usr/bin/grep Accep
2026-06-09T19:59:10.496758+00:00 Target sudo: root : TTY=/dev/pts/0 ; PWD=/home/target ; USER=root ; COMMAND=/usr/bin/grep Accep
root@Target:/home/target# grep "Failed password" /var/log/auth.log | head -1
2026-06-09T19:20:59.691252+00:00 Target sshd-session[1705]: Failed password for target from 192.168.56.20 port 43756 ssh2
root@Target:/home/target# grep "Failed password" /var/log/auth.log | wc -l
39
root@Target:/home/target#
```

Рисунок 3.18 – Успішно підібраний пароль, кількість спроб до блокування та час скільки тривала атака

Аналіз логів першого досліду дав такі результати: перша невдала спроба зафіксована о $t_0 = 19:21:01$, блокування IP-адреси відбулось о $t_{\text{ban}} = 19:21:01.546$. Латентність захисту за формулою

Перевіряємо це з іншим λ . Перезапускаємо цей дослід з 64 потоками:

hydra -l target -P wordlist_A.txt ssh://192.168.56.10 -t 64 -V 2>&1 | tee hydra_A_t64.txt

Перевіряємо після атаки чи була заблокована адреса (рис. 3.19):

```
root@Target:/home/target# sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 1
| |- Total failed: 47
| - Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
- Actions
| |- Currently banned: 1
| |- Total banned: 1
| - Banned IP list: 192.168.56.20
root@Target:/home/target# grep "Failed password" /var/log/auth.log | head -1
2026-06-09T20:41:17.272812+00:00 Target sshd-session[1572]: Failed password for target from 192.168.56.20 port 41118 ssh2
root@Target:/home/target# grep "Accepted password" /var/log/auth.log
2026-06-09T20:41:20.258888+00:00 Target sshd-session[1640]: Accepted password for target from 192.168.56.20 port 41458 ssh2
root@Target:/home/target# grep "Failed password" /var/log/auth.log | wc -l
47
root@Target:/home/target# _
```

Рисунок 3.19 – Заблокована IP-адреса за допомогою утиліти Fail2ban, та аналіз логи, що отримано в наслідок дослідження

Прописавши наступну команду було отримано час коли система заблокувала IP-адресу, на рисунку 3.20 результат виконання команди.

grep -i "ban 192.168.56.20" /var/log/fail2ban.log

```
2026-06-09 20:41:18,092 fail2ban.actions [1011]: NOTICE [sshd] Ban 192.168.56.20
```

Рисунок 3.20 – Час блокування IP-адреси за допомогою fail2ban

Після аналізу $L_{f2b} = t_{\text{ban}} - t_0 = 20:41:18.092 - 20:41:17 = 1.092 \approx 1$ с. Після минулого взлому був аналогічний результат, програма заблокувала IP-адресу до

того, як було отримано сповіщення що систему успішно зламано це зображено на рисунку 3.21.

```
2026-06-09 19:21:01,546 fail2ban.actions [1009]: NOTICE [sshd] Ban 192.168.56.20
```

Рисунок 3.21 – Час блокування IP-адреси за допомогою fail2ban

3.5 Превентивний сценарій: автентифікація за ключовою парою Ed25519 як контрольний сценарій верифікації

Третій сценарій є контрольним у структурі дослідження – він верифікує центральну гіпотезу роботи про якісну відмінність між реактивним і превентивними підходами до захисту SSH. На відміну від сценаріїв 1 і 2 де вектор таки існував і реалізовувався через парольну автентифікацію, у даному сценарії парольна автентифікація повністю вимикається на рівні конфігурації OpenSSH, що унеможлиблює атаку типу Brute Force як клас загроз. Для розгортання ключової автентифікації на цільовому вузлі Target виконано такі кроки. На вузлі Kali Linux згенеровано ключову пару Ed25519 командою:

```
ssh-keygen -t ed25519 -C "diplom_test" -f ~/.ssh/id_ed25519_test
```

Результат виконання коду зображено на рисунку 3.22.

```
(kali@kali)-[~]
$ ssh-keygen -t ed25519 -C "diplom_test" -f ~/.ssh/id_ed25519_test
Generating public/private ed25519 key pair.
Enter passphrase for "/home/kali/.ssh/id_ed25519_test" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kali/.ssh/id_ed25519_test
Your public key has been saved in /home/kali/.ssh/id_ed25519_test.pub
The key fingerprint is:
SHA256:decLF1S/SW1P4JDg67NP1BR6Gu3+g8Vu2pLSAtbYXvM diplom_test
The key's randomart image is:
+--[ED25519 256]--+
|      .. oo+  |
|      .  ..= +. |
|      o = *. =  |
|      Teach . o @.o+ |
|      S = = =o. |
|      = = = +  |
|      . = + X   |
|      B = .E   |
|      ..+.+.o  |
+-----[SHA256]-----+
testdiplom_test
(kali@kali)-[~]
$
```

Рисунок 3.22 – Згенеровано ключ Ed25519

Були змінені файли конфігурації SSH на цільовому вузлі:

nano /etc/ssh/sshd_config

Було змінено такі параметри як *PasswordAuthentication* та *PubkeyAuthentication* змінені параметри зображені на рисунку 3.23.

```

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
MaxAuthTries 100
#MaxSessions 10

PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to "no" here!
PasswordAuthentication no
PermitEmptyPasswords yes

```

Рисунок 3.23 – Вимкнення автентифікації за допомогою пароля, та ввімкнення автентифікації за ключовою парою

Публічний ключ скопійовано на цільовий вузол командою:

```
ssh-copy-id -i ~/.ssh/id_ed25519_test.pub target@192.168.56.10
```

Результат зображено на рисунку 3.24.

```
(kali@kali)-[~]
$ ssh-copy-id -i ~/.ssh/id_ed25519_test.pub target@192.168.56.10
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/kali/.ssh/id_ed25519_test.pub"
The authenticity of host '192.168.56.10 (192.168.56.10)' can't be established.
ED25519 key fingerprint is: SHA256:DLxLSRBSVTtNiTNqje7tty80j0v3yuZCNnj1TwI6SI4
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
target@192.168.56.10's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh -i /home/kali/.ssh/id_ed25519_test 'target@192.168.56.10'"
and check to make sure that only the key(s) you wanted were added.
```

Рисунок 3.24 – Результат копіювання ключа

Генерація ключової пари виконана саме на вузлі Kali Linux, а не на цільовому сервері Target, що є принципово важливим з точки зору безпеки та повністю відповідає стандарту RFC 8709 [31] і рекомендаціям NIST IR 7966 [23]. Відповідно до цих документів, приватний ключ має генеруватися і зберігатися виключно на стороні того хто автентифікується – тобто на клієнтському вузлі. Мережею передається лише публічний ключ, який не є секретом і перехоплення якого не надає зловмиснику жодних переваг. Генерація ключа на сервері з подальшою передачею приватного ключа клієнту є грубою помилкою безпеки оскільки в такому разі приватний ключ передається мережею і може бути перехоплений. Таким чином, архітектура розгортання ключової автентифікації у даному дослідженні повністю відповідає встановленим міжнародним стандартам.

Свідомим методологічним рішенням є використання вузла Kali Linux одночасно як клієнта для ключової автентифікації і як атакуючого вузла у попередніх сценаріях. Це рішення обґрунтовується концепцією Zero Trust [16, 23], яка стверджує що рівень захисту системи має визначатися виключно механізмом автентифікації, а не ідентичністю або репутацією вузла мережі.

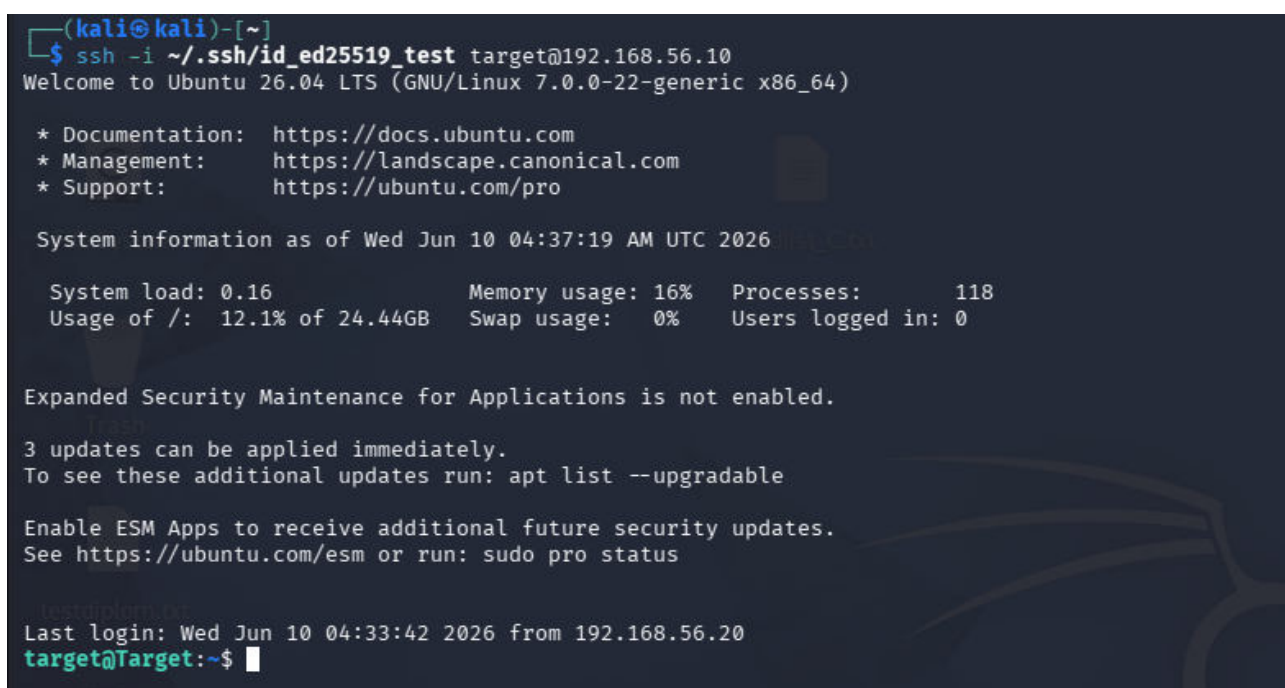
Та сама машина яка у сценаріях 1 і 2 здійснювала brute-force атаку, у сценарії 3 отримує легітимний доступ через ключову автентифікацію – і навпаки, після підтвердження легітимного доступу проти неї запускається повторна атака Hydra з тим самим словником і тією самою інтенсивністю це зображено на рисунку 3.27. Це дозволяє порівняти два стани тієї самої машини і довести що вектор

атаки закривається зміною механізму автентифікації, а не блокуванням конкретного вузла мережі.

Щоб перевірити, чи працює автентифікація за ключовою парою введено наступну команду:

```
ssh -i ~/.ssh/id_ed25519_test target@192.168.56.10
```

Результат виконання команди зображено на рисунку 3.25.



```
(kali@kali)-[~]
$ ssh -i ~/.ssh/id_ed25519_test target@192.168.56.10
Welcome to Ubuntu 26.04 LTS (GNU/Linux 7.0.0-22-generic x86_64)

 * Documentation:  https://docs.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Wed Jun 10 04:37:19 AM UTC 2026

System load: 0.16           Memory usage: 16%    Processes:      118
Usage of /:  12.1% of 24.44GB Swap usage:   0%      Users logged in: 0

Expanded Security Maintenance for Applications is not enabled.

3 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Wed Jun 10 04:33:42 2026 from 192.168.56.20
target@target:~$
```

Рисунок 3.25 – Успішний вхід по SSH

З цієї ж машини, можна перевірити в лог файлах автентифікації, як було під’єднано до системи командою:

```
sudo grep "Accepted publickey" /var/log/auth.log
```

Результат виконання команди зображено на рисунку 3.26, на ньому видно, що автентифікація була здійснена за допомогою Ed25519.


```
target@target:~$ sudo grep "Accepted publickey" /var/log/auth.log
2026-06-10T04:35:34.855002+00:00 Target sudo: target : TTY=/dev/pts/1 ; PWD=/home/target ; USER=root ; COMMAND=/usr/bin/grep Accepted publickey /var/log/auth.log
2026-06-10T04:37:19.447634+00:00 Target sshd-session[3138]: Accepted publickey for target from 192.168.56.20 port 54258 ssh2: ED25519 SHA256:declF1S/SW1P4J0g67NP18REGu3+gBVu2pLSAtbYXvM
2026-06-10T04:54:00.214345+00:00 Target sudo: target : TTY=/dev/pts/1 ; PWD=/home/target ; USER=root ; COMMAND=/usr/bin/grep Accepted publickey /var/log/auth.log
target@target:~$
```

Рисунок 3.26 – Результат перевірки логів

На рисунку 3.27 видно, що атака, не змогла відбутись через автентифікацію за ключовою парою.

```
(kali@kali)-[~]
$ hydra -l target -P ~/Desktop/wordlist_A.txt ssh://192.168.56.10 -t 64 -V 2>61
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-06-10 12:41:32
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 64 tasks per 1 server, overall 64 tasks, 104 login tries (l:1/p:104), ~2 tries per task
[DATA] attacking ssh://192.168.56.10:22/
[ERROR] target ssh://192.168.56.10:22/ does not support password authentication (method reply 4).
```

Рисунок 3.27 – Результат невдалої атаки на 22 порт

На рисунку 3.28 зображено аналіз логів та виклик статусу ssh через програму fail2ban, на ньому видно, що атаки не відбулось, з'єднань не було, заблокованих IP-адрес немає.

```
root@target:/home/target# sudo grep "Accepted password" /var/log/auth.log
2026-06-09T21:26:40.035500+00:00 Target sudo: root : TTY=/dev/pts/0 ; PWD=/home/target ; USER=root ; COMMAND=/usr/bin/grep Accepted password /var/log/auth.log
root@target:/home/target# grep "Failed password" /var/log/auth.log
root@target:/home/target# grep "Accepted publickey" /var/log/auth.log
root@target:/home/target# sudo fail2ban-client status sshd
Status for the jail: sshd
- Filter
  - Currently failed: 0
  - Total failed: 0
  - Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
- Actions
  - Currently banned: 0
  - Total banned: 0
  - Banned IP list:
```

Рисунок 3.28 – Аналіз логів та статусу Fail2ban

Отримані результати підтвердили що жодної успішної автентифікації з боку атакуючого вузла не зафіксовано. Кількість записів "Failed password" у /var/log/auth.log дорівнює нулю – з'єднання відхиляються на рівні протоколу SSH ще до будь-якого аналізу логів Fail2ban, оскільки сервер не приймає парольну автентифікацію як метод взагалі. Це принципова архітектурна відмінність від реактивного сценарію: Fail2ban навіть не залучається до захисту бо атакуючий не може ініціювати валідну спробу автентифікації.

3.6 Порівняльний аналіз отриманих результатів та верифікація моделі

Для верифікації розробленої інформаційної моделі проведено розрахунок імовірності компрометації $P(S)$ для кожного з трьох досліджених сценаріїв, використовуючи експериментальні дані, отримані на тестовому стенді.

Згідно з інформаційною моделлю (формула 3.1) ймовірність компрометації обчислюється залежно від коефіцієнтів – коефіцієнту вразливості порту V_{port} , автентифікації V_{auth} , потужності ключового простору $|K|$, інтенсивності атаки λ_{att} та латентності захисту L_{f2b} .

1. Сценарій 1. Без засобів захисту:

У цьому сценарії цільова система була відкрита для атаки, а засоби блокування були відсутні $L_{f2b} \rightarrow \infty$. Атака здійснювалася за невеликим словником (Додаток А), тому потужність ключового простору $|K| = D = 13$ паролів. За відсутності обмежень часу N прямує до нескінченності, або обмежується лише розміром словника. Оскільки атакуючий має достатньо часу для повного перебору, імовірність компрометації досягає свого максимуму:

$$P(S_1) \rightarrow 1 \text{ (або 100\%)}$$

Емпіричні дані підтверджують це – система була зламана за 1.26 секунди.

2. Реактивний захист (Fail2ban)

У цьому сценарії працював механізм Fail2ban, який обмежує час атаки. Зафіксовані такі емпіричні параметри: Словник (Додаток Б) містить $D = 106$ паролів. Отже $|K| = 106$. Інтенсивність атаки інструментом Hydra у 64 потоки становила $\lambda \approx 47$ спроб/с (виміряна емпірично за лог-файлом, оскільки реальна пропускна здатність SSH-сервера обмежує кількість одночасно оброблюваних з'єднань). Аналіз логів Fail2ban показав, що перша спроба зафіксована о 20:41:17, а блокування відбулося о 20:41:18.092. Реальна кількість записів «Failed password»

у вікні вразливості, зафіксована у лог-файлі, становила 47. Розрахункове значення за формулою (2.6):

$$N_{window} = \lambda \cdot L_{f2b} = 47 \cdot 1 = 47 \text{ спроби}$$

Підставивши ці дані у формулу для розрахунку ймовірності компрометації (2.9), отримано:

$$P(S_2) \approx 1 - (0.9906)^{47} \approx 0.357$$

Отримана ймовірність 35.7% математично доводить явище Race Condition. Завдяки затримці в 1 секунду та інтенсивності атаки ~ 47 спроб/с, зломисник встиг відправити 47 запитів до моменту бану, що дало йому майже 36% шансів на успіх при використанні даного словника зі 106 паролів. Важливо зазначити, що незважаючи на відносно невисоку теоретичну ймовірність, експеримент підтвердив успішний злам – це пояснюється словниковим характером атаки, де реальний пароль «admin» знаходився в першій половині словника.

3. Сценарій 3: Превентивний захист (Ключова пара Ed25519)

У даному сценарії автентифікація за паролем повністю вимкнена, тому вразливість автентифікації $V_{auth} = 0$. Зломисник позбавлений вектору атаки, а всі запити відхиляються на рівні протоколу до аналізу логів. Ймовірність компрометації тотожно дорівнює нулю. Експериментальні дані це підтвердили: у логах відсутні навіть записи про невдалі спроби входу.

Висновки щодо верифікації зведені в таблиці 3.2

Таблиця 3.2 – Зведена таблиця отриманих результатів

Параметр	Базовий	Реактивний	Превентивний
Коефіцієнт автентифікації V_{auth}	1	1	0

Продовження таблиці 3.2

Параметр	Базовий	Реактивний	Превентивний
Ймовірність компрометації	$\approx 100\%$	35.7%	0%
λ (спроб/с)	10.3	64	0
Емпіричний результат	Успішний злам	Успішний злам	Атака неможлива
Латентність L_{f2b}	Не обмежена	1с	Відсутня
Кількість спроб Nwindow	13	47	0

У таблиці 3.2 наведено округлене значення 1 с як консервативна оцінка, що відповідає максимальному зафіксованому значенню та є більш безпечним припущенням для розрахунку ймовірності компрометації — оскільки більше значення L_{f2b} дає більше N_{window} і, відповідно, вищу розрахункову $P(S)$, що не знижує реальний ризик. Базовий сценарій використовував словник Додатку А ($|K|=13$) для демонстрації швидкості злому без захисту. Реактивний — Додаток Б ($|K|=106$) для вимірювання латентності Fail2ban при реалістичному навантаженні. Параметри навмисно відрізняються: перший сценарій досліджує відсутність захисту, другий — поведінку захисту під навантаженням.

Проведені експериментальні дослідження дозволили не лише зібрати кількісні показники стійкості різних архітектурних конфігурацій протоколу SSH, а й візуалізувати приховані процеси, що відбуваються під час атаки. Отримані в розділі 3 лог-файли демонструють критичну вразливість реактивного підходу — явище «динаміки перегонів» (Race Condition) у механізмах захисту.

Як було показано на графі станів марківського процесу (розділ 2.1), під час атаки система переходить зі стану спокою S_0 у стан «вікна вразливості» S_1 . Далі існують два конкуруючі переходи:

1. $S_1 \rightarrow S_2$: перехід у стан блокування (спрацьовує Fail2ban).

2. $S_1 \rightarrow S_3$: перехід у стан компрометації (зловмиснику вдається підібрати пароль).

Експериментально зафіксовано ситуацію, коли мітка часу блокування (Ban) у файлі *fail2ban.log* (20:41:18.092) передує або майже збігається із записом про успішний вхід *Accepted password* у файлі *auth.log*. Оскільки інтенсивність атаки була високою (64 паралельних потоки інструменту Hydra, $\lambda \approx 47$ спроб/с), система, перебуваючи в стані S_1 з латентністю $L_{f2b} = 1$ с, накопичила 47 запитів швидше, ніж скрипти Fail2ban встигли проаналізувати логи та оновити правила міжмережевого екрана *iptables*.

У результаті відбувся розгалужений перехід: система формально ініціювала перехід у захищений стан S_2 (блокування IP-адреси 192.168.56.20), але через програмну латентність L_{f2b} паралельно здійснився фатальний перехід у поглинаючий стан компрометації S_3 . Тобто Fail2ban заблокував зловмисника вже після того, як один із паралельних потоків встиг встановити легітимну SSH-сесію.

Цей факт має принципове значення для інтерпретації розробленої математичної моделі та доводить два ключових висновки:

- Навіть коректно налаштований реактивний захист не гарантує безпеки при достатній інтенсивності атаки λ та недостатній ентропії пароля. Теоретична $P(S_2) = 35.7\%$ при рівномірному розподілі по ключовому простору підтверджує наявність вікна вразливості. Фактичний злам відбувся через словниковий характер атаки, де пароль «admin» знаходився у першій половині словника – що є окремим, більш несприятливим сценарієм порівняно з рівномірним розподілом.

- Латентність L_{f2b} не є недоліком конкретної утиліти Fail2ban, а є фундаментальною архітектурною вадою будь-якої системи захисту, що працює за принципом постфактум-аналізу подій. Навіть при мінімальній латентності 0.5 с (дослід 1, 50 потоків) атака виявилась успішною, що підтверджує структурний характер цієї вразливості.

Натомість, превентивний сценарій (Ed25519) повністю виключає стан S_1 з графа переходів, оскільки механізм перевірки криптографічного ключа інтегрований безпосередньо у процес встановлення з'єднання на рівні протоколу,

зводячи імовірність Race Condition до нуля. При $V_{auth} = 0$ вектор атаки Brute Force закривається на рівні протоколу SSH до будь-якого аналізу логів, що підтверджено експериментально: жодного запису «Failed password» у */var/log/auth.log* не зафіксовано.

4 РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ МОДЕЛІ ТА РЕКОМЕНДАЦІЇ ЩОДО БЕЗПАРОЛЬНОЇ АРХІТЕКТУРИ В КОРПОРАТИВНОМУ СЕРЕДОВИЩІ

4.1 Практичне застосування моделі: рекомендації щодо безпарольної архітектури в корпоративному середовищі

На основі розробленої інформаційної моделі оцінки залежності захисту комп'ютерних мереж від факторів вразливостей (Розділ 2) та її успішної верифікації на тестовому стенді (Розділ 3), сформульовано практичні рекомендації для побудови захищених корпоративних інфраструктур.

Головним висновком моделювання є те, що традиційний парольний захист, навіть підсилений реактивними компонентами типу Fail2ban, містить неусувний архітектурний ризик – часову латентність обробки подій L_{f2b} , що створює вікно вразливості для атак високої інтенсивності. Тому для побудови сучасних безпечних мереж рекомендується повний перехід на безпарольну архітектуру (Passwordless Architecture) за концепцією Zero Trust («Нульова довіра»).

Основними практичними кроками для впровадження безпарольної архітектури на рівні корпоративного середовища є:

1. Повна деактивація парольної автентифікації. У конфігураційних файлах SSH-демонів корпоративних серверів (`sshd_config`) необхідно директивно встановити параметри *PasswordAuthentication no*. Це примусово знижує коефіцієнт вразливості автентифікації V_{auth} до 0.

2. Перехід на асиметричні криптографічні ключі. Замість застарілих алгоритмів RSA рекомендовано стандартне використання сучасних еліптичних кривих, зокрема алгоритму Ed25519. Потужність його ключового простору ($|K| = 2^{256}$) робить математично неможливим успішний brute-force або dictionary-атаку в межах існуючого технологічного укладу.

3. Реалізувати централізоване управління ключами.

4.2 Аналіз ризиків і переваг Open Source рішень у світлі отриманих результатів

Розгортання ключової автентифікації Ed25519 не потребує довіри до клієнтського вузла – приватний ключ залишається на клієнті, публічний розміщується на сервері, що повністю відповідає принципу мінімальних привілеїв та архітектурі Zero Trust [16]. Те що клієнтом виступає Kali – свідоме рішення: показати що та сама машина яка атакувала паролем не може атакувати при ключовій автентифікації. Використання Open Source рішень (таких як OpenSSH, Fail2ban, Kali Linux) у ході дослідження дозволило детально проаналізувати їхній безпековий баланс.

Переваги Open Source рішень:

- Відповідність концепції Zero Trust. Розгортання ключової автентифікації Ed25519 не потребує надлишкової довіри до клієнтського вузла або стороннього інструменту. Приватний ключ генерується та залишається виключно на стороні клієнта, а на сервері розміщується лише публічний ідентифікатор. Це повністю відповідає принципу мінімальних привілеїв [16].
- Відкритий вихідний код криптографічних бібліотек гарантує відсутність недекларованих можливостей (backdoors), що є критичним для корпоративних систем захисту інформації.
- Можливість адаптації конфігурації під специфічні критерії інтенсивності трафіку.

4.3 Організаційно-економічна ефективність запропонованих заходів

Економічна доцільність переходу на безпарольну архітектуру обґрунтовується результатами проведеного дослідження через порівняння витрат на впровадження превентивного захисту та потенційних збитків від успішної компрометації системи.

Результати верифікації інформаційної моделі (розділ 3.6) кількісно підтвердили, що реактивний захист на основі Fail2ban має структурну ймовірність компрометації $P(S_2) = 35.7\%$ при словниковій атаці з інтенсивністю $\lambda \approx 47$ спроб/с. Це означає, що при кожній третій подібній атаці система з парольною автентифікацією буде скомпрометована навіть за наявності активного засобу захисту. З точки зору методології FAIR (Factor Analysis of Information Risk), така ймовірність є неприйнятно високою для корпоративного середовища, де SSH-доступ надається до серверів з критичними даними.

Натомість превентивний підхід на основі ключової пари Ed25519 забезпечує $P(S_3) = 0\%$ при нульових витратах на ліцензування, оскільки OpenSSH є відкритим програмним забезпеченням, що входить до стандартного складу будь-якого дистрибутиву Linux. Впровадження ключової автентифікації зводиться до одноразового виконання команд генерації ключа та модифікації конфігураційного файлу *sshd_config*, що не потребує залучення додаткових фінансових ресурсів.

Важливим організаційним аспектом є те, що реактивний захист вимагає постійного адміністративного супроводу: моніторингу списків заблокованих IP-адрес, коригування параметрів *maxretry* та *findtime* відповідно до динаміки атак, а також реагування на випадки хибного блокування легітимних користувачів. Превентивна архітектура на основі Ed25519 після одноразового розгортання не потребує регулярного втручання адміністратора, що суттєво знижує операційні витрати на підтримку системи захисту.

Розроблена інформаційна модель дозволяє кількісно обґрунтувати перед керівництвом організації необхідність переходу на безпарольну архітектуру, надаючи конкретне числове значення ймовірності компрометації при збереженні поточної конфігурації захисту, що є основою для прийняття обґрунтованих управлінських рішень щодо інвестицій у кібербезпеку.

4.4 Напрямки подальших досліджень: розширення моделі, нові фактори вразливостей, автоматизація оцінки

Проведене дослідження та верифікована інформаційна модель формують основу для низки перспективних напрямків подальшої наукової та практичної роботи.

Розширення моделі на розподілені атаки. Розроблена модель коректна для одиночного джерела атаки з однією IP-адресою, що є обмеженням, зазначеним у розділі 2.3. Реальні атаки на корпоративні мережі часто здійснюються через ботнети з тисячами розподілених вузлів, де кожен вузол надсилає лише кілька запитів – недостатньо для спрацювання Fail2ban за стандартними налаштуваннями ($\text{maxretry} = 3$). Перспективним напрямком є розширення вектору стану системи S додатковим параметром кількості атакуючих вузлів та розробка агрегованої функції ймовірності компрометації для розподіленого сценарію. Марківська модель станів $\{S_0, S_1, S_2, S_3\}$, запропонована у розділі 2.1, може бути адаптована для опису паралельних ланцюгів переходів від кожного вузла ботнету.

Врахування нестандартних портів як фактору вразливості. У поточній моделі параметр V_{port} є бінарним: стандартний порт TCP/22 або нестандартний. Однак зміна порту є лише засобом зниження видимості сервісу, а не реальним захистом. Перспективним є кількісне дослідження залежності інтенсивності атаки λ від номеру порту – зокрема, наскільки використання нестандартного порту реально знижує λ у часовому вимірі, та інтеграція цього параметру у функцію моделі (3.1) як коефіцієнта зниження інтенсивності атаки.

Автоматизація оцінки захищеності. Розроблена математична модель (формула 3.1) є аналітично замкненою та допускає автоматизовану реалізацію у вигляді програмного інструменту. Перспективним є розробка скрипту або веб-застосунку, який автоматично зчитує параметри з конфігураційних файлів *sshd_config* та *jail.local*, аналізує */var/log/auth.log* для визначення реальної інтенсивності атак λ та обчислює поточне значення $P(S)$ у реальному часі. Такий інструмент міг би інтегруватись із системами SIEM для автоматичного сповіщення

адміністратора при перевищенні граничного значення ймовірності компрометації.

Розширення моделі на інші протоколи віддаленого доступу. Поточна верифікація проведена виключно для протоколу SSH. Концептуальна структура моделі – вектор стану S , поняття вікна вразливості L_{f2b} та формула (3.1) – є універсальною і може бути застосована до інших протоколів автентифікації, зокрема RDP (Remote Desktop Protocol), FTP та веб-застосунків з парольною автентифікацією. Порівняльне дослідження латентності реактивних засобів захисту для різних протоколів дозволить узагальнити модель та підтвердити її універсальність.

ВИСНОВКИ

У кваліфікаційній роботі вирішено науково-практичне завдання розробки інформаційної моделі оцінки залежності захисту комп'ютерних мереж від впливу факторів вразливостей. Отримані результати дозволяють сформулювати такі висновки.

1. Проведено аналіз нормативної бази та існуючих підходів до оцінки вразливостей.

Встановлено що чинна законодавча база України у сфері кібербезпеки – зокрема Закон України «Про основні засади забезпечення кібербезпеки України» (зі змінами 2025 року), Постанова КМУ № 518 та стандарти серії НД ТЗІ 2.5 – визначає загальні вимоги до захисту інформаційно-комунікаційних систем, однак не містить інструментарію для кількісного оцінювання динамічної залежності між параметрами атаки та рівнем захисту. Міжнародні стандарти ISO/IEC 27001, ISO/IEC 27002:2022 та NIST CSF 2.0 встановлюють вимоги до систем управління інформаційною безпекою і визначають необхідність впровадження стійких методів автентифікації, проте також не забезпечують конкретного математичного апарату для оцінки ефективності реактивних засобів захисту в умовах активної атаки. Система CVSS надає числову оцінку критичності вразливостей, але оцінює їх як окремі статичні сутності, не враховуючи динаміку взаємодії між інтенсивністю атаки та часом реакції захисної системи. Це підтверджує існування суттєвої прогалини між наявними методиками та практичними потребами кількісного оцінювання захищеності.

У роботі визначено вектор стану системи $S = \langle V_{port}, V_{auth}, L_{f2b}, E_{str}, \lambda \rangle$, що охоплює п'ять ключових факторів вразливості: ознаку використання стандартного порту SSH, тип механізму автентифікації, латентність реактивного засобу захисту Fail2ban, ентропію автентифікаційних даних та інтенсивність атаки. Встановлено що протокол SSH на стандартному порту TCP/22 є оптимальним об'єктом дослідження через масовість використання у корпоративних середовищах, наявність детальних лог-файлів для точного вимірювання часових

параметрів та доступність верифікованих інструментів для обох сторін – OpenSSH з боку захисту та Hydra з боку атаки. Згідно з класифікацією MITRE ATT&CK техніка T1110 (Brute Force) є одним з найпоширеніших векторів початкового доступу.

2. Розроблена інформаційна модель формалізує залежність ймовірності компрометації $P(S)$ від параметрів вектору стану системи через основну функцію моделі (формула 3.1). Модель інтегрує апарат теорії ймовірностей для оцінки ентропії ключового простору, теорії черг для моделювання потоку запитів злоумисника як пуасонівського процесу з інтенсивністю λ , та Марківських процесів для формального опису динаміки зміни стану захищеності системи через множину станів $S = \{S0, S1, S2, S3\}$. Центральним поняттям моделі є «вікно вразливості» L_{f2b} – часовий інтервал між першою спробою несанкціонованого доступу та моментом блокування атакуючої IP-адреси реактивною системою захисту, що обчислюється за формулою (2.7). Кількість спроб автентифікації у вікні вразливості визначається як $N_{window} = \lambda \cdot L_{f2b}$ (формула 2.6), що є прямим входом для розрахунку ймовірності компрометації. Модель також дозволяє оцінювати відповідність конфігурації захисту вимогам функціонального класу FIA_UAU стандарту ISO/IEC 15408-2 щодо стійкості механізму автентифікації. Експериментальні дослідження, проведені у третьому розділі, підтверджують високу критичність атак типу Brute-force на протокол віддаленого керування SSH. Відповідно до аналітичних звітів CERT-UA, компрометація автентифікаційних даних через цей вектор залишається одним із найбільш масових та статистично значущих методів первинного проникнення злоумисників до корпоративних та державних ІКС України.

3. Верифікацію проведено на ізольованому тестовому стенді у середовищі Oracle VM VirtualBox 7.2.6, що включав цільовий вузол Ubuntu Server (192.168.56.10) з OpenSSH та Fail2ban і атакуючий вузол Kali Linux (192.168.56.20) з інструментом Hydra 9.5, об'єднані в ізольовану мережу Internal Network «DiplomNet».

Базовий сценарій (без засобів захисту) підтвердив що за відсутності активного захисту словниковий пароль "admin" ($E_{str} = 23.5$ біт) підбирається за 1.26 секунди при інтенсивності атаки $\lambda \approx 8.72$ спроб/с та кількості спроб $N_{window} = 13$. Ймовірність компрометації $P(S) = 1$, що відповідає теоретичному прогнозу моделі при $L_{f2b} \rightarrow \infty$.

Реактивний сценарій (Fail2ban увімкнений, $maxretry = 3$, $findtime = 600$ с) виявив ключовий феномен вікна вразливості: при інтенсивності атаки $\lambda \approx 47$ спроб/с латентність захисту становила $L_{f2b} \approx 1.0$ с, що дало $N_{window} = 47$ спроб до моменту блокування. Незважаючи на те що Fail2ban успішно заблокував атакуючу IP-адресу (Total banned: 1), пароль було підібрано ще до спрацювання блокування – $P(S)$ факт. = 1. Це експериментально підтверджує центральну гіпотезу роботи: реактивний захист має структурний недолік у вигляді вікна вразливості, розмір якого лінійно залежить від інтенсивності атаки. Теоретична ймовірність компрометації за рівномірного розподілу по ключовому простору словника ($|K| = 106$) становить $P(S_2) \approx 35.7\%$, однак словниковий характер атаки зводить практичну ймовірність до 1 – що вказує на принципову різницю між математичною ентропією пароля та його реальною стійкістю до словникових атак.

Превентивний сценарій (ключова пара Ed25519, парольна автентифікація вимкнена) підтвердив що при $V_{auth} = 0$ вектор атаки Brute Force повністю закривається на рівні протоколу SSH до будь-якого аналізу логів. Ентропія приватного ключа Ed25519 становить $E_{str} = 256$ біт, що дає $|K| = 2^{256} \approx 1.16 \cdot 10^{77}$ – математичне очікування успішного підбору дорівнює нулю при будь-якій реально досяжній інтенсивності атаки. $P(S) = 0$ підтверджено експериментально: жодної успішної автентифікації з боку атакуючого вузла не зафіксовано.

4. На основі отриманих результатів сформульовано практичні рекомендації щодо побудови захищених корпоративних інфраструктур. Обґрунтовано необхідність повного переходу на безпарольну архітектуру (Passwordless Architecture) за концепцією Zero Trust та використання асиметричних криптографічних ключів (зокрема Ed25519). Доведено організаційно-економічну ефективність такого підходу, оскільки превентивний захист на базі Open Source рішень

знижує ймовірність компрометації до нуля без додаткових витрат на ліцензування. Також визначено перспективні напрямки подальших досліджень, серед яких розширення моделі на розподілені атаки (ботнети), врахування нестандартних портів та розробка програмного інструменту для автоматизованої оцінки захищеності в реальному часі.

ПЕРЕЛІК ПОСИЛАНЬ

1. Статистика, тренди та факти про антивіруси та кібербезпеку до 2024 року. URL: <https://mediacom.com.ua/statistika-trendi-ta-fakti-pro-antivirusi-ta-kiberbezpeku-do-2024-roku/> (дата звернення: 29.05.2026).
2. Кібератаки на критичну інфраструктуру: кейси і рекомендації з досвіду впровадження захисту – AM Integrator Group. URL: <https://amintegrator.com/en/kiberataky-na-krytychnu-infrastrukturu-kejsy-i-rekomendacziyi-z-dosvidu-vprovadzhennya-zahystu/> (дата звернення: 29.05.2026).
3. Татохіна О. Кібервійна Росії проти України: Держспецзв'язку презентувала звіт про три роки атак і глобальні виклики. URL: <https://detector.media/infospace/article/241232/2025-05-26-kiberviyna-rosii-proty-ukrainy-derzhspetsvvyazku-prezentovala-zvit-pro-try-roky-atak-i-globalni-vyklyky/> (дата звернення: 29.05.2026).
4. Статистичний звіт за результатами роботи Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки в 2023 році. scpc.gov.ua. URL: <https://scpc.gov.ua/uk/articles/334> (дата звернення: 29.05.2026).
5. Найпоширеніші кіберзагрози у 2023 році та прогнози на 2024. URL: <https://megatrade.ua/news/reviews/nayposhirenishi-kiberzagrozi-u-2023-rotsi-ta-prognozi-na-2024> (дата звернення: 29.05.2026).
6. Для чого потрібна база даних CVE (Common Vulnerabilities and Exposures)?. URL: <https://tseivo.com/b/memecode/t/xzxb9xrq0g/dlia-choho-potribna-baza-danykh-cve-common-vulnerabilities-and-exposures> (дата звернення: 29.05.2026).
7. CVSS v3.1 Specification Document. FIRST – Forum of Incident Response and Security Teams. URL: <https://www.first.org/cvss/v3.1/specification-document> (дата звернення: 29.05.2026).
8. Korniyenko B., Galata L. IRISK METHOD FOR SECURITY ESTIMATION OF THE SIMULATION POLYGON FOR THE PROTECTION OF CRITICAL

INFORMATION RESOURCES. Visnyk Universytetu “Ukraina”. 2019. URL: <https://doi.org/10.36994/2707-4110-2019-2-23-27> (дата звернення: 29.05.2026).

9. ПІДХІД ДО ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ КЛАСУ «1» | Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». URL: <https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/224> (дата звернення: 29.05.2026).

10. Річний аналітичний огляд кіберпростору: жовтень 2023 — вересень 2024 / Рада національної безпеки і оборони України. URL: https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/20250109/Year%20in%20review_UKR_upd.pdf (дата звернення: 29.05.2026).

11. CVE: Common Vulnerabilities and Exposures. URL: <https://cve.mitre.org> (дата звернення: 29.05.2026).

12. National Vulnerability Database. URL: <https://nvd.nist.gov> (дата звернення: 29.05.2026).

13. Прогнози кібербезпеки на 2024 рік. URL: <https://corewin.ua/news/cybersecurity-forecasts-2024/> (дата звернення: 29.05.2026).

14. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. – К., 2024.– №5 (травень) . – 316 с.

15. Що сталося з NVD: проблематика, наслідки, рішення? URL: <https://corewin.ua/blog/what-do-you-need-to-know-about-nvd-violations-causes-consequences-solutions/> (дата звернення: 29.05.2026).

16. Zero Trust Architecture : NIST Special Publication 800-207 / S. Rose, O. Borchert, S. Mitchell, S. Connelly. – National Institute of Standards and Technology, 2020. – 53 p. URL: <https://csrc.nist.gov/publications/detail/sp/800-207/final> (дата звернення: 29.05.2026).

17. Міщенко М. В. Інформаційна технологія виявлення та прогнозування загроз для корпоративних комп'ютерних мереж : дис. ... канд. техн. наук. — Чернівці : ЧНТУ, 2025. URL: https://stu.cn.ua/wp-content/uploads/2025/02/dysertacziya_mishhenkom.v. final.pdf

18. В CERT-UA підготували аналітичний звіт «Російські кібероперації» H2'2024: кількість кіберінцидентів зросла на 48%. URL: <https://cybersec.net.ua/statti/868-v-cert-ua-pidhotuvaly-analitychnyi-zvit-rosiiski-kiberoperatsii-h22024-kilkist-kiberintsydentiv-zroslo-na-48protsent.html> (дата звернення: 29.05.2026).

19. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення: 29.05.2026).

20. Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 05.07.1994 № 80/94-ВР. URL: <https://zakon.rada.gov.ua/laws/show/80/94-вр> (дата звернення: 29.05.2026).

21. Detection of SSH Brute-Force Attacks Using Machine Learning. URL: <https://www.diva-portal.org/smash/get/diva2:1981478/FULLTEXT01.pdf>

22. T. Ylonen and C. Lonvick, “The secure shell (ssh) protocol architecture.” URL: <https://www.rfc-editor.org/rfc/rfc4251>, 2006. RFC 4251. (дата звернення: 29.05.2026).

23. T. Ylonen, P. Turner, K. Scarfone, and M. Souppaya, “Security of interactive and automated access management using secure shell (ssh),” Tech. Rep. NISTIR 7966, National Institute of Standards and Technology, 2015.

24. Аналітичний звіт про стан виконання Плану реалізації Стратегії кібербезпеки України за 2025 рік. URL: <https://docs.google.com/viewer?url=https://cip.gov.ua/services/cm/api/attachment/download?id=73801&embedded=true&a=bi> (дата звернення: 29.05.2026).

25. План реалізації Стратегії кібербезпеки України : затверджено Указом Президента України від 01.02.2022 р. No 37/2022. URL: <https://zakon.rada.gov.ua/laws/show/n0087525-21> (дата звернення: 29.05.2026).

26. Захист інформації в комп'ютерних системах та мережах. Частина II: підручник / Ю.В. Костюк, П.М. Складанний. – Київ : Київський столичний університет імені Бориса Грінченка, 2026. – 386 с.

27. ТОП-платформи ШІ для кібербезпеки 2026: Огляд рішень від Microsoft, Google, та CrowdStrike. URL: <https://nt.ua/top-ai-platforms-for-cybersecurity-in-2026> (дата звернення: 29.05.2026).

28. Stop Counting Vulnerabilities. Start Proving Risk. URL: <https://www.forbes.com/councils/forbestechcouncil/2026/06/01/stop-counting-vulnerabilities-start-proving-risk> (дата звернення: 03.06.2026).

29. ISO/IEC 15408-2:2022. Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components.

30. Fail2Ban: ban hosts that cause multiple authentication errors. URL: <https://github.com/fail2ban/fail2ban> (дата звернення: 30.05.2026).

31. RFC 8709: Ed25519 and Ed448 Public Key Algorithms for the Secure Shell (SSH) Protocol. URL: <https://datatracker.ietf.org/doc/html/rfc8709> (дата звернення: 30.05.2026).

32. About Oracle VirtualBox URL: <https://www.virtualbox.org/manual/UserManual.html> (дата звернення: 30.05.2026)

33. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) // Official Journal of the European Union. – 2022. – L 333. – P. 80-152. – URL: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj> (дата звернення: 29.05.2026).

34. Теорія ймовірностей та математична статистика: навчальний посібник / О. І. Огірко, Н. В. Галайко. – Львів: ЛьвДУВС, 2017. – 292 с

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

36. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2 : НД ТЗІ 2.5-008-2002 Київ : ДСТСЗІ СБУ, 2002.

37. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги : ДСТУ ISO/IEC 27001:2015 (ISO/IEC 27001:2013; Cor 1:2014, IDT). – [Чинний від 2016-07-01]. – Київ : ДП «УкрНДНЦ», 2016. – 33 с.

38. Information security, cybersecurity and privacy protection — Information security controls : ISO/IEC 27002:2022. – 3rd ed. – Geneva : International Organization for Standardization, 2022. – 152 p.

39. MITRE ATT&CK®. MITRE ATT&CK®. URL: <https://attack.mitre.org/> (дата звернення: 30.05.2026).

40. Теорія систем масового обслуговування : навч. посібник / А. Л. Литвинів ; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. – Харків : ХНУМГ ім. О. М. Бекетова, 2018. – 141 с.

41. THC-Hydra: A very fast and flexible online password cracking tool. URL: <https://github.com/vanhauser-thc/thc-hydra> (дата звернення: 29.05.2026).

42. «Теорія інформації та обробка сигналів-1»: конспект лекцій [Електронний ресурс]: навч. посіб. для студ. спеціальності 171 «Електроніка», освітньої програми «Електронні компоненти і системи» / КПІ ім. Ігоря Сікорського ; уклад.: Ю.С. Ямненко, К. С. Клен. – Електронні текстові данні (1 файл: 2,107 Мбайт). – Київ: КПІ ім. Ігоря Сікорського, 2019. – 120 с.

43. Захист інформації в комп'ютерних системах : підручник для студентів спеціальності 123 «Комп'ютерна інженерія» / уклад.: О. М. Гапак, С. І. Балога. Ужгород : ДВНЗ «УжНУ», 2021. 184 с.

password

root

1234

12345

qwerty

test

letmein

pass

admin

123456

145785

asetvi

123

ДОДАТОК Б

123456
password
123456789
12345678
12345
111111
1234567
sunshine
qwerty
iloveyou
princess
welcome
666666
abc123
football
123123
monkey
654321
!@#%&^*
charlie
donald
password1
qwerty123
shadow
master
123321
dragon
pass
test
1234
soccer
hockey
killer
george
andrew
jordan
harley
ranger
daniel
hello
whatever
joshua
superman

samuel
jessica
tigger
batman
hockey1
michael
robert
admin
access
121212
000000
654321
passw0rd
baseball
basketball
letmein
mustang
1234567890
qwertyuiop
987654321
zxcvbnm
asdfghjkl
superman1
batman1
pokemon
nintendo
cheese
computer
internet
starwars
galaxy
matrix
thunder
winter
summer
spring
autumn
flower
money123
silver
golden
hunter
rabbit
turtle

cookie
coffee
orange
apple12
banana1
cherry1
lemon123
grape123
peach123
melon123
mango123
kiwi1234
pear1234
plum1234
lime1234
fig12345
date1234