Аналіз підходів до впровадження кіберполігонів у підготовці фахівців з кіберзахисту

Максим Делембовський[1], Сергій Гнатюк[2], Борис Корнійчук[3]

[1]Київський національний університет будівництва і архітектури,
пр-т Повітряних Сил, 31, м.Київ, Україна, 03037,
[2]Державний університет «Київський авіаційний інститут»,
просп, Гузара Любомира 1, м.Київ, Україна, 03058,
[1]delembovskyi.mm@knuba.edu.ua, orcid.org/0000-0002-6543-0701,
[2]serhii.hnatiuk@npp.nau.edu.ua, orcid.org/ 0000-0003-4992-0564,
[3]korniichuk.bv@knuba.edu.ua, orcid.org/0000-0003-3881-1581

Received 17.09.2025, accepted 24.10.2025
https://doi.org/10.32347/st.2025.4.1201

Анотація. У представленій статті здійснено всебічний аналіз сучасних стратегій застосування кіберполігонів (Cyber Ranges) як інтелектуальних платформ для розвитку професійних компетенцій у сфері кібербезпеки. Дослідження охоплює еволюцію від статичних віртуальних лабораторій до динамічних екосистем, що базуються на хмарних технологіях та цифрових двійниках реальних інфраструктур. Особлива увага приділена інтеграції передових педагогічних концепцій, таких як таксономія Блума та цикл Колба, із галузевими стандартами фреймворку NICE. У роботі детально розглянуто роль автоматизації через агентні системи Retrieval-Augmented Generation (ARCeR) та багатоагентне навчання з підкріпленням (MARL), що дозволяє створювати адаптивні сценарії навчання. Результати дослідження підкреслюють важливість використання багатомодальної аналітики, включаючи біометричний моніторинг стресу, для об'єктивної оцінки готовності фахівців до дій у кризових ситуаціях..

Ключові слова: Кіберполігони, кіберзахист, фреймворк NICE, таксономія Блума, агентні системи RAG, багатоагентне навчання з підкріпленням, цифрові двійники, ситуаційна обізнаність, автоматизація сценаріїв.

Максим Делембовський
Зав. кафедри кібербезпеки та комп'ютерної інженерії
к.т.н., доц.

Сергій Гнатюк
проректор Державного університету «Київський авіаційний інститут»
д.т.н., проф.

Борис Корнійчук
доцент кафедри професійної освіти
к.т.н., доц.

ВСТУП

Стрімка цифровізація суспільства та інтеграція штучного інтелекту в повсякденні бізнес-процеси призвели до розширення поверхні кіберзагроз до глобальних масштабів. Станом на 2024–2025 роки світова економіка зазнає збитків від кіберзлочинності, що перевищують 9,5 трильйона доларів США щороку. При цьому глобальний дефіцит кваліфікованих кадрів у сфері кібербезпеки сягає близько 4 мільйонів працівників. Традиційні академічні методи, що базуються переважно на теоретичних лекціях, демонструють свою неспроможність підготувати персонал до протидії сучасним поліморфним атакам.

Кіберполігони вирішують цю проблему, надаючи ізольовані, високонадійні віртуальні середовища для практичного відпрацювання навичок виявлення та реагування на інциденти. Сучасні платформи стають критично важливими інструментами, які дозволяють фахівцям отримувати «бойовий» досвід без ризику для реальних систем організації.

ОСНОВНІ ПОЛОЖЕННЯ

1. Архітектурні моделі та технологічна база кіберполігонів

Ефективність кіберполігона як навчального інструмента визначається тим, наскільки переконливо середовище відтворює реальні умови функціонування цифрових систем. У практиці досліджень та проєктування доцільно розглядати поняття вірності моделювання як багатовимірне. Воно охоплює функціональну правдоподібність атак і захисту, технологічну відповідність стеку, реалістичність часових характеристик, операційний контекст організаційних процедур, а також когнітивне навантаження на учасника під час виконання вправи.

У науковій літературі та галузевих підходах найчастіше виділяють чотири моделі кіберполігонів (рис. 1). Симуляційні платформи відтворюють поведінку систем на рівні програмної логіки та модельованих об’єктів, що забезпечує масштабованість і низьку потребу в апаратних ресурсах. Емуляційні платформи розгортають реальні операційні системи, служби та мережеві компоненти у віртуалізованому або контейнеризованому вигляді, що підвищує автентичність і дозволяє відпрацьовувати професійні процедури практично без спрощень. Накладні підходи будуються на реальній інфраструктурі та доповнюються віртуальними компонентами для безпечного моделювання сценаріїв. Гібридні підходи комбінують властивості симуляції, емуляції та накладання, що дозволяє балансувати реалізм, вартість і керованість.

Для систематичного огляду важливо підкреслити, що ці моделі часто застосовуються одночасно в межах однієї платформи. Наприклад, емуляційний контур може забезпечувати доменну інфраструктуру, робочі станції, SIEM та EDR, тоді як симуляція генерує фоновий трафік користувачів, типові мережеві шумові події та “побутову” активність. Саме така композиція дозволяє створити навчальне середовище, у якому детекція і реагування відбуваються в умовах неповної інформації та великої кількості хибних або малозначущих сигналів.

Рис. 1. Основні категорії полігонів (згенеровано за допомогою ШІ)

Ключовою тенденцією останніх років є перехід від ручного розгортання лабораторій до керованого життєвого циклу середовищ на основі інфраструктури як коду. В такому підході топології мереж, образи машин, правила доступу, політики журналювання та компоненти ін’єкції подій описуються декларативно та зберігаються у репозиторіях. Це забезпечує відтворюваність, прозорість змін, можливість автоматизованого тестування середовищ перед запуском занять, а також контроль версій навчального контенту. У наукових роботах, присвячених мовам опису топологій та підходам до автоматизації розгортання, підкреслюється, що формалізований опис середовищ зменшує ризик “дрейфу конфігурацій” та полегшує масштабування занять на великі групи (Dalla Costa, 2023).

Технологічна база кіберполігонів зазвичай включає кілька шарів (рис. 2). На інфраструктурному рівні використовуються платформи віртуалізації або хмарні сервіси, які надають обчислювальні ресурси та ізоляцію. На рівні мережі застосовуються віртуальні комутатори, маршрутизація, сегментація, а також механізми безпечного виходу в інтернет або повної ізоляції. На рівні ідентичностей зазвичай розгортаються каталоги користувачів, контроль доступу на основі ролей та політики мінімальних привілеїв, оскільки саме помилки в цих механізмах найчастіше стають джерелом інцидентів. На рівні спостережуваності інтегруються компоненти збору логів і телеметрії, а також інструменти кореляції та

візуалізації. У навчальних сценаріях для SOC цей шар стає центральним, адже він дозволяє тренуватися працювати не “по інструкції”, а через розслідування за даними.

Окремим напрямом є полігони для промислових систем та інтернету речей. Тут підвищуються вимоги до гетерогенності середовища та до правдоподібності технологічних сигналів. Через це широко використовується концепція цифрових двійників, яка дозволяє моделювати процеси та одночасно забезпечувати потоки телеметрії для моніторингу й аналізу. Такий підхід зменшує ризики небезпечних наслідків помилок та робить навчання повторюваним.

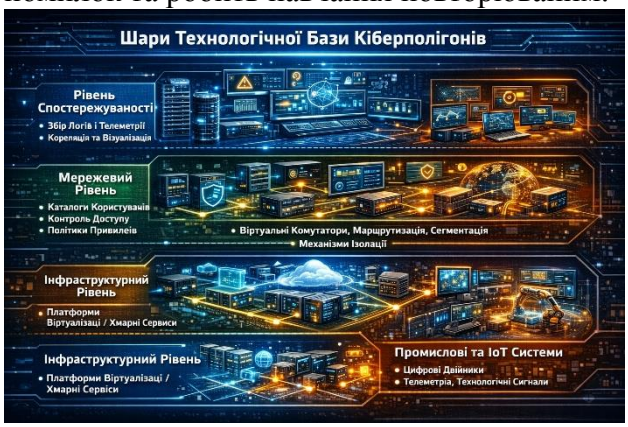

Рис. 2. Шари технологічної бази кіберполігонів (згенеровано за допомогою ШІ)

2. Педагогічні стратегії та розвиток професійного мислення

Впровадження кіберполігона в освітній процес не може бути зведене до надання студентам доступу до “віртуальної мережі”. Потрібна методика, яка перетворює практичні дії на структуроване формування компетенцій. У цьому контексті основним викликом стає керування складністю, адже надто прості вправи формують поверхневі навички, а надто складні породжують хаотичне “вгадування” та втрату мотивації.

Таксономія Блума дозволяє будувати навчальний шлях як послідовність рівнів, де кожен наступний рівень спирається на попередній. На початкових етапах учасники засвоюють базові поняття, класи атак, терміни, а також типові індикатори компрометації. На середніх рівнях вони застосовують знання в операційних процедурах, виконують тріаж, розрізняють події безпеки та експлуатаційні аномалії, здійснюють первинну локалізацію інциденту. На просунутих рівнях ключовим стає аналіз. Учасник вчиться корелювати сигнали з різних джерел, будувати часову лінію подій, висувати гіпотези та перевіряти їх, а також працювати з неповними даними. На рівні оцінювання з’являються елементи управління ризиками, коли необхідно обґрунтовувати пріоритети, оцінювати наслідки блокувань і вибирати стратегію реагування з урахуванням бізнес-критичності. Рівень створення формується тоді, коли учасник здатний проектувати правила детекції, писати плейбуки, вибудовувати архітектуру сегментації, планувати відновлення і розробляти комплексні політики безпеки.

Цикл Колба підсилює практичне навчання, оскільки робить його ітеративним. Практика починається з конкретного досвіду участі у сценарії, після чого необхідна рефлексія. Рефлексія має бути структурованою та відбуватися за принципом післядієвого аналізу. Учасники фіксують, що саме відбулося, які сигнали були ключовими, що було пропущено, які рішення виявилися помилковими та чому. Далі формується узагальнення, коли інструктор або команда перетворює події вправи на правила та патерни, які можна повторно застосувати. Завершальною фазою стає експериментування, коли сценарій повторюється з модифікаціями. Така модифікація може змінювати точку входу, техніку латерального руху, тип маскування, набір лог-джерел, обмеження в правах доступу або часові рамки. Саме повтор із варіативністю формує стійкі навички, а не одноразовий “успіх”.

Важливим елементом у кіберполігонах є командна педагогіка. У реальному середовищі фахівці працюють у ролях і з чіткими зонами відповідальності. Тому вправи повинні включати розподіл ролей, наприклад аналітик першої лінії, аналітик другої лінії, інцидент-менеджер, спеціаліст з форензіки, threat hunter, адміністратор систем. Оцінювання має враховувати не лише технічний результат, а й якість координації та комунікації. У систематичних дослідженнях, присвячених адаптації програм кібернавчання, підкреслюється важливість

безперервного узгодження навчальних активностей з реальними вимогами організацій і ринку праці (Hatzivasilis et al., 2020).

Гейміфікація може підсилювати мотивацію, однак у науковому контексті вона має бути інструментом, а не метою. Практичним компромісом є використання балів і рівнів для підтримки залученості, але з акцентом на професійні артефакти. Такими артефактами виступають коректний звіт про інцидент, обґрунтований таймлайн, правильно сформована рекомендація з пом'якшення ризику, якісно написане правило детекції, коректна ескалація та документація. Підхід, що поєднує гейміфікацію і навчальну аналітику, детально розглядається у контексті платформ нового покоління (Nespoli et al., 2025).

3. Стандартизація компетенцій через фреймворк NICE

Кіберполігони цінні тим, що вони дозволяють оцінювати компетенції не через теоретичні відповіді, а через поведінку в середовищі, де розгортається інцидент. Для того щоб така оцінка була порівнюваною та релевантною вимогам ринку праці, необхідна стандартизація. NICE Framework, описаний у NIST SP 800-181r1, забезпечує структуру, яка поєднує робочі ролі, завдання, знання та навички у форматі, придатному для проєктування навчальних траєкторій (Petersen et al., 2020).

Практичний сенс інтеграції NICE у кіберполігон полягає в тому, що сценарії перестають бути випадковим набором задач. Кожна вправа починає відповідати конкретним завданням з каталогу ролей. Наприклад, для ролі аналітика кіберзахисту сценарій може вимагати ідентифікації аномалій у мережевому трафіку, кореляції подій між різними джерелами телеметрії, визначення ймовірного вектора атаки, класифікації інциденту та формування рекомендацій. Для ролі інцидент-респондера акцент переноситься на локалізацію, стримування, відновлення та комунікацію. Для ролі спеціаліста з оцінки вразливостей важливою стає методичність сканування, пріоритизація за ризиком, валідація, а також доказовість висновків.

У контексті систематичного огляду корисно розділяти оцінювання на три рівні. Перший рівень показує, чи виконана задача як результат. Другий рівень відображає, наскільки коректно побудований процес, включно з повнотою перевірок і якістю прийнятих рішень. Третій рівень демонструє швидкість та якість, що в кібербезпеці часто має вирішальне значення. Наприклад, час до першого коректного припущення або час до локалізації може бути не менш важливим за факт успішного завершення сценарію.

Додатковою перевагою NICE є можливість будувати персоналізовані траєкторії розвитку. Коли учасник систематично демонструє слабкість на певному типі завдань, наприклад у кореляції подій або у правильному визначенні "первинної точки компрометації", полігон може пропонувати серію вправ, спрямованих саме на ці компоненти. Такий підхід збільшує ефективність навчання, оскільки замінює повтор цілого курсу на цільову роботу з прогалинами.

4. Автоматизація сценаріїв та роль агентного штучного інтелекту

Одним із центральних висновків практики впровадження кіберполігонів є те, що головною статтею витрат часто стає не інфраструктура, а створення і супровід сценарного контенту. Сценарій повинен бути правдоподібним, відтворюваним, контрольованим за складністю, безпечним, а також методично забезпеченим. Потрібно підготувати ін'єкцію подій, фонова активність, лог-джерела, критерії оцінювання та інструкції для викладача. Без автоматизації створення такого контенту стає тривалим і складним процесом.

Agentic RAG-підходи пропонують механізм, який переводить розробку вправ у напівавтоматичний режим. Агент отримує опис сценарію природною мовою, звертається до баз знань, підтягує шаблони топологій, образи хостів, типові конфігурації вразливостей, фрейми оцінювання та компоненти ін'єкції. Далі він генерує файли розгортання, скрипти налаштувань, а також перевіряє працездатність середовища. У науковому контексті підхід ARCeR демонструє цю логіку як механізм автоматизованого визначення кіберполігонів,

де агент не лише генерує, а й ітеративно виправляє помилки, забезпечуючи придатність середовища до використання (Lupinacci et al., 2025).

Разом з тим, систематичний огляд має включати критичний аналіз ризиків агентної автоматизації. Генеративні моделі можуть створювати некоректні конфігурації, підбирати неіснуючі параметри або помилково поєднувати несумісні компоненти. Додаткові ризики пов'язані з ланцюгом постачання, коли автоматично підтягуються сторонні образи або скрипти. У навчальних середовищах також існує ризик перенесення небезпечних технік за межі полігону. Тому найбільш практичним підходом є модель контролю з боку інструктора. Інструктор задає обмеження, політики безпеки, допустимі межі сценарію та критерії завершення, тоді як агент виконує рутинну частину розгортання та наповнення контентом.

Другий напрям сучасної автоматизації спирається на багатоагентне навчання з підкріпленням. У такому підході сценарій перестає бути фіксованим. Він стає змаганням автономних агентів, які можуть змінювати поведінку в реальному часі. Атакувальні агенти можуть бути агресивними, економними або прихованими, а захисні агенти навчаються будувати стратегію на основі спостережень. Дослідження, присвячені багатоагентним методам автономного кіберзахисту та ієрархічним моделям, підкреслюють, що такі підходи здатні підвищувати різноманітність і динамічність навчальних ситуацій (Kiely et al., 2025; Singh et al., 2025). Для освітнього контексту це означає, що учасники стикаються з більш реалістичною невизначеністю, а не з повторюваним набором скриптів.

Окремим фактором, що змінює вимоги до кіберполігонів, є поширення LLM у наступальних і захисних задачах. Генеративні моделі можуть посилювати фішингові кампанії, автоматизувати пошук вразливостей та прискорювати адаптацію тактик. Водночас вони можуть підтримувати захисників у пошуку кореляцій, підготовці правил детекції та документуванні. У дослідженнях, присвячених Red і Blue teaming в епоху LLM, підкреслюється необхідність перегляду підходів до тренувань, оскільки суттєво змінюється тактичний ландшафт і швидкість ескалації атак (Abuadbba et al., 2023). Звідси випливає вимога до полігонів, які навчають не лише технікам, а й правильній взаємодії з ШІ, включно з перевіркою порад і контролем помилок.

5. Багатомодальна аналітика, оцінювання та ситуаційна обізнаність

Оцінювання у кіберполігоні має демонструвати реальну професійну готовність. Прості метрики на кшталт "виконано або не виконано" є недостатніми, оскільки вони не показують якості мислення та прийняття рішень. Сучасні платформи переходять до навчальної аналітики, яка збирає дані про процес виконання завдання. Приклади такого поєднання кастомізованих вправ, гейміфікації та навчальної аналітики описані для платформ нового покоління (Nespoli et al., 2025).

Найбільш корисними є кілька груп показників. Операційні показники відображають швидкість виявлення та реагування, а також темп переходу від первинних спостережень до коректних дій. Якісні показники демонструють точність класифікації інциденту, частку хибних висновків, повноту зібраних доказів і надійність побудованого таймлайну. Процесні показники дозволяють оцінити, чи діяв учасник методично, чи робив "стрибки" між непов'язаними гіпотезами, чи повторно перевіряв ключові припущення. Командні показники відображають розподіл ролей, узгодженість дій, правильність ескалації та якість комунікації. Показники стійкості демонструють, наскільки стабільним є результат при повторенні сценаріїв або при зміні умов.

Ситуаційна обізнаність є однією з ключових компетенцій у кіберзахисті. Вона включає здатність виявляти сигнали, інтерпретувати їх у контексті, а також прогнозувати наступні дії противника. У дослідженнях запропоновано підходи до формалізованого оцінювання ситуаційної обізнаності в кіберполігонах, зокрема через SASS, що дозволяє перевести оцінювання з

рівня інтуїції інструктора на рівень системних метрик (Damianou et al., 2024). Для освітніх програм це важливо, оскільки дозволяє порівнювати результати між групами та будувати корекційні траєкторії навчання.

Багатомодальна аналітика розширює оцінювання за рахунок поєднання технічної телеметрії з додатковими каналами даних. Біометричні показники можуть розглядатися як індикатори когнітивного навантаження та стресу під час виконання вправ. У навчальній логіці це може бути корисним для стрес-інокуляційних тренувань, коли метою є не покарання за "стрес", а виявлення етапів сценарію, які призводять до когнітивних помилок, і побудова вправ для підвищення стійкості.

Етичні аспекти такого підходу потребують окремого підкреслення. Біометричні дані повинні збиратися за прозорою згодою та з мінімізацією, а також використовуватися як допоміжний сигнал. Стрес не є прямим еквівалентом некомпетентності, тому інтерпретація має бути обережною та багатофакторною.

6. Забезпечення безпеки, ізоляції та керованості навчального середовища

Кіберполігон є парадоксальним об'єктом. Він одночасно має бути максимально наближеним до реальності та максимально безпечним. У систематичному огляді важливо виділити технічні й організаційні механізми, які забезпечують такий баланс.

Ізоляція середовища реалізується через мережеву сегментацію, контрольовані шлюзи та політики виходу в інтернет. У багатьох випадках застосовується концепція "закритого контуру", де інтернет-вихід або відсутній, або замінений на модельовані служби. Такий підхід зменшує ризик неконтрольованого поширення шкідливих дій. Керування доступом повинно базуватися на ролях та мінімальних привілеях, а також включати облік дій користувачів, що важливо і для безпеки, і для оцінювання.

Керованість також включає механізми швидкого відновлення. Після кожної вправи середовище має повертатися до контрольованого стану через снепшоти, повторне розгортання або автоматизоване "очищення" компонентів. Відтворюваність виступає умовою справедливого оцінювання та об'єктивного порівняння результатів.

Для навчальних програм, які залучають різні групи або зовнішніх учасників, важливою стає мультиорендність. Вона забезпечує можливість запускати паралельні копії одного сценарію для різних команд без перетину трафіку, логів та впливу на результати. Це безпосередньо впливає на масштабування.

7. Інтеграція кіберполігонів у навчальні програми та організаційний життєвий цикл

Кіберполігон стає ефективним, коли він інтегрований у навчальну програму системно, а не епізодично. Практика показує, що найбільш результативним є підхід, у якому кіберполігон використовується як наскрізний інструмент від базових дисциплін до випускних проєктів. На початкових курсах він може застосовуватися для формування фундаментальних навичок у мережах, операційних системах, базовій криптографії, аналізі логів. На середніх курсах він підтримує дисципліни з інцидент-реагування, аналізу шкідливого ПЗ, захисту вебдодатків, безпеки хмарних середовищ. На старших курсах він стає платформою для командних навчань, капстон-проєктів, симуляцій SOC, а також для наближення студентів до реальних виробничих процедур.

Життєвий цикл впровадження зазвичай включає етап аналізу ролей, визначення компетенцій, вибір архітектури, створення бібліотеки сценаріїв, запуск з телеметрією, а потім безперервне вдосконалення. Безперервне вдосконалення є критичним, оскільки тактики атак змінюються, а навчальні матеріали без оновлення швидко втрачають актуальність. У цьому контексті автоматизація на основі IaC та агентних систем стає не просто технологічним бонусом, а способом підтримувати полігон у робочому стані без надмірного навантаження на команду викладачів.

8. Обмеження, ризики та дослідницькі прогалини

Попри очевидні переваги, кіберполігони мають обмеження, які необхідно враховувати у систематичному огляді. Один з ризиків

полягає у “CTF-ефекті”, коли учасники навчаються досягати короткострокової перемоги, але не формують процедурної дисципліни й документування. Цей ризик зростає тоді, коли оцінювання орієнтоване лише на результат і не враховує процес.

Інше обмеження пов’язане з тим, що якість навчання залежить від сценаріїв і методики, а не від платформи як такої. Навіть найкраща інфраструктура не забезпечить ефекту без добре спроєктованих вправ, адекватного рівня складності, коректних критеріїв оцінювання та якісного післядієвого аналізу.

Підтримка полігона потребує ресурсів. Оновлення образів, сумісність агентів, зміни у версіях інструментів, патчинг, безпекові політики та контроль ізоляції формують постійне навантаження. Це створює потребу у чітких процесах експлуатації та у використанні автоматизованих інструментів розгортання і перевірки працездатності.

Дослідницькі прогалини часто пов’язані з валідацією метрик. Не всі показники, які легко зібрати, корелюють з реальною ефективністю фахівця на робочому місці. Тому перспективним напрямом є створення доказових моделей, які пов’язують результати вправ із професійною успішністю, а також розробка безпечних підходів до агентної генерації сценаріїв із формальними обмеженнями та перевіркою результатів.

ВИСНОВКИ

Кіберполігони еволюціонують від допоміжних тренажерів до центральних елементів стратегічного управління кіберризиками. Інтеграція Agentic RAG та MARL робить платформу здатною до саморозгортання та динамічної зміни сценаріїв атак, що критично важливо в умовах «ШІ-фікації» сучасних загроз. Поєднання технічного реалізму з глибокою педагогічною основою та об'єктивною аналітикою дозволяє трансформувати підготовку фахівців у формат безперервних «місійних репетицій». Такий підхід забезпечує не лише наявність теоретичних знань, а й високу психологічну та практичну готовність до протидії реальним кризам у цифровому просторі.

REFERENCES

1. **Abuadbba, A., Hicks, C., Moore, K., Mavroudis, V., et al.** (2023). From Promise to Peril: Rethinking Cybersecurity Red and Blue Teaming in the Age of LLMs. arXiv preprint arXiv:2506.13434v1.
2. **Agrawal, G., Kaur, A., & Myneni, S.** (2024). A Review of Generative Models in Generating Synthetic Attack Data for Cybersecurity. Electronics, 13(2), 322.
3. **Damianou, A., Mazi, M. S., Rizos, G., Voulgaridis, A., & Votis, K.** (2024). Situational Awareness Scoring System in Cyber Range Platforms. 2024 IEEE International Conference on Cyber Security and Resilience (CSR).
4. **Dalla Costa, A.** (2023). Development of a Cyber Range with description language for network topology definition (Master's thesis). University of Turku.
5. **Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., et al.** (2020). Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees. Applied Sciences, 10(16), 5702.
6. **Kiely, M., et al.** (2025). Exploring the Efficacy of Multi-Agent Reinforcement Learning for Autonomous Cyber Defence: A CAGE Challenge 4 Perspective. AAAI Conference on Artificial Intelligence.
7. **Lupinacci, M., Blefari, F., Romeo, F., Pironti, F. A., & Furfaro, A.** (2025). ARCeR: An Agentic RAG for the Automated Definition of Cyber Ranges. Availability, Reliability and Security, 23-40.
8. **Miller, E., Mink, D., Spellings, P., Bagui, S. S., & Bagui, S. C.** (2025). Classifying Cyber Ranges: A Case-Based Analysis Using the UWF Cyber Range. Encyclopedia, 5(4), 162.
9. **Nespoli, P., Albaladejo-González, M., Ruipérez-Valiente, J. A., & Garcia-Alfaro, J.** (2025). SCORPION Cyber Range: Fully Customizable Cyberexercises, Gamification, and Learning Analytics to Train Cybersecurity Competencies. Human-centric Computing and Information Sciences, 15(67).
10. **Petersen, R., Santos, D., Smith, M. C., Wetzel, K. A., & Gitte, W.** (2020). Workforce Framework for Cybersecurity (NICE Framework). NIST Special Publication 800-181r1.
11. **Singh, A. V., Rathbun, E., Graham, E., Oakley, L., et al.** (2025). Hierarchical Multi-agent Reinforcement Learning for Cyber Network Defense. Reinforcement Learning Journal.
12. **Wen, D.** (2021). Automated Cyber Ranges: Design Features, Architectures, Scenarios and

Impacts (Undergraduate Honors Thesis). Brigham Young University.

Analysis of approaches to the implementation of cyber ranges in the training of cyber security specialists

Maksym Delembovskyi, Sergiy Gnatyuk, Borys Korniichuk

Abstract. This article provides a comprehensive analysis of current strategies for the use of cyber ranges as intellectual platforms for the development of professional competencies in the field of cybersecurity. The study covers the evolution from static virtual laboratories to dynamic ecosystems based on cloud technologies and digital twins of real infrastructures. Particular attention is paid to the integration of advanced pedagogical concepts, such as Bloom's taxonomy and Kolb's cycle, with the industry standards of the NICE framework. The paper examines in detail the role of automation through Retrieval-Augmented Generation (ARCeR) agent systems and multi-agent reinforcement learning (MARL), which allows for the creation of adaptive learning scenarios. The results of the study emphasize the importance of using multimodal analytics, including biometric stress monitoring, for an objective assessment of specialists' readiness to act in crisis situations.

Keywords: Cyber ranges, cyber defense, NICE framework, Bloom's taxonomy, RAG agent systems, multi-agent reinforcement learning, digital twins, situational awareness, scenario automation.