Отримані результати показали, що запропонований підхід дозволяє автоматизувати значну частину первинного аналізу інцидентів інформаційної безпеки. Інтеграція Threat Intelligence та AI-моделі забезпечує швидке оцінювання ризику та скорочує час реагування на інциденти. Крім того, використання SOAR-підходу дозволяє знизити навантаження на SOC-аналітиків та підвищити ефективність процесів моніторингу безпеки.

Таким чином, результати дослідження підтверджують доцільність використання штучного інтелекту та SOAR-платформ для автоматизації виявлення та пріоритезації інцидентів інформаційної безпеки. Подальші дослідження можуть бути спрямовані на інтеграцію додаткових джерел Threat Intelligence, удосконалення моделей оцінювання ризику та розширення автоматизованих механізмів реагування.

1. SANS Institute. AI-Driven SecOps: Unifying Controls, Automating Response, and Advancing the Modern SOC Using Cortex XSIAM. 2025. URL: https://www.sans.org/white-papers/ai-driven-secops-unifying-controls-automating-response-advancing-modern-soc-using-cortex-xsiam.
2. VirusTotal. API Overview. URL: https://docs.virustotal.com/reference/overview.
3. Anthropic. Anthropic Claude Documentation. URL: https://platform.claude.com/docs/en/home.
4. Umesh Bartwal, Subhasis Mukhopadhyay, Rohit Negi, Shashank Shukla. Security Orchestration, Automation, and Response Engine for Deployment of Behavioural Honeypots. 2022. URL: https://doi.org/10.1109/DSC54232.2022.9888808.
5. Jay Roy, Sandeep Singh. AgentSOC: A Multi-Layer Agentic AI Framework for Security Operations Automation. 2026. URL: https://doi.org/10.1109/ICAIC67076.2026.11395783.

Методологія забезпечення мережевої ізоляції та динамічного масштабування ресурсів у середовищі змагального кіберполігону

УДК 004.056:378.147

Богдан Маліцький[1], Михайло Євдокімов[2], Данило Куташ[3], Василь Різак[4]

Ужгородський національний університет,
[1]bohdan.malitskyi@uzhnu.edu.ua, [2]mykhailo.yevdokimov@uzhnu.edu.ua,
[3]danylo.kutash@student.uzhnu.edu.ua, [4]vrizak@uzhnu.edu.ua

Проведення CTF-чемпіонату регіонального масштабу ставить низку технічних вимог до інфраструктури: ізоляція вразливих сервісів від основної мережі закладу освіти, контрольований віддалений доступ для учасників з різних міст, можливість швидко повертати середовище у вихідний стан між раундами та одночасна робота з десятками учасників. Виконати ці вимоги на базі діючого навчального кіберполігону можливо лише за умови комплексної адаптації його архітектури – на рівні платформи віртуалізації, мережі, доступу та змагальної системи. Метою роботи є розробка та впровадження методології,

що забезпечує мережеву ізоляцію та динамічне масштабування ресурсів кіберполігону, на базі кафедри твердотільної електроніки та інформаційної безпеки Ужгородського національного університету для проведення першого чемпіонату Закарпатської області з кібербезпеки (CTF-змагань) ТЕІВ-2026.

Архітектуру кіберполігону адаптовано за чотирма напрямками. На рівні віртуалізації виконано перехід на серверний гіпервізор Proxmox VE, який підтримує одночасну роботу з віртуальними машинами і контейнерами та керується з єдиного інтерфейсу; цей перехід продиктований необхідністю обслуговувати багатьох учасників одночасно та швидко повертати середовища у вихідний стан через знімки. Базова апаратна конфігурація серверного вузла включає 12 ядер CPU, 64 ГБ RAM та 1 ТБ сховища; під час змагань на ньому одночасно функціонували 14 віртуальних машин. На рівні платформи розгорнуто змагальну систему CTFd, як окрему віртуальну машину з декількома контейнеризованими сервісами, відокремленими від основного трафіку через reverse proxy. На рівні мережі до існуючих навчальних сегментів додано окремі домени для роботи учасників і для розміщення вразливих сервісів, ізольовані firewall-правилами. На рівні доступу впроваджено VPN-підключення з автентифікацією за сертифікатами (OpenVPN), що дозволяє відключати конкретного учасника без впливу на інших.

В межах адаптованої інфраструктури підготовлено 69 практичних завдань у семи категоріях; статичні артефакти (forensic-образи, мережевий трафік, криптографічні артефакти) розміщено централізовано на змагальній платформі, а інтерактивні завдання – у персональних ізольованих середовищах із поверненням до вихідного стану між раундами. Експлуатація під час змагання: 24 години безперервної роботи, до 58 одночасних VPN-підключень, 7 811 спроб розв'язання завдань – без зафіксованих збоїв. Спостереження за телеметрією під час пікової фази зафіксували завантаження процесора до 50 % та використання оперативної пам'яті близько 90 % (рис. 1). Передзмагальне навантажувальне тестування (Load, Stress та Endurance Testing загальною тривалістю понад 78 годин) із застосуванням Apache Bench, iperf3, stress-ng, hping3, siege та Nmap визначило верхню межу стабільної роботи стенду: 850 одночасних HTTP-з'єднань, до 1,8 Гбіт/с внутрішнього трафіку, 14 000 подій журналювання за хвилину при деградації продуктивності в межах 4–6 % після стрес-фази.

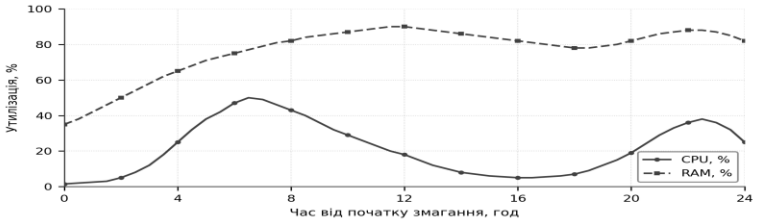

Рис.1. Динаміка утилізації CPU та RAM серверного вузла протягом 24 годин змагання

Запропонована методологія належить до класу локальних навчально-змагальних кіберполігонів і концептуально близька до інших академічних

рішень: автономної контейнерної платформи UNIWA на основі OpenStack та Docker [1] та платформи EMP для bootcamp-формату на 6–11 віртуальних машинах [2]. Відмінність полягає у комбінованому використанні віртуальних машин і контейнерів на базі гіпервізора рівня закладу освіти (Proxmox VE) замість хмарних платформ, що знижує бар'єри впровадження для регіональних університетів [3].

Результати апробації підтверджують працездатність запропонованої методології. Контейнеризація CTFd-сервісів і сегментація мережі firewall-правилами забезпечили повну ізоляцію вразливих сервісів від штатних навчальних середовищ протягом 24 годин роботи. Механізм знімків Proxmox VE дозволив швидко повертати середовища у вихідний стан між раундами без впливу на сусідні команди. Фактичне навантаження під час змагання (CPU до 50 %, RAM близько 90 %) залишилося нижчим за граничні показники стенду (850 одночасних HTTP-з'єднань, 1,8 Гбіт/с трафіку), що свідчить про наявний запас потужності. Розроблена методологія придатна для проведення CTF-змагань регіонального масштабу на базі кіберполігонів закладів освіти з open-source стеком віртуалізації.

1. Chouliaras N., Kantzavelou I., Maglaras L., Pantziou G., Ferrag M. A. A novel autonomous container-based platform for cybersecurity training and research. PeerJ Computer Science. 2023. Vol. 9. Article e1574. DOI: 10.7717/peerj-cs.1574.
2. Arnold D., Ford J., Saniie J. Architecture of an Efficient Environment Management Platform for Experiential Cybersecurity Education. Information. 2025. Vol. 16, No. 7. Article 604. DOI: 10.3390/info16070604.
3. Schafeitel-Tähtinen T., Lazarov W. Teaching and Learning Cybersecurity Using Capture the Flag: Effectiveness Comparison Between University Students in Finland and Czechia. Computer Applications in Engineering Education. 2025. Vol. 33, No. 5. Article e70082. DOI: 10.1002/cae.70082.

Privacy and information security in social media

UDK 004.056.5:004.738.5

Andrii Manko[1], Zhanna Babiak[2]

Ternopil Ivan Puluj National Technical University,
[1]andreymanko4@gmail.com, [2]b.janna73@gmail.com

Social media have become the primary channel for interpersonal and mass communication: according to DataReportal estimates, in 2025 they were actively used by more than 5.2 billion people — about 64 % of the world population. Modern platforms accumulate unprecedented volumes of personal data: contacts, geolocations, biometric templates (face and voice recognition), interaction history, behavioural patterns and psychometric profiles. The combination of these data with artificial intelligence tools, in particular AI-based open-data aggregation and generative models (deepfake), creates qualitatively new risks to the privacy and information security of users, organisations and the state as a whole [1, 2].