**DOI: 10.18372/2225-5036.31.20703**

# БАЗОВІ ПРИНЦИПИ РОЗРОБКИ ТА ЗАСТОСУВАННЯ КІБЕРПОЛІГОНІВ ДЛЯ ПІДГОТОВКИ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ

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

*[1]Київський національний університет будівництва і архітектури, Україна*
*[2] Державний університет «Київський авіаційний інститут», Україна*

**ДЕЛЕМБОВСЬКИЙ Максим Михайлович,** к.т.н., доцент
*Рік та місце народження:* 1986 рік, м. Лієпая, Латвія.
*Освіта:* Державний університет інформаційно-комунікаційних технологій, 2019 рік.
*Посада:* завідувач кафедри кібербезпеки та комп'ютерної інженерії КНУБА з 2025 року.
*Наукові інтереси:* кібербезпека, ICS/SCADA, SOC, OSINT.
*Публікації:* більше 50 наукових публікацій, серед яких монографії, наукові статті та патенти на винаходи.
*E-mail:* delembovskyi.mm@knuba.edu.ua
Orcid: 0000-0002-6543-0701

**ГНАТЮК Сергій Олександрович,** д.т.н., професор
*Рік та місце народження:* 1985 рік, м. Нетішин, Хмельницька область, Україна
*Освіта:* Національний авіаційний університет, 2007 рік.
*Посада:* проректор з наукових досліджень та трансферу технологій КАІ з 2024 року.
*Наукові інтереси:* інформаційна безпека, квантова криптографія, управління інцидентами інформаційної безпеки, захист критичної інформаційної інфраструктури держави.
*Публікації:* більше 350 наукових публікацій, серед яких монографії, статті у провідних вітчизняних та закордонних наукових виданнях, патенти та авторські свідоцтва.
*E-mail:* s.gnatyuk@kai.edu.ua
Orcid: 0000-0003-4992-0564

**КОРНІЙЧУК Борис Валерійович** к.т.н., доцент
*Рік та місце народження:* 1977 рік, Київ, Україна.
*Освіта:* Київський національний університет будівництва і архітектури, 2012 рік.
*Посада:* доцент кафедри професійної освіти КНУБА з 2012 року.
*Наукові інтереси:* інформаційна безпека, реагування на інциденти інформаційної безпеки, квантова криптографія.
*Публікації:* більше 90 наукових публікацій, серед яких монографії, наукові статті, матеріали та тези доповідей на конференціях, патенти та авторські свідоцтва.
*E-mail:* korniichuk.bv@knuba.edu.ua
Orcid: 0000-0003-3881-1581

***Анотація.*** *У статті здійснено комплексний огляд базових принципів проєктування та практичного застосування кіберполігонів як керованих навчально-дослідних середовищ для формування професійних компетентностей у сфері кіберзахисту. Показано еволюцію тренувальних платформ від статичних віртуальних лабораторій до масштабованих хмарних екосистем і цифрових двійників інфраструктур, які відтворюють реалістичні мережеві топології, типові бізнес-сервіси та поведінку користувачів. Аргументовано, що на тлі зростання економічних втрат від кіберзлочинності та розширення розриву в кадровому забезпеченні, кіберполігони стають ключовим інструментом набуття «бойового» досвіду в безпечних умовах. З урахуванням фреймворку NICE, педагогічних моделей Блума та Колба, а також сучасних підходів до автоматизації сценаріїв, запропоновано узагальнену систему принципів, що охоплює архітектуру, керування контентом, оцінювання результатів, безпеку й відповідність етичним та правовим обмеженням. Окрему увагу приділено використанню штучного інтелекту, агентних RAG-підходів і багатоагентного навчання з підкріпленням для підвищення адаптивності вправ і якості аналітики навчання.*

***Ключові слова:*** *кіберполігон; кіберзахист; підготовка кадрів; NICE Framework; таксономія Блума; цикл Колба; сценарії «сценарій як код»; інфраструктура як код; цифрові двійники; ситуаційна обізнаність; learning analytics; SIEM/SOAR; Agentic RAG; багатоагентне навчання з підкріпленням; Purple Team.*

**Вступ.** Цифровізація критичних сервісів і бізнес-процесів призвела до того, що кіберпростір став повноцінним полем конкуренції, злочинності та геополітичного протистояння. За оцінками Cybersecurity Ventures, сукупні втрати світової економіки від кіберзлочинності оцінюються на рівні 10,5 трлн доларів США на 2025 рік. Паралельно зростає кадровий дефіцит. Згідно з результатами дослідження ISC2, оцінка глобальної чисельності кібербезпекового персоналу становить 5 468 173 фахівці, а розрив потреби та наявної пропозиції визначено як 4 763 963 фахівці. У таких умовах освітні програми стикаються з жорсткою вимогою забезпечити не лише теоретичну базу, а й відтворювані практичні результати, порівнювані з реальним досвідом роботи в SOC, групах реагування або командах пентесту.

Водночас класичні формати підготовки, орієнтовані на лекційний контент і окремі «ізольовані» лабораторні, погано відповідають

природі сучасних атак, що розгортаються як ланцюжки дій, використовують автоматизацію, хмарні сервіси, компрометацію ідентичностей, латеральний рух і приховане утримання доступу. Роботодавці також послідовно підвищують планку до практичного досвіду. Наприклад, у звіті NIST на основі даних Burning Glass зазначено, що 83% вакансій у кібербезпеці вимагали щонайменше 3 роки досвіду, а середні вимоги сягали 5,4 року. Це створює парадокс «потрібен досвід, щоб отримати досвід», який без спеціалізованих тренажерних середовищ долається повільно і не системно.

Кіберполігони як інструмент підготовки дають змогу відпрацьовувати повні цикли виявлення, аналізу, реагування та відновлення, не наражаючи на ризик продуктивну інфраструктуру. Вони дозволяють поєднати технічну реалістичність із педагогічним дизайном, а також забезпечити вимірюваність результатів через метрики, телеметрію, журнали подій і моделі компетентностей. Саме тому дослідження базових принципів створення та використання кіберполігонів є актуальним як для університетської підготовки, так і для корпоративного навчання та оцінювання персоналу.

**Аналіз існуючих досліджень**

Наукові та прикладні дослідження кіберполігонів пройшли шлях від опису віртуальних лабораторій до розгляду кіберполігонів як «керованих екосистем компетентностей». У ранніх роботах домінував технічний акцент, зосереджений на віртуалізації, мережевій сегментації та відтворенні типових сервісів. Сучасні публікації, навпаки, прагнуть стандартизувати підхід до побудови вправ, повторного використання контенту, вимірювання навчальних результатів і підв'язки до професійних профілів. У керівництві NIST щодо кіберполігонів наголошено на доцільності узгодження вправ і навчальних активностей із NICE Framework, зокрема через прив'язку до завдань, знань і навичок, а також наводиться узагальнена типологія кіберполігонів (simulation, overlay, emulation, hybrid). Це підкреслює тенденцію до єдиного понятійного апарату та опори на формалізовані моделі компетентностей.

Другий потужний напрям стосується автоматизації та використання штучного інтелекту. З'являються підходи, що мінімізують ручну працю інструктора під час проєктування топологій, генерації конфігурацій і підготовки «вкидів» інцидентів. У межах Agentic RAG-підходів демонструється можливість перетворювати опис інфраструктури природною мовою у формальні артефакти розгортання, з автоматичною перевіркою помилок і відновленням працездатності сценарію. Паралельно розвиваються середовища для багатоагентних змагань захисту та нападу, де поведінка «супротивника» моделюється як динамічна, адаптивна, з варіацією тактик і умов.

Третій напрям присвячений педагогічній ефективності. Тут домінують підходи, що інтегрують таксономію Блума, цикл Колба, deliberate practice, а також елементи гейміфікації й навчальної аналітики. Особливий акцент робиться на тому, що реалістичність інфраструктури сама по собі не гарантує навчального ефекту, якщо не визначені вимірювані результати, критерії успіху, механізми зворотного зв'язку та сценарії рефлексії.

***Метою*** цього дослідження є систематизація базових принципів розробки та застосування кіберполігонів, які забезпечують ефективне формування практичних навичок кіберзахисту через поєднання технологічної архітектури, автоматизації, професійних стандартів NICE та педагогічних моделей, а також визначення вимог до оцінювання, безпеки й керування контентом кібернавчання.

**Основна частина дослідження**

*1. Функціонал і роль кіберполігонів у підготовці фахівців*

Кіберполігон доцільно розуміти як кероване ізольоване середовище, що відтворює інфраструктуру, загрози та операційні процеси кіберзахисту з можливістю контрольованого запуску подій, збору телеметрії та оцінювання дій учасників. На відміну від «лабораторної» моделі, де студент виконує фрагментарні кроки за інструкцією, кіберполігон орієнтований на місійність. Учасники отримують роль, контекст, обмеження часу, реалістичні артефакти, а також вимірюваний результат, що відповідає завданням реальної діяльності.

У професійній підготовці кіберполігон виконує принаймні чотири функції.

- Тренувальна – це формування навичок через повторювані вправи зі зростанням складності.
- Оціночна – це перевірка готовності за метриками часу, точності, повноти та якості рішень.
- Дослідницька – це експерименти з політиками безпеки, інструментами детекції, моделями атак.
- Організаційна – це командна взаємодія, комунікація, передача зміни, документування інцидентів, робота зі стандартами й процедурами.

Ці функції важливі в умовах кадрового дефіциту та високих вимог до досвіду. Коли переважна частка вакансій вимагає кількарічної практики, кіберполігон стає механізмом «прискорення досвіду» через симуляцію тисяч реалістичних подій у стислий навчальний період.

*2. Типологія кіберполігонів і критерії вибору моделі*

Вибір типу кіберполігона визначає баланс між вартістю, реалістичністю та керованістю. У керівництві NIST виокремлюються чотири узагальнені типи кіберполігонів.

Simulation range відтворює мережеву поведінку синтетично, зазвичай у віртуальних інстансах. Перевага полягає в швидкій реконфігурації та масштабуванні. Обмеження пов'язані з меншою точністю апаратних ефектів і мережевих характеристик.

Overlay range працює поверх реальної інфраструктури. Це підвищує реалістичність, але ускладнює безпечну ізоляцію і збільшує витрати.

Emulation range прагне максимальної відповідності реальному середовищу через емуляцію обладнання, ПЗ і мережевих умов. Це доречно для специфічних технологій, наприклад, промислових протоколів або мережевого обладнання конкретних виробників.

Hybrid range поєднує елементи попередніх підходів, створюючи оптимальний компроміс під конкретний сценарій.

Практичний вибір типу доцільно здійснювати за критеріями (табл. 1):

- вимоги до достовірності, включно з мережевими затримками, специфікою протоколів і поведінкою сервісів;
- масштабованість для груп і потоків студентів;
- відтворюваність і керованість станів;
- вартість володіння та супроводу;
- ризик впливу на зовнішні системи, зокрема юридичні та етичні аспекти;
- потреба в інтеграції з інструментами SOC, SIEM, SOAR і EDR.

Для університетського навчання найчастіше оптимальними є simulation або hybrid-підходи, оскільки вони краще підтримують автоматизоване масове розгортання, а також дають змогу забезпечити однакові умови для великої кількості учасників.

Таблиця 1

Порівняння типів кіберполігонів за критеріями впровадження

| *Тип кіберполігона* | *Рівень реалістичності* | *Масштабованість* | *Складність супроводу* | *Орієнтовна вартість* | *Типові кейси застосування* |
|---|---|---|---|---|---|
| Симуляційний | Середній | Висока | Низька | Низька | Масове навчання, базові SOC-вправи, відпрацювання процесів |
| Емуляційний | Високий | Середня | Висока | Висока | Протоколи та обладнання конкретних вендорів, ICS/SCADA-лабораторії |
| Накладений (overlay) | Високий | Низька–середня | Висока | Висока | Тестування процедур на "живій" інфраструктурі, аудит детекцій |
| Гібридний | Високий (керований) | Висока | Середня | Середня–висока | Комбіновані навчальні програми, Purple Team, комплексні сценарії |

*3. Принципи проєктування навчальної цінності, а не лише інфраструктури*

Типовою помилкою під час впровадження кіберполігона є сприйняття його як «великої лабораторії». Такий підхід призводить до того, що інвестиції йдуть у віртуальні машини та мережі, але не в навчальний дизайн. Базовий принцип полягає в тому, що кіберполігон повинен бути спроєктований від цілі до інфраструктури, а не навпаки.

Ціль вправи має бути визначена як конкретний вимірюваний результат, пов'язаний із робочою роллю. Наприклад, «визначити ланцюжок компрометації та локалізувати інцидент без втрати критичного сервісу» або «застосувати політику сегментації, знизивши латеральний рух до нуля в межах 30 хвилин». Далі формуються критерії оцінки, артефакти, сигнали, обмеження часу, точки ухвалення рішень, очікувані дії та ризикові помилки.

Другий принцип полягає в поступовості. Навчання має рухатися від керованих умов до невизначеності. На ранніх етапах учасник отримує підказки, спрощений ландшафт подій, обмежений набір інструментів і зрозумілу модель атаки. На наступних етапах збільшується шум, додаються хибні спрацювання, з'являються паралельні події, обмеження ресурсів і комунікаційні задачі.

Третій принцип стосується рефлексії. Будь-яка «місія» повинна завершуватися розбором. У межах кіберполігона це реалізується як автоматизований debriefing з таймлайном подій, порівнянням очікуваних і фактичних дій, аналізом втрат часу та помилкових гіпотез. Саме на цьому етапі формується стійке знання та перенос у професійну практику.

*4. Архітектурні шари кіберполігона та технологічний стек*

Архітектуру кіберполігона доцільно описувати як багатошарову систему, де кожен шар підтримує принципи модульності та керованості.

Обчислювально-інфраструктурний шар включає віртуалізацію, контейнери, мережеву віртуалізацію, сховища, балансування та механізми ізоляції. На практиці використовують комбінації гіпервізорів і контейнерної інфраструктури. Гіпервізори забезпечують сильну ізоляцію для «важких» компонентів, тоді як контейнери дають високу щільність і швидкий старт для допоміжних сервісів і агентів.

Мережевий шар включає сегментацію, віртуальні комутатори, маршрутизацію, політики доступу, моделювання NAT, VPN, DMZ, а також керування трафіком. Для навчання важливо відтворювати типові архітектури підприємств, де зони довіри не однорідні, а права доступу прив'язані до ролей. Сегментація має бути не просто схемою

VLAN, а набором правил, які можна перевірити через сценарій атаки й сценарій захисту.

Шар ідентичностей та доступу є критичним, оскільки компрометація облікових записів часто лежить в основі реальних інцидентів. У кіберполігоні цей шар реалізують через доменні служби, керування привілеями, багатофакторну автентифікацію та механізми аудитингу. З методичної точки зору важливо, щоб учасник бачив наслідки надмірних прав, слабких політик паролів, відсутності сегрегації обов'язків і неправильного налаштування привілеїв.

Шар спостережуваності та безпекових інструментів охоплює журнали подій, мережеву телеметрію, SIEM, EDR, IDS/IPS, систему керування кейсами, а також інструменти автоматизації реагування. Для SOC-орієнтованих вправ саме цей шар стає центральним, оскільки забезпечує матеріал для аналітики та ухвалення рішень.

Шар навчального керування включає LMS або спеціалізований RLMS, що забезпечує реєстрацію учасників, видачу завдань, контроль часу, збір результатів, формування звітів і дашбордів. Перевага спеціалізованих рішень полягає в тому, що оцінювання може бути не тільки підсумковим, а й процесним, з аналізом стратегій та вибору інструментів.

*5. Оркестрація, «інфраструктура як код» і відтворюваність сценаріїв*

Базова вимога до кіберполігона, який використовується системно, полягає у відтворюваності. Навчальна група повинна отримувати однакові стартові умови, а інструктор має бути здатний швидко відновити середовище після помилок або активних атак. Це неможливо забезпечити ручним розгортанням.

Тому ключовим принципом стає використання «інфраструктури як код» і «сценарію як код». У першому випадку мережі, віртуальні машини, правила доступу та служби описуються декларативно і версіонуються. У другому випадку описуються події, «вкиди», ролі, чекпоїнти, оцінювальні правила та умови завершення місії.

Оркестраційний контур доцільно будувати за CI/CD-логікою. Кожна зміна сценарію проходить лінтинг, тестування, перевірку залежностей, розгортання в тестовому середовищі, автоматичне програвання контрольних кроків і лише після цього потрапляє до «виробничого» контуру навчання. Така практика знижує ризик того, що студенти стикаються з «поламаним» стендом і втрачають навчальний час.

Важливим є механізм керування станами. Для складних вправ корисно мати контрольні точки, що дозволяють повернути середовище до певного етапу без повного перерозгортання. Це прискорює навчання і дозволяє багаторазово відпрацьовувати конкретні навички, що є основою deliberate practice.

*6. Керування контентом, життєвий цикл вправи та якість сценаріїв*

Сценарії є «навчальним продуктом» кіберполігона, а інфраструктура є «виробничою платформою». Звідси випливає принцип контентного керування. Сценарій повинен мати паспорт, що включає навчальну мету, профіль аудиторії, вхідні вимоги, зв'язок із робочою роллю, часовий бюджет, набір інструментів, очікувані артефакти, критерії оцінки, ризики й обмеження.

Життєвий цикл вправи включає етапи:

- проєктування навчального результату та карти компетентностей;
- проєктування сюжету, подій і «сигналів»;
- розроблення та інтеграція інфраструктурних компонентів;
- валідація, яка включає програвання сценарію контрольним виконавцем;
- проведення, збір телеметрії та результатів;
- debriefing і оновлення;
- архівація або перетворення на модуль, що повторно використовується.

Валідація повинна охоплювати не лише технічну працездатність, а й педагогічну адекватність. Якщо сценарій надто складний для заданого рівня, учасник «тонутиме» в шумі й не сформує цільової навички. Якщо сценарій надто простий, виникає ілюзія компетентності. Практично корисним є введення показників складності. Наприклад, кількість паралельних подій, співвідношення істинних і хибних спрацювань, частка дій з високою невизначеністю, кількість можливих гіпотез.

Для підвищення реалістичності корисно прив'язувати сценарій до моделей тактик і технік. Наприклад, карта подій може узгоджуватися з відомими матрицями тактик, де кожен етап атаки має свої артефакти в логах, мережевих потоках і системних подіях. Це підвищує перенос навчання у практику та спрощує оцінювання.

*7. Педагогічний дизайн на основі таксономії Блума та циклу Колба*

Технічна грамотність у кібербезпеці формується як «сходи» від базових знань до творчого проєктування захисту. Таксономія Блума дозволяє формалізувати ці рівні та прив'язати їх до вправ.

На рівні запам'ятовування учасник розпізнає атаки, артефакти, журнали та базові протоколи.

На рівні розуміння пояснює причинно-наслідкові зв'язки та механізми вразливостей.

На рівні застосування виконує інструментальні дії, наприклад, запускає аналіз трафіку, сканує, перевіряє конфігурації.

На рівні аналізу будує гіпотези, корелює події й реконструює таймлайн.

На рівні оцінювання приймає рішення щодо пріоритетів, ризиків і компромісів між безпекою та доступністю.

На рівні створення проєктує стратегію, план відновлення, політики доступу та архітектуру захисту.

Цикл Колба доповнює цю модель через навчальну ітерацію. Спочатку учасник отримує конкретний досвід у вправі. Далі відбувається рефлексія, де аналізуються помилки та успіхи. Потім формується узагальнена концепція, яка пояснює, чому рішення було правильним чи хибним. Завершальний етап полягає в активному експериментуванні, коли учасник застосовує нову стратегію в зміненому сценарії. Така модель є основою «усвідомленої практики», де ключовим є багаторазове відпрацювання слабких місць із миттєвим зворотним зв'язком.

*8. Стандартизація компетентностей через NICE Framework і модель TKS*

Перевага NICE Framework полягає в тому, що він дозволяє перевести навчання зі сфери «загальних вражень» у сферу вимірюваних компетентностей. NIST прямо вказує на можливість інтеграції NICE у програмування кіберполігонів і прив'язку активностей до категорій робочих ролей та компонентів TKS (табл. 2).

Модель TKS включає завдання, знання та навички. Для кіберполігона це означає, що:

- завдання мають бути реалізовані як спостережувані дії в системі, включно з кроками розслідування, ескалації та документування;
- знання мають перевірятися через рішення, пояснення, вибір методів, а не лише тестом;
- навички мають бути вимірювані за результатом і процесом, наприклад, швидкістю побудови таймлайну, точністю атрибуції, мінімізацією хибних висновків.

Практична реалізація полягає в створенні карти відповідності. Для кожної вправи визначається робоча роль або набір ролей. Далі виписуються ключові завдання, які повинен виконати учасник, і визначаються індикатори успіху. Наприклад, для ролі аналітика SOC можна оцінювати: коректність первинної тріаж-оцінки, здатність відрізнити шум від сигналу, якість ескалації інциденту та формування рекомендацій. Для ролі спеціаліста з реагування оцінюються рішення ізоляції, відновлення, збереження доказів і мінімізації впливу на доступність.

Окрема перевага NICE полягає в можливості використовувати кіберполігон як інструмент добору персоналу та оцінювання прогалин. На відміну від інтерв'ю, де значну частку займає самоопис, кіберполігон дає поведінкові дані та знижує суб'єктивність оцінки.

Важливим педагогічним принципом є управління когнітивним навантаженням. У кіберполігоні легко перевантажити учасника обсягом логів, інструментів і тривог. Тому сценарії мають бути спроєктовані як «сходи складності», де на кожному рівні є обмежений набір нових змінних, а все інше залишається стабільним.

Таблиця 2

Приклад мапінгу NICE (TKS) до артефактів кіберполігона та джерел телеметрії

| *Компонент TKS* | *Що перевіряється на полігоні* | *Артефакти, які збираються* | *Джерела даних* |
|---|---|---|---|
| Завдання (Tasks) | Дії учасника в межах ролі | Таймлайн дій, ескалації, застосовані плейбуки | SIEM, SOAR, журнали команд, тикет-система |
| Знання (Knowledge) | Розуміння принципів та причин | Пояснення рішень, обґрунтування вибору методів | Короткі звіти, контрольні питання, debriefing |
| Навички (Skills) | Спостережувана здатність виконувати роботу | Швидкість, точність, ефективність реагування | Теле-метрики вправи, журнали інструментів, network telemetry |

*9. Формати вправ і командна взаємодія, включно з Red, Blue та Purple Team*

Кіберполігони підтримують різні формати навчання. Вибір формату визначається метою та рівнем підготовки.

Індивідуальні вправи корисні для відпрацювання інструментальних навичок і базового аналізу. Вони легко масштабується на потоки студентів, але слабше формують командну взаємодію.

Командні Blue Team-вправи формують навички оборони. Тут важливі процеси моніторингу, реагування, документування, комунікації, передачі зміни. Вони наближені до роботи SOC і дозволяють оцінювати не лише техніку, а й операційні компетентності.

Red Team-вправи орієнтуються на моделювання атак, експлуатацію, пост-експлуатацію, прихованість і досягнення цілей. У навчанні вони корисні для розуміння мислення атакувальника, але потребують жорсткого контролю безпеки.

Purple Team-підхід поєднує напад і захист у форматі спільного навчання. Він дає високу дидактичну цінність, оскільки дозволяє узгодити очікувані артефакти атаки, уточнити правила детекції та зробити налаштування інструментів спостережуваності. У довгостроковій перспективі саме Purple Team-практики підвищують якість детекційного контенту і зрілість процедур.

CTF-формат є сильним мотиваційним інструментом. Проте для професійної підготовки його слід доповнювати «контекстом», інакше учасник вирішує головоломки без розуміння операційних наслідків. Тому в академічних програмах доцільно поєднувати CTF із сценарними місіями, де є бізнес-сервіс, SLA, користувачі, ризики й вимоги документування.

*10. Оцінювання результатів, ситуаційна обізнаність і навчальна аналітика*

Традиційна оцінка «правильно чи неправильно» не відображає реальної складності кіберзахисту. Практичні результати залежать від того, як швидко учасник побачив сигнал, яку гіпотезу побудував, чи перевірив альтернативи, як мінімізував побічні втрати, чи зберіг докази.

Тому базовим принципом є процесне оцінювання, де враховується траєкторія дій. Це можливо завдяки телеметрії, зокрема журналам команд, запитам до SIEM, змінам політик, викликам API, маніпуляціям із хостами. На основі цих даних можна оцінювати:

- час до первинного виявлення та час до локалізації;
- точність атрибуції та частку хибних висновків;
- кількість «дорогих» помилок, наприклад, зупинка сервісу без потреби;
- якість документування, включно з таймлайном та рекомендаціями;
- ефективність командної комунікації, що може вимірюватися затримками між ескалаціями та виконанням дій.

Окремий пласт становить оцінка ситуаційної обізнаності. У межах кіберполігона можна вимірювати, чи учасник лише «бачить події», чи розуміє їх значення, чи може прогнозувати розвиток і обирати оптимальну дію. Такий підхід дає змогу перейти від оцінки інструментів до оцінки мислення.

Аналітика навчання набуває практичної цінності, якщо вона подається інструктору у вигляді інтерпретованих дашбордів. Наприклад, розподіл часу на етапи інциденту, порівняння команд, типові помилки, граф залежностей подій і дій. Це дозволяє коригувати програму, формувати індивідуальні траєкторії та планувати додаткові тренування.

*11. Автоматизація сценаріїв і роль штучного інтелекту*

Автоматизація є необхідною умовою масштабування кіберполігона. Вона охоплює розгортання, генерацію подій, контроль станів, оцінювання та підготовку debriefing.

Штучний інтелект підсилює цей контур у трьох напрямах:

*Генерація та адаптація контенту* - агентні RAG-підходи дозволяють будувати сценарії на основі описів природною мовою, перетворюючи їх у артефакти розгортання і правила оцінювання. Це скорочує час підготовки і зменшує бар'єр для викладачів, які не є DevOps-спеціалістами.

*Інтелектуальні опоненти* - багатоагентне навчання з підкріпленням дає можливість моделювати динамічного супротивника, який змінює тактики залежно від дій захисника. Це зменшує «заучування» сценарію та підтримує ефект новизни.

*Аналітика навчання* - моделі можуть класифікувати стратегії, виявляти типові помилки, прогнозувати, на якому етапі учасник «застрягне», та пропонувати адресний зворотний зв'язок.

Разом із перевагами виникають ризики. Моделі можуть генерувати некоректні конфігурації, помилятися у трактуванні подій або створювати небезпечні поради. Тому принцип безпечної інтеграції ШІ включає перевірюваність, контроль доступу, журналювання дій агента і режим «людина в контурі» для критичних змін. У навчальному контексті важливо не допустити ситуації, коли студент «виконує підказку», але не формує компетентність. Тому підказки повинні бути дозованими і не замінювати мислення.

*12. Безпека, етика та правові обмеження під час експлуатації кіберполігонів*

Кіберполігон працює з потенційно небезпечним контентом, включно зі зразками шкідливого ПЗ, експлойтами, техніками обходу й інструментами, що можуть бути використані зловмисно. Це формує обов'язковий принцип «безпечного навчання», який включає технічні та організаційні заходи.

Технічні заходи включають ізоляцію середовища, контроль виходу в інтернет, фільтрацію, обмеження привілеїв, сегментацію, моніторинг і швидке відновлення. Для сценаріїв із «живими» зразками шкідливого ПЗ доцільно застосовувати додаткові контрзаходи, включно з окремими мережами, політиками відсутності маршрутизації у зовнішні сегменти і автоматичним знищенням середовища після завершення вправи.

Організаційні заходи включають правила використання, політики академічної доброчесності, підписані зобов'язання, контроль доступу, аудит дій інструкторів та учасників. Правова частина передбачає, що навчання не повинно переходити межі дозволеного, зокрема у випадках, коли сценарій може впливати на реальні зовнішні ресурси.

Етичний аспект полягає в тому, що навчання має формувати відповідальне ставлення. Учасники повинні розуміти, що навіть у симуляції дії мають наслідки, а компетентність кібербезпеки пов'язана з довірою та відповідальністю. Корисною практикою є включення в сценарії елементів регуляторних вимог, вимог до збереження доказів, приватності й комунікації з керівництвом.

*13. Приклади сценаріїв, орієнтованих на реальні загрози*

Сценарії мають бути максимально наближені до реальних інцидентів, але адаптовані до рівня підготовки.

Сценарій «вразливість мережевого сервісу та боковий рух». Мета полягає в тому, щоб учасники виявили первинну компрометацію, зупинили латеральний рух, відновили сервіс і підготували звіт. У такому сценарії важливо забезпечити артефакти в мережевих потоках і журналах, а також додати

елементи «зашумлення», щоб змоделювати реальне навантаження SOC.

Сценарій «шифрувальник і відновлення» учасники повинні визначити ланцюжок зараження, локалізувати інцидент, оцінити масштаб, перевірити резервні копії, ухвалити рішення щодо відновлення та підготувати комунікаційний план. Навчальна цінність полягає у відпрацюванні компромісів між часом, доступністю та збереженням доказів.

Сценарій «DDoS і забезпечення безперервності» у моделі важливо поєднати технічний аспект фільтрації трафіку з аспектом управління сервісом, де частина ресурсів обмежена, а рішення мають прийматися під тиском часу.

Сценарій «компрометація ідентичності» у ньому акцент робиться на аналізі журналів автентифікації, виявленні аномалій, використанні MFA, обмеженні привілеїв і сегментації. Такий сценарій особливо корисний, оскільки відображає сучасний тренд атак на облікові записи та хмарні середовища.

Сценарії для ICS/SCADA та IoT можуть включати моделювання промислових протоколів, HMI, PLC-логіки та сегментації між офісною і технологічною мережами. Тут важливо враховувати вимоги безперервності і те, що «зупинка процесу» може бути недопустимою навіть у симуляції. Тому оцінювання має враховувати не лише детекцію, а й безпечність реагування.

*14. Економіка впровадження та модель Cyber Range as a Service*

Для навчальних закладів і невеликих організацій ключовим бар'єром є вартість створення, підтримки та оновлення середовищ. Модель «кіберполігон як сервіс» зменшує капітальні витрати та переносить акцент на керування сценаріями й методикою. При цьому важливо зберегти контроль над даними, можливість кастомізації під навчальні плани та відповідність політикам безпеки.

Економічна ефективність підвищується, якщо:

- середовище проектується як модульне, з бібліотекою повторно використовуваних компонентів;
- сценарії параметризуються, що дозволяє генерувати багато варіантів на основі одного шаблону;
- оцінювання автоматизується, скорочуючи час інструктора;
- навчальна аналітика використовується для оптимізації програми, зменшуючи «марні» повтори.

**Висновки**

Отже, метою цієї статті є систематизація базових принципів розробки та застосування кіберполігонів як керованих навчально-дослідних середовищ для формування і об'єктивного оцінювання практичних компетентностей фахівців з кібербезпеки. Для досягнення поставленої мети узагальнено підходи до типології кіберполігонів, окреслено вимоги до їхньої багатошарової архітектури та технологічного стека, визначено роль оркестрації й відтворюваності через інфраструктуру як код і сценарій як код, а також обґрунтовано необхідність поєднання технологічних рішень із педагогічними моделями таксономії Блума та циклу Колба. Окремо показано, що стандартизація підготовки за фреймворком NICE дозволяє здійснювати мапінг навчальних активностей на завдання, знання та навички, що підвищує релевантність тренувань до вимог ринку праці та зменшує суб'єктивність оцінювання.

Отримані результати підтверджують, що кіберполігони перетворилися з допоміжного інструмента демонстрацій у повноцінні інтелектуальні платформи, здатні відтворювати комплексні інциденти та забезпечувати вимірюваність навчальних результатів. Підвищення практичної цінності кіберполігонів досягається за рахунок модульності архітектури, автоматизації розгортання, керування життєвим циклом сценаріїв і застосування метрик, які оцінюють не лише факт виконання завдання, а й процес ухвалення рішень, швидкість виявлення та локалізації інциденту, якість детекції й коректність відновлення сервісів. Перспективним напрямом визначено інтеграцію штучного інтелекту, зокрема агентних RAG-підходів і багатоагентного навчання з підкріпленням, для автоматизованого проєктування сценаріїв, адаптації складності та формування динамічних моделей противника, однак така інтеграція потребує контрольованості, верифікації та режиму участі людини в критичних рішеннях.

Важливо підкреслити, що дана стаття є логічним продовженням дисертаційного дослідження за темою «Методологічні основи створення інтелектуальних кіберполігонів для комплексного моделювання атак та захисту інформаційних систем». У межах дисертаційної роботи окреслені в цій публікації принципи розглядаються як базовий фундамент для подальшого поглиблення методології, зокрема для формалізації моделей сценаріїв і метаданих, розроблення системи показників ситуаційної обізнаності та комплексного оцінювання готовності, а також для побудови адаптивних механізмів генерації і програвання кібернавчальних місій у середовищах різного рівня достовірності. Отже, результати статті можуть бути використані як теоретико-прикладна основа для проєктування кіберполігонів у закладах вищої освіти та корпоративних програмах підготовки, а також як підґрунтя для подальших досліджень, спрямованих на підвищення масштабованості, об'єктивності оцінювання та відповідності тренувань реальним загрозам і операційним процесам кіберзахисту.

**Література**

[1] Petersen R. Workforce Framework for Cybersecurity (NICE Framework) / R. Petersen, D. Santos, M. C. Smith, K. A. Wetzel, G. Witte // NIST Special Publication 800-181r1. Gaithersburg, 2020. DOI: 10.6028/NIST.SP.800-181r1.

[2] NIST. The Cyber Range: A Guide // National Institute of Standards and Technology. Gaithersburg, 2024.

[3] ISC2. Results of the 2024 ISC2 Cybersecurity Workforce Study // ISC2 Research Insights. Clearwater, 2024.

[4] Cybersecurity Ventures. Official 2026 Cybersecurity Market Report: Predictions and Statistics // Cybercrime Magazine, 2025.

[5] Hatzivasilis G. Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees / G. Hatzivasilis, S. Ioannidis, M. Smyrlis, G. Spanoudakis та ін. // Applied Sciences. 2020. Vol. 10, No. 16. Art. 5702. DOI: 10.3390/app10165702.

[6] Lupinacci M. ARCeR: An Agentic RAG for the Automated Definition of Cyber Ranges / M. Lupinacci, F. Blefari, F. Romeo, F. A. Pironti, A. Furfaro // Availability, Reliability and Security. 2025. P. 23–40. DOI: 10.1007/978-3-032-00630-1_2.

[7] Nespoli P. SCORPION Cyber Range: Fully Customizable Cyberexercises, Gamification, and Learning Analytics to Train Cybersecurity Competencies / P. Nespoli, M. Albaladejo-González, J. A. Ruipérez-Valiente, J. Garcia-Alfaro // Human-centric Computing and Information Sciences. 2025. Vol. 15. Art. 67.

[8] Damianou A. Situational Awareness Scoring System in Cyber Range Platforms / A. Damianou, M. S. Mazi, G. Rizos, A. Voulgaridis, K. Votis // 2024 IEEE International Conference on Cyber Security and Resilience (CSR). 2024. DOI: 10.1109/CSR61664.2024.10679451.

[9] Kiely M. Exploring the Efficacy of Multi-Agent Reinforcement Learning for Autonomous Cyber Defence: A CAGE Challenge 4 Perspective / M. Kiely та ін. // Proceedings of the AAAI Conference on Artificial Intelligence. 2025. Vol. 39, No. 28. P. 28907–28913. DOI: 10.1609/aaai.v39i28.35158.

[10] Singh A. V. Hierarchical Multi-agent Reinforcement Learning for Cyber Network Defense / A. V. Singh, E. Rathbun, E. Graham, L. Oakley та ін. // Reinforcement Learning Journal. 2025.

**УДК 004.056:378.147**

***Delembovskyi M., Gnatyuk S., Korniichuk B. Fundamental principles for the design and application of cyber ranges for training cybersecurity specialists***

***Abstract.*** *This paper presents a comprehensive analysis of the fundamental principles for designing and applying cyber ranges as controlled learning and research environments for developing professional cybersecurity competencies. The evolution from static virtual labs to scalable cloud-based ecosystems and digital twins is outlined, emphasizing realistic network topologies, business services, and user behavior modeling. The study substantiates the need to combine technological automation with instructional design, including Bloom's taxonomy and Kolb's experiential learning cycle, and to align training outcomes with the NICE Workforce Framework. Particular attention is given to scenario lifecycle management, reproducibility through Infrastructure as Code and "scenario as code", and objective performance assessment using learning analytics and situational awareness metrics. The paper also discusses the role of AI-driven automation, including agentic RAG approaches and multi-agent reinforcement learning, for adaptive scenario generation and dynamic adversary modeling, while highlighting the importance of verification and controlled use in training settings.*

***Keywords:*** *cyber range; cybersecurity training; NICE Framework; Bloom's taxonomy; Kolb's cycle; Infrastructure as Code; scenario as code; digital twins; situational awareness; learning analytics; SIEM/SOAR; agentic RAG; multi-agent reinforcement learning; Purple Team.*

**Делембовський Максим Михайлович**, кандидат технічних наук, доцент, завідувач кафедри кібербезпеки та комп'ютерної інженерії, Київський національний університет будівництва і архітектури, Україна.
**Delembovskyi Maksym,** PhD (Engineering), Associate Professor, Head of the Department of Cybersecurity and Computer Engineering, Kyiv National University of Construction and Architecture, Ukraine.

**Гнатюк Сергій Олександрович**, доктор технічних наук, професор, проректор з наукових досліджень та трансферу технологій Державного університету «Київський авіаційний інститут».
**Gnatyuk Sergiy,** Doctor of Technical Sciences, Professor, Vice-Rector for Research and Technology Transfer at State University «Kyiv Aviation Institute».

**Корнійчук Борис Валерійович**, кандидат технічних наук, доцент, доцент кафедри професійної освіти, Київський національний університет будівництва і архітектури, Україна.
**Korniichuk Borys**, PhD (Engineering), Associate Professor, Associate Professor of the Department of Vocational Education, Kyiv National University of Construction and Architecture, Ukraine.