УДК 004.056

**В. О. Паламарчук**
**О. В. Войтович**

# ПІДХІД ДО ПОБУДОВИ КІБЕРПОЛІГОНУ ДЛЯ ВИВЧЕННЯ DDOS-АТАК

Вінницький національний технічний університет

***Анотація***

*У статті досліджуються принципи побудови сучасних кіберполігонів. Розглянуто ключові інфраструктурні аспекти, включно з відтворюваністю конфігурацій, масштабованістю, ізоляцією, моніторингом та автоматизацією розгортання сценаріїв. Описані методи реалізації цих критеріїв із використанням контейнеризації, оркестрації, декларативного опису інфраструктури та систем управління конфігураціями, таких як Terraform, Ansible та Nix. Проаналізовано переваги підходів для гнучкого створення експериментальних сендбоксів та контролю складних сценаріїв атак.*

**Ключові слова:** кіберполігон, відтворюваність, декларативна інфраструктура, масштабованість, моніторинг, автоматизація, ddos-атаки.

***Abstract***

*This paper investigates the design principles of modern cyber ranges. Key infrastructural aspects are examined, including configuration reproducibility, scalability, isolation, monitoring, and automation of scenario deployment. Methods for implementing these criteria are described using containerization, orchestration, declarative infrastructure descriptions, and configuration management tools such as Terraform, Ansible, and Nix. The advantages of these approaches are analyzed for flexible creation of experimental sandboxes and controlled execution of complex attack scenarios.*

**Keywords:** cyber range, reproducibility, declarative infrastructure, scalability, monitoring, automation, ddos-attacks.

## Вступ

За останні кілька років питання кібербезпеки набули особливої актуальності у зв’язку зі зростанням кількості та складності кібератак, зокрема атак типу DDoS, що реалізуються із застосуванням бот-мереж [1]. Для дослідження таких загроз, перевірки ефективності засобів захисту та відпрацювання методів виявлення зловмисної активності дедалі частіше використовуються спеціалізовані кіберполігони. Вони забезпечують можливість контрольованого моделювання реалістичних сценаріїв атак у ізольованому середовищі без ризику для реальних інформаційних систем.

Незважаючи на активний розвиток технологій віртуалізації, контейнеризації та мережевої ізоляції, побудова кіберполігону залишається складним інженерним завданням [2]. Необхідно одночасно забезпечити безпеку експериментального середовища, його масштабованість, керованість та відтворюваність сценаріїв. Помилки на етапі проєктування інфраструктури можуть призвести до неконтрольованого поширення шкідливого трафіку, спотворення результатів експериментів або неможливості адекватного моніторингу поведінки бот-мереж.

Для побудови кіберполігонів застосовуються різні інфраструктурні підходи, зокрема на основі віртуальних машин, контейнерних технологій або їх гібридного поєднання. Кожен із цих підходів має свої переваги та обмеження з точки зору ізоляції, продуктивності, гнучкості налаштувань та складності керування.

Метою дослідження є аналіз інфраструктурних вимог і архітектурних підходів до побудови кіберполігону для контрольованої емуляції бот-мереж і проведення експериментальних досліджень DDoS-атак з метою обґрунтування раціонального способу його реалізації.

Обґрунтований вибір інфраструктурних рішень для кіберполігону є ключовим фактором достовірності експериментів і ефективності подальших досліджень у сфері виявлення та аналізу бот-мереж.

## Результати дослідження

У науковій літературі кіберполігони визначають як інтерактивні симульовані середовища, що відтворюють мережеві інфраструктури, системи та сервіси для тренувань у сфері кібербезпеки, тестування засобів захисту та оцінки реакції на реалістичні сценарії атак [3-10]. Вони забезпечують безпечне моделювання поведінки атакувальних і захисних агентів у контрольованих умовах, зменшуючи ризик впливу експериментів на продуктивні системи та критичну інфраструктуру. Водночас у сучасних дослідженнях дедалі частіше наголошується на необхідності розглядати кіберполігон не лише як набір заздалегідь визначених сценаріїв, а як універсальне експериментальне середовище, у межах якого можливі довільні зміни конфігурацій і поведінки компонентів [4].

Інфраструктура кіберполігону повинна передбачати комплексну ізоляцію середовища, що охоплює мережеві сегменти, домени зберігання даних, керування конфігураціями та системи спостереження. У практичних реалізаціях це досягається шляхом використання окремих віртуальних мереж, програмно-визначених мережевих політик, контрольованої маршрутизації та обмеження доступу до зовнішніх ресурсів. Для зберігання даних і журналів застосовуються відокремлені сховища, що дозволяє локалізувати наслідки експериментів і зберігати повний контроль над інформаційними потоками.

Ключовою вимогою до сучасного кіберполігону залишається відтворюваність і контроль стану середовища. Наукові роботи вказують, що відсутність чіткого механізму відновлення конфігурацій унеможливлює коректний аналіз результатів і порівняння експериментів. Для розв’язання цієї проблеми широко застосовуються декларативні підходи до опису інфраструктури, зокрема інструменти на кшталт Terraform, Nix або конфігураційні менеджери типу Ansible. Інтеграція з системами автоматизації розгортання, зокрема Jenkins чи іншими CI/CD-платформами, дозволяє фіксувати стани середовища та відновлювати їх у незмінному вигляді. Концепції на зразок impermanence додатково зменшують накопичення прихованого стану, що спрощує контроль змін у довготривалих експериментах.

Масштабованість і гнучкість інфраструктури розглядаються як критично важливі для моделювання складних розподілених атак, включно з бот-мережами. Реалізація цього критерію здійснюється через контейнеризацію, віртуалізацію та оркестраційні платформи, такі як Kubernetes або Docker Swarm, а також через автоматизоване керування ресурсами на рівні гіпервізора чи апаратних вузлів. Така організація дозволяє динамічно додавати або видаляти вузли, змінювати мережеві топології і конфігурації без перезавантаження або повного перебудовування середовища, забезпечуючи можливість відтворення сценаріїв різної складності та масштабності.

Моніторинг подій і телеметрія займають центральне місце у функціонуванні кіберполігону. Для цього застосовуються централізовані системи логування, такі як ELK Stack або Prometheus, а також спеціалізовані механізми кореляції подій і побудови аналітичних панелей. Завдяки інтеграції цих інструментів безпосередньо в середовище експериментів дослідник отримує можливість проводити детальний аналіз, виявляти аномалії і документувати критичні події.

Автоматизація розгортання сценаріїв і конфігурацій значно зменшує ручну роботу і підвищує керованість середовища. Використання скриптів, шаблонів і доменоспецифічних мов опису, а також інструментів управління конфігураціями (Terraform, Ansible, Nix) дозволяє швидко формувати нові експериментальні набори і змінювати конфігурації систем без обмежень, накладених жорстко визначеними сценаріями. У результаті кіберполігон перетворюється на універсальну пісочницю, де можливо максимально точно відтворювати попередні експерименти, а також виконувати довільні команди, досліджувати поведінку шкідливих компонентів і адаптувати середовище під нові експериментальні завдання, зберігаючи контроль і безпеку.

## Висновки

Для дослідження складних кіберзагроз, зокрема бот-мереж, кіберполігон доцільно розглядати як універсальне середовище, у якому можливі довільні експерименти без ризику втрати керованості. Ключовими характеристиками такого підходу є відтворюваність, декларативний опис інфраструктури та контроль стану середовища. Вони дозволяють багаторазово відновлювати ідентичні умови експериментів, мінімізувати вплив людського фактору та забезпечити достовірність результатів незалежно від складності та деструктивності досліджуваних сценаріїв.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ


1. Kampourakis V., Kavallieratos G., Spathoulas G., Gkioulos V., Katsikas S. LLM-Assisted AHP for Explainable Cyber Range Evaluation. Dec. 11, 2025. URL: https://arxiv.org/abs/2512.10487
2. Glas M., Hilmer C., Pernul G. Cyber Ranges: Five Use Cases for Improving Cybersecurity Skills Development in Organizations. IEEE Security & Privacy Magazine, May 2025. URL: https://doi.org/10.1109/MSEC.2025.3596735
3. Miller E., Mink D., Spellings P., Bagui S., Bagui S. Classifying Cyber Ranges: A Case-Based Analysis Using the UWF Cyber Range. Encyclopedia, Vol. 5, Iss. 4, 2025, p. 162. URL: https://doi.org/10.3390/encyclopedia5040162
4. European Cyber Security Organisation (ECSO). Understanding Cyber Ranges: From Hype to Reality. ECSO Whitepaper, Nov. 5, 2025. URL: https://academy.cybersuiteproject.eu/repository/understanding-cyber-ranges-from-hype-to-reality/
5. EdTech Magazine. Cyber Ranges Prepare Students for Cybersecurity Careers. Aug. 2025. URL: https://edtechmagazine.com/higher/article/2025/08/cyber-ranges-prepare-students-cybersecurity-careers
6. Global Growth Insights. Cyber Range For Education Market Size | Industry Trends 2025–2033. 2025. URL: https://www.globalgrowthinsights.com/market-reports/cyber-range-for-education-market-113323
7. Business Research Insights. Cyber Range Platform Market Trend, Size & Share | CAGR of 8%. 2025. URL: https://www.businessresearchinsights.com/market-reports/cyber-range-platform-market-113157
8. ECSO Cyber Range Features Checklist, List of European Providers (2025 edition). European Cyber Security Organisation, 2025. URL: https://ecs-org.eu/activities/cyber-range-features-checklist-list-of-european-providers
9. A Study on the Multi-Cyber Range Application of Mission-Based Cybersecurity Testing and Evaluation in Association with the Risk Management Framework. Information, Vol. 15, Iss. 1, Dec. 28, 2023. URL: https://doi.org/10.3390/info15010018
10. Lillemets P., Jawad N. B., Kashi J., Sabah A., Dragoni N. A Systematic Review of Cyber Range Taxonomies: Trends, Gaps, and a Proposed Taxonomy. Future Internet, Vol. 17, Iss. 6, 2025. URL: https://doi.org/10.3390/fi17060259



***Паламарчук Владислав Олегович*** — студент групи 1БС-24м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, email: vladpalamarchuk2003@gmail.com

***Войтович Олеся Петрівна*** — к. т. н., доцент, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail: voytovych.olesya@vntu.edu.ua

***Vladyslav Palamarchuk*** — a student of the 1BS-24m group, Faculty of Information Technologies, Vinnytsia National Technical University, Vinnytsia, email: vladpalamarchuk2003@gmail.com.

***Olesya Voytovych*** — associate professor at the Department of Information Security, Vinnytsia National Technical University, Vinnytsia, email: voytovych.olesya@vntu.edu.ua