МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “НАПРЯМИ Й ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ СИМУЛЯЦІЙНИХ МЕТОДІВ У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ”

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Вадим ЯРМОЛЕНКО

(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ-61

Керівник:
к. держ. упр., доц. Тетяна МУЖАНОВА

Рецензент:

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра Управління кібербезпекою та захистом інформації
Ступінь вищої освіти магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедрою УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____” _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Студенту Ярмоленку Вадиму Ярославовичу

Тема кваліфікаційної роботи: «Напрями й перспективи застосування симуляційних методів у забезпеченні кібербезпеки»

керівник кваліфікаційної роботи Тетяна МУЖАНОВА, к.держ.упр., доц.

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “30” жовтня 2025 р. №467.

1. Строк подання кваліфікаційної роботи “25” грудня 2025 р.
2. Вихідні дані до кваліфікаційної роботи: забезпечення кібербезпеки, симуляційні технології
3. Перелік питань, які потрібно розробити:
   1. Дослідити теоретичні основи застосування симуляційних технологій у кібербезпеці.
   2. Проаналізувати технології та засоби створення симуляційних середовищ, які використовуються в ІКС для забезпечення кібербезпеки.
   3. Встановити особливості впровадження та перспективи розвитку симуляційних систем.
4. Перелік ілюстративного матеріалу: презентація
5. Дата видачі завдання “02” жовтня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2025	
2.	Збір та аналіз літератури.	23.10.2025	
3.	Дослідження теоретичних основ застосування симуляційних технологій у кібербезпеці.	27.10.2025	
4.	Аналіз технологій та засобів створення симуляційних середовищ.	10.11.2025	
5.	Встановлення особливостей впровадження та перспектив розвитку симуляційних систем.	15.11.2025	
6.	Формулювання висновків за результатами дослідження.	22.11.2025	
7.	Оформлення роботи.	04.12.2025	
8.	Оформлення презентації.	14.12.2025	
9.	Отримання рецензії на роботу.	18.12.2025	
10.	Захист в ЕК.	__.01.2026	

Здобувач вищої освіти _____ Вадим ЯРМОЛЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Тетяна МУЖАНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Ярмоленко В.Я. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека та захист інформації
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Напрями й перспективи застосування симуляційних методів у забезпеченні кібербезпеки"
Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач **ЯРМОЛЕНКО Вадим** у кваліфікаційній роботі проаналізував теоретичні аспекти симуляційних технологій в кібербезпеці, дослідив методи та засоби симуляційних технологій в кібербезпеці, а також дослідив практичне впровадження симуляційних технологій для кібербезпеки організації та напрямки їх розвитку.

ЯРМОЛЕНКО Вадим показав достатню теоретичну і практичну підготовку, володіння науково-дослідницькими методами, вміння самостійно знаходити шляхи вирішення проблеми дослідження. Результати дослідження апробовані на конференції "Стратегії кіберстійкості: управління ризиками та безперервність бізнесу" 27 лютого 2025 року.

Все це дозволяє оцінити кваліфікаційну роботу здобувача **ЯРМОЛЕНКА Вадима** на позитивну оцінку та присвоїти йому кваліфікацію "Магістр з кібербезпеки та захисту інформації за освітньо-професійною програмою Управління інформаційною та кібернетичною безпекою".

Керівник кваліфікаційної роботи _____ Тетяна МУЖАНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Ярмоленко В.Я. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри управління
кібербезпекою та захистом інформації

_____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

здобувачки вищої освіти Ярмоленка Вадима Ярославовича
на тему "Напрями й перспективи застосування симуляційних методів у забезпеченні кібербезпеки "

Актуальність Сучасна парадигма забезпечення інформаційної та кібербезпеки переживає фундаментальну трансформацію, зумовлену зміною характеру кіберзагроз. Тому традиційні моделі безпеки, що спираються виключно на превентивні механізми та сигнатурну детекцію, виявляють свою неефективність перед обличчям сучасних загроз. Це спонукає наукову та професійну спільноту до зміни парадигми на користь динамічних стратегій захисту та проактивної верифікації інфраструктури. Ключовим інструментом у цьому процесі стають симуляційні технології, які дозволяють проводити емпіричні дослідження складних телекомунікаційних систем, не створюючи ризиків для їхньої стабільності та доступності.

Позитивні сторони

1. У роботі здійснено комплексне дослідження теоретико-методологічних засад застосування симуляційних технологій у сфері кібербезпеки. Проведено аналіз та розмежування понять «віртуалізація», «емуляція» та «симуляція. Визначено роль цих технологій у переході до проактивної моделі захисту та представлено класифікацію сучасних програмно-апаратних засобів симуляції.
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків. Автор опрацював актуальну джерельну базу, зокрема англомовні публікації.
3. За результатами дослідження запропоновано структуровану чотирифазну модель розгортання симуляційних платформ в інфраструктурі організації.

Недоліки

1. Доцільно було б приділити більше уваги аналізу економічних бар'єрів впровадження таких систем для малого та середнього бізнесу в Україні, а також детальніше розглянути практичні кейси використання вітчизняних розробок у сфері кіберполігонів.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на достатньому науково-методичному рівні і заслуговує позитивної оцінки, а здобувач Ярмоленко Вадим Ярославович заслуговує присвоєння кваліфікації "Магістр кібербезпеки за освітньо-професійною програмою "Управління інформаційною безпекою".

Рецензент: _____

підпис

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 80 стор., 13 рис., 1 табл., 60 джерел.

Метою роботи є дослідження напрямів і перспектив застосування симуляційних технологій у забезпеченні кібербезпеки, розробка практичних рекомендацій.

Об'єктом дослідження є симуляційні технології у кібербезпеці.

Предмет дослідження – засоби, методи, найкращі практики у застосуванні симуляційних технологій у кібербезпеці.

Методи дослідження. Для вирішення поставлених завдань використовуються методи системного аналізу (для класифікації технологій віртуалізації, емуляції та симуляції), порівняльного аналізу (для оцінки ефективності комерційних та Open Source рішень), теорія графів (для моделювання сценаріїв та шляхів атак), а також методи структурно-функціонального моделювання архітектури систем безпеки.

Короткий зміст роботи. Як результат у роботі проведено аналіз існуючих засобів, методів та найкращих практик у застосуванні симуляційних технологій у кібербезпеці, завдяки чому досліджено та систематизовано підходи їх використання, визначено імовірні перспективи їх розвитку.

Галузь застосування. Розроблені підходи можуть бути використані при плануванні та впроваджені симуляційних технологій у системах забезпечення кібербезпеки підприємства.

КЛЮЧОВІ СЛОВА : СИМУЛЯЦІЙНЕ МОДЕЛЮВАННЯ, BREACH AND ATTACK SIMULATION (BAS), CYBER RANGE, DECEPTION TECHNOLOGY, КІБЕРПОЛІГОН, АКТИВНИЙ ЗАХИСТ, HONEYPOT.

ABSTRACT

The text part of the qualification work for obtaining a master's degree: 80 pages, 12 figures, 1 table, 60 sources.

The purpose of the work s to research and systematize simulation technologies in ensuring cybersecurity.

Object of research is simulation technologies in cybersecurity.

Subject ***of research*** covers the tools, methods, and best practices in the application of simulation technologies in cybersecurity.

Research methods To solve the set tasks, the following methods are used: system analysis (for classifying virtualization, emulation, and simulation technologies), comparative analysis (for evaluating the effectiveness of commercial and Open Source solutions), graph theory (for modeling attack scenarios and paths), as well as structural-functional modeling methods for security system architectures.

Brief content of research. As a result, the work analyzed the main characteristics of informational conflict, including between subjects of entrepreneurial activity; the peculiarities of managing the information security of the enterprise in the conditions of information struggle are investigated, in particular, the scheme of current threats to the information security of the enterprise is presented, taking into account the specified specifics; the directions and methods of ensuring the information security of the enterprise in the process of information struggle are defined in accordance with the proposed classification of threats.

Field of research. The developed approaches can be used in the planning and implementation of simulation technologies within enterprise cybersecurity assurance systems.

KEYWORDS: SIMULATION MODELING, BREACH AND ATTACK SIMULATION (BAS), CYBER RANGE, DECEPTION TECHNOLOGY, ACTIVE DEFENSE, HONEYPOT.

ЗМІСТ

ВСТУП

Сучасний ландшафт кібербезпеки характеризується стрімкою еволюцією загроз та безпрецедентним зростанням їхньої складності, що робить традиційні статичні моделі захисту дедалі менш ефективними. В умовах активізації APT-угруповань та появи поліморфного шкідливого програмного забезпечення покладання виключно на превентивні механізми та сигнатурний аналіз вже не гарантує стійкості інформаційних систем. Ця ситуація зумовлює необхідність фундаментальної зміни парадигми безпеки: від пасивного реагування на інциденти до проактивного виявлення вразливостей та верифікації захищеності інфраструктури в умовах реальних сценаріїв атак.

Ключовим інструментом реалізації такого підходу виступають симуляційні технології, які дозволяють застосовувати емпіричні методи дослідження до складних систем без ризику порушення їхньої цілісності. Впровадження автоматизованих платформ симуляції атак (BAS), кіберполігонів і технологій обману (Deception Technology) забезпечує перехід до концепції доказової безпеки, де кожне архітектурне рішення перевіряється на практиці. У цій роботі досліджено напрями та перспективи застосування зазначених технологій, що дозволяють трансформувати систему кіберзахисту в керований, адаптивний процес, здатний ефективно протистояти сучасним викликам.

Мета роботи полягає у дослідженні напрямів і перспектив застосування симуляційних технологій у забезпеченні кібербезпеки, розробка практичних рекомендацій.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Дослідити теоретичні основи застосування симуляційних технологій у кібербезпеці.
2. Проаналізувати технології та засоби створення симуляційних середовищ, які використовуються в ІКС для забезпечення кібербезпеки.
3. Встановити особливості впровадження та перспективи розвитку симуляційних систем.

Об'єкт дослідження - симуляційні методи у кібербезпеці.

Предмет дослідження – засоби, методи, найкращі практики у застосуванні симуляційних технологій у кібербезпеці.

Методи дослідження. Для вирішення поставлених завдань використовуються методи системного аналізу (для класифікації технологій віртуалізації, емуляції та симуляції), порівняльного аналізу (для оцінки ефективності комерційних та Open Source рішень), теорія графів (для моделювання сценаріїв та шляхів атак), а також методи структурно-функціонального моделювання архітектури систем безпеки.

Наукова новизна одержаних результатів полягає в удосконаленні методологічного підходу до впровадження симуляційних технологій у корпоративну інфраструктуру через розробку адаптивної чотирифазної моделі, що узгоджує технічні засоби з бізнес-процесами організації.

Практичне значення одержаних результатів полягає у розробленні підходу що може бути використані при плануванні та впроваджені симуляційних технологій у системах забезпечення кібербезпеки підприємства.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ЗАСТОСУВАННЯ СИМУЛЯЦІЙНИХ МЕТОДИ У КІБЕРБЕЗПЕЦІ

Сучасна парадигма забезпечення інформаційної та кібербезпеки переживає фундаментальну трансформацію, зумовлену зміною характеру кіберзагроз. Ландшафт кібербезпеки характеризується безпрецедентною складністю та динамічністю, що зумовлено стрімким розвитком технологій, глобалізацією цифрових систем і швидким зростанням кількості та різноманітності кіберзагроз [1–2]. Еволюціонувало шкідливе програмне забезпечення, з’явились автоматизовані ботнети та розвинулись APT-групи (Advanced Persistent Threats), так зокрема в Україні протягом 2025 року Національна команда реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA фіксує в середньому близько 15 кіберінцидентів на день та відслідковує понад 150 кластерів кіберзагроз (UAC). Основним джерелом кібератак залишається російська федерація. Окрім цього, спостерігається активність з Білорусі, Китаю, КНДР та з боку груп, що діють з тимчасово окупованих територій України [3].

Це призвело до того, що статичні моделі захисту, які базуються виключно на превентивних заходах та сигнатурному аналізі, демонструють недостатню стійкість [4]. У науковій спільноті та серед практиків галузі формується консенсус щодо необхідності переходу до динамічних методів захисту та проактивного тестування інфраструктури. Фундаментом цього підходу виступають симуляційні технології, які дозволяють застосовувати емпіричні методи дослідження до складних інформаційно-телекомунікаційних систем без ризику порушення їхньої цілісності чи доступності.

Теоретичні основи застосування симуляції в кібербезпеці базуються на принципах системного аналізу та математичного моделювання, що дозволяє формалізувати складні процеси інформаційного протиборства. У даному контексті кіберзахист розглядається не як набір статичних налаштувань, а як

безперервна динамічна взаємодія між системою захисту та зовнішніми загрозами, параметри яких описуються через «модель порушника». Ця абстракція дозволяє систематизувати уявлення про потенційного зловмисника, його цілі та інструментарій, трансформуючи невизначеність реальних атак у структуровані сценарії для моделювання [7]. Поєднання такого сценарного підходу з технологіями віртуалізації, емуляції та симуляції забезпечує створення контрольованого середовища, де стає можливою безпечна верифікація політик безпеки та проведення кібернавчань на базі інфраструктури кіберполігонів (Cyber Range exercises) [8]. Однак, ефективна імплементація цих механізмів вимагає чіткого понятійного апарату та глибокого розуміння архітектурних і прикладних відмінностей між різними видами моделювання.

У даному розділі здійснено комплексний аналіз теоретико-методологічних засад використання симуляційних технологій. Структура розділу підпорядкована логіці наукового пізнання: від визначення базових категорій та класифікації технологій (підрозділ 1.1) до аналізу їхньої функціональної ролі у процесах виявлення та протидії загрозам (підрозділ 1.2). Окрему увагу приділено нормативно-правовому аспекту (підрозділ 1.3), оскільки легітимізація проведення симуляційних атак (Pentesting, Red Teaming) вимагає суворої відповідності міжнародним стандартам серії ISO/IEC 27000, NIST SP 800 та національному законодавству. Метою розділу є формування цілісного уявлення про місце симуляційних технологій у сучасній архітектурі кібербезпеки.

1.1 Поняття та класифікація симуляційних методів (симуляція, емуляція, віртуалізація)

У сучасній фаховій літературі з питань інформаційної безпеки та комп'ютерної інженерії термінологічний апарат, що описує створення штучних обчислювальних середовищ, вимагає чіткої формалізації. Поняття «симуляція», «емуляція» та «віртуалізація» базуються на різних рівнях абстракції та мають відмінне цільове призначення, що унеможливлює їх синонімічне вживання при проектуванні архітектури систем захисту.

Для систематизації цих технологій у науковій практиці застосовується таксономічний підхід, що базується на критеріях рівня віртуалізації (рівень інструкцій, апаратного забезпечення або високорівневої мови) та ступеня ізоморфізму — відповідності між гостьовою та хостовою системами. Згідно з цим підходом виділяють три базові категорії:

Віртуалізація — забезпечує логічне розділення ресурсів однієї апаратної платформи між декількома ізольованими середовищами, при цьому зберігається нативна архітектура набору інструкцій (ISA — Instruction Set Architecture).

Емуляція — передбачає повну програмну інтерпретацію інструкцій однієї архітектури на іншій, що забезпечує крос-платформну сумісність, але супроводжується значними накладними витратами обчислювальних ресурсів.

Симуляція моделює поведінку системи на високому рівні абстракції, фокусуючись на статистичних характеристиках та реакціях на зовнішні події, а не на точному відтворенні внутрішніх станів компонентів.

Така диференціація є визначальною для сфери кібербезпеки: віртуалізація формує інфраструктурний базис для ізольованого виконання коду («пісочниці»), емуляція є необхідною для аналізу шкідливого ПЗ несумісних архітектур (наприклад, IoT-пристроїв), а симуляція виступає інструментом для побудови кіберполігонів та сценарного моделювання атак.

Віртуалізація (Virtualization) виступає фундаментальним інфраструктурним шаром для розгортання сучасних екосистем безпеки. У технічному розумінні це процес створення рівня абстракції, що відокремлює логічні операційні системи від фізичного обладнання, дозволяючи консолідувати обчислювальні потужності.

У процесі визначення сутності віртуалізації її часто помилково ототожнюють із симуляцією або емуляцією. Хоча віртуалізація має спільні риси з обома технологіями, вона залишається самостійним поняттям. Розуміння взаємозв'язку між цими категоріями ускладнюється тим, що віртуалізація, подібно до симуляції, передбачає імітацію поведінки фізичного аналога. Симуляцію визначають як імітацію операцій або функцій однієї системи засобами іншої; вона спирається на модель або віртуальне представлення, щоб відтворити поведінку реального об'єкта. Віртуалізація ж функціонує інакше. Хоча ця технологія забезпечує роботу віртуальних копій серверів, вона не обмежується створенням поведінкової моделі. Головна відмінність полягає в тому, що симуляція створює віртуальний образ, який лише наслідує дії реальної системи, тоді як віртуалізація перетворює сервер на віртуальний екземпляр, який функціонально є самим реальним об'єктом, а не просто його імітацією

Історичний розвиток технології віртуалізації пов’язаний з епохою мейнфреймів 1960-х років, коли виникла потреба у розділенні машинного часу. Корпорація IBM заклала основи апаратного розділення ресурсів. Після тривалого періоду стагнації у 1980–90-х роках, зумовленого домінуванням персональних комп'ютерів з однозадачними операційними системами, наприкінці 1990-х років відбувся «ренесанс віртуалізації». Впровадження технологій бінарної трансляції для архітектури x86 (VMware), а згодом — інтеграція наборів інструкцій для апаратної підтримки гіпервізорів провідними виробниками процесорів (Intel VT-x, AMD-V), дозволили мінімізувати втрати продуктивності та зробити віртуалізацію загальнодоступним стандартом.

Центральним елементом системи віртуалізації є монітор віртуальних машин (VMM), або гіпервізор. Загальноприйнята класифікація виділяє два

основні типи гіпервізорів. («Bare-metal»): Інсталюється безпосередньо на апаратне забезпечення без проміжної операційної системи. Цей тип забезпечує найвищий рівень ізоляції та продуктивності, що робить його стандартом для розгортання промислових кіберполігонів та хмарних середовищ. Тип 2 («Hosted»): Функціонує як прикладне програмне забезпечення поверх хостової операційної системи. Цей тип найчастіше використовується аналітиками кібербезпеки для локального розгортання лабораторних стендів та безпечного дослідження зразків шкідливого коду.

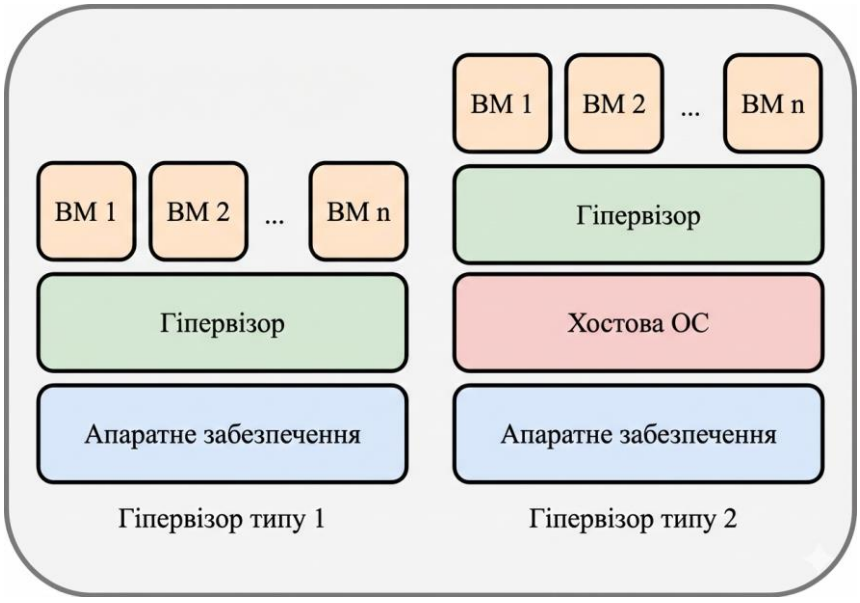

Рис. 1.1. Порівняння структур гіпервізорів 1 та 2 типу

Функціональне значення віртуалізації в сучасній екосистемі кібербезпеки є багатовекторним і реалізується через низку критичних механізмів, які трансформують статичну інфраструктуру в динамічне середовище, здатне до миттєвого відновлення після інцидентів та безпечного моделювання деструктивних впливів:

- Ізоляція середовища (Sandboxing): Локалізація підозрілих процесів у віртуальному контейнері запобігає компрометації основної інфраструктури, що є ключовим для систем динамічного аналізу (Malware Detonation).

- Керування станом системи (Snapshoting): Можливість створення миттєвих знімків пам'яті та дискового простору дозволяє дослідникам циклічно відтворювати інциденти, повертаючи систему до еталонного стану після інфікування за лічені секунди.
- Віртуалізація мережевих функцій (NFV): Технологія дозволяє динамічно розгортати віртуальні засоби захисту (брандмауери, IDS/IPS) для кожного окремого сегмента мережі, реалізуючи концепцію мікросегментації.

Окремим вектором розвитку є контейнерна віртуалізація, яка використовує спільне ядро операційної системи. Це знижує рівень ізоляції порівняно з апаратною віртуалізацією, проте дозволяє масштабувати симуляційні сценарії зі значно меншими витратами ресурсів, що є актуальним зокрема для моделювання масованих DDoS-атак.

Наступною ланкою в ієрархії технологій створення штучних середовищ є емуляція, яка, на відміну від віртуалізації, вирішує завдання відтворення функціональності однієї обчислювальної системи засобами іншої без вимоги до відповідності апаратних архітектур. Фундаментальною відмінністю емуляції є відсутність прямого виконання коду на фізичному процесорі; натомість застосовується механізм динамічної бінарної трансляції або повної програмної інтерпретації інструкцій (рис. 1.2) [9]. Це дозволяє гостьовій системі, скомпільованій для одного типу процесора (наприклад, ARM або MIPS), функціонувати на хост-системі з архітектурою x86/x64. Хоча такий підхід супроводжується значними накладними витратами обчислювальних ресурсів і зниженням швидкодії, він забезпечує найвищий рівень гнучкості та сумісності, що є критичним для специфічних завдань.

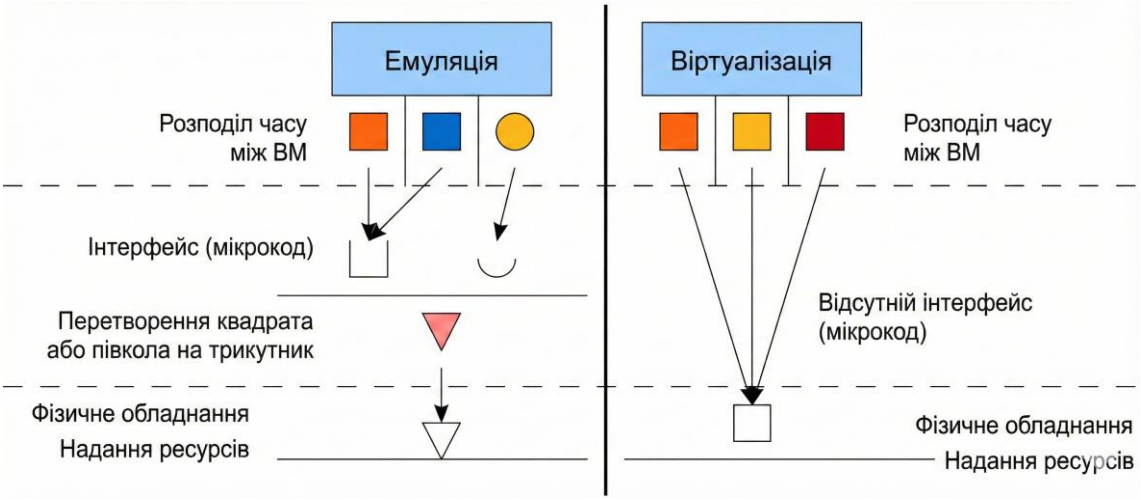

Рис. 1.2. Порівняння емуляції та віртуалізації

Фундаментальною властивістю технології віртуалізації є забезпечення високого рівня гнучкості при розподілі апаратних ресурсів, що дозволяє абстрагувати логічні обчислювальні одиниці від фізичного обладнання. Ця архітектурна особливість уможливлює динамічне масштабування окремих систем (вертикальне масштабування) шляхом зміни виділених квот CPU та RAM без зупинки сервісів. Проте, для реалізації глобального горизонтального масштабування та управління інфраструктурою рівня підприємства, можливостей окремого гіпервізора недостатньо — необхідне впровадження рівня оркестрації. Яскравим прикладом такого рішення є платформа VMware vSphere, яка дозволяє консолідувати розрізнені фізичні сервери (ESXi-хости) в єдині логічні кластери ресурсів. Засобами оркестратора забезпечується автоматизований розподіл навантаження (DRS), відмовостійкість (High Availability) та централізоване управління віртуальними мережами, що трансформує набір серверів у гнучку хмарну інфраструктуру, здатну адаптуватися до змінних потреб у сервісах в реальному часі.

У сучасній практиці кіберзахисту технологія емуляції набула стратегічного значення у сфері аналізу шкідливого програмного забезпечення для вбудованих систем та Інтернету речей (IoT). Зважаючи на гетерогенність апаратного забезпечення IoT-пристроїв, аналітики стикаються з проблемою неможливості запуску їхніх мікропрограм (firmware) у стандартних пісочницях.

Застосування емуляторів, таких як QEMU (Quick Emulator), дозволяє дослідникам розгортати віртуалізовані копії маршрутизаторів, IP-камер чи промислових контролерів без наявності фізичного обладнання. Це надає можливість проводити динамічний аналіз коду, досліджувати мережеву активність ботнетів та виявляти вразливості у прошивках у контрольованому, ізольованому середовищі [5]. Крім того, емуляція використовується для відтворення застарілих (legacy) систем, підтримка яких припинена виробником, але які залишаються критичними для бізнес-процесів, що дозволяє інтегрувати сучасні засоби захисту в застарілу інфраструктуру.

Третім, якісно відмінним компонентом розглянутої класифікації, є технологія симуляції. Якщо емуляція прагне до точності внутрішньої структури, то симуляція фокусується на моделюванні поведінки системи та її зовнішніх реакцій на подразники. У контексті кібербезпеки цей метод дозволяє абстрагуватися від низькорівневих технічних деталей заради масштабування. Замість запуску повноцінних операційних систем для кожного вузла мережі, симулятори використовують математичні моделі для імітації мережевого трафіку, протоколів та сервісів. Це є фундаментом для побудови масштабних сценаріїв навчань з використання інфраструктури кіберполігонів (Cyber Ranges), де необхідно імітувати функціонування інфраструктури для занурення персоналу, що проходить таке тренування в умови, максимально наближені до бойових, без ризику для продуктивних систем (рис. 1.3).

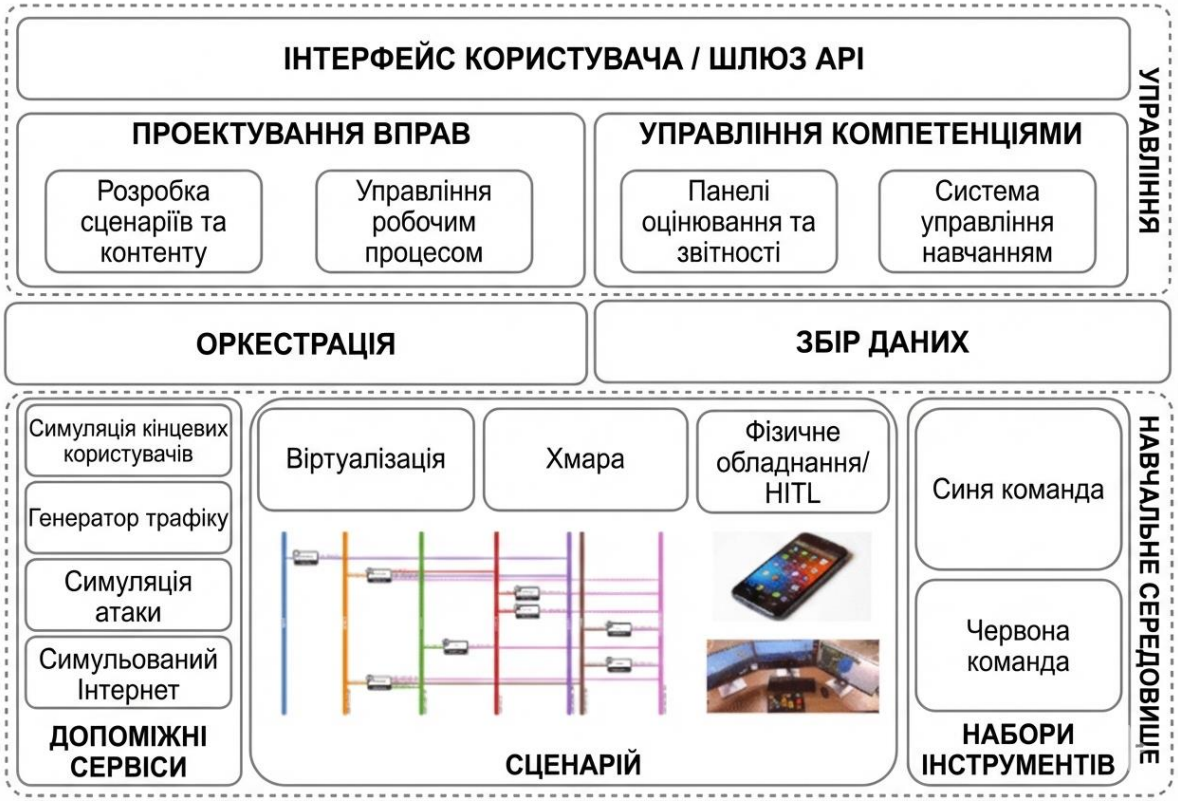

Рис. 1.3. Архітектура кіберполігону

У зв’язку з різним функціональним спрямуванням та можливостями, перелічені технології використовуються у поєднанні однієї з іншою, формуючи багатошарові екосистеми для вирішення комплексних задач кібербезпеки. У такій архітектурі віртуалізація виступає фундаментом для реалізації кіберполігонів, забезпечуючи економічно ефективну імітацію складних систем: традиційні віртуальні машини під управлінням гіпервізорів типу 1 або 2 надають необхідну гнучкість і контроль для розгортання повноцінних ОС, попри вимоги до інфраструктури, тоді як контейнеризація оптимізує ресурси для легковагових додатків, хоча й обмежена в моделюванні глибоких інфраструктурних компонентів на кшталт Active Directory [6]. Цей базис доповнюється хмарною віртуалізацією, що пропонує засоби оркестрації та динамічне масштабування через публічні, приватні або гібридні моделі. У розгорнуту віртуальну мережу інтегруються засоби емуляції, які дозволяють відтворити роботу специфічного апаратного забезпечення (наприклад, IoT-пристроїв чи маршрутизаторів з архітектурою, відмінною від x86), а завершує

цю конструкцію шар симуляції, що наповнює статичну інфраструктуру «життям» — генерує синтетичний трафік, імітує поведінку користувачів та автоматизовано відтворює сценарії кібератак.

Особливим напрямом розвитку симуляційних технологій є еволюція засобів активного захисту та введення зловмисника в оману. Історично цей напрям базувався на концепції ханіпота (Honeypot, горщик з медом, «приманка») — ізольованого ресурсу, який симулює вразливий сервіс або сервер з метою детекції спроб отримання несанкціонованого доступу (рис. 1.4). У науковій літературі прийнято розділяти їх на системи низького рівня взаємодії (Low-interaction), що імітують лише мережевий стек та відповіді окремих портів, та системи високого рівня взаємодії (High-interaction), які представляють собою реальні ОС із засобами моніторингу. Проте класичні ханіпоти мають суттєвий архітектурний недолік: вони є статичними, реактивними та локалізованими в окремих сегментах мережі, що робить їх менш ефективними проти сучасних загроз, орієнтованих на горизонтальне переміщення.

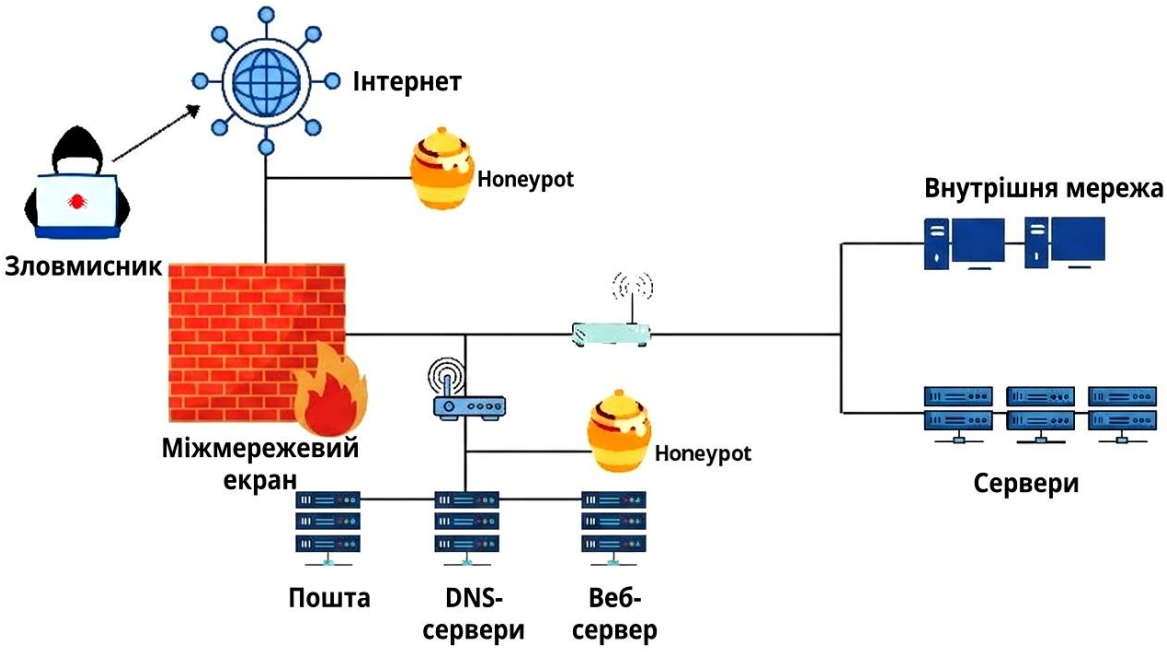

Рис. 1.4. Місце ханіпота в структурі мережі

Відповіддю на ці виклики стала поява технологій обману нового покоління — Deception Technologies. На відміну від точкових пасток, Deception-платформи реалізують концепцію «всюдисущого обману» (Ubiquitous Deception). Архітектура таких рішень передбачає автоматизоване розповсюдження на реальних робочих станціях та серверах спеціальних маркерів — «хлібних крихт» (breadcrumbs) або принад (lures). Це можуть бути фальшиві облікові дані в пам'яті lsass.exe, історія підключень RDP, збережені паролі в браузерах або ключі SSH, які ведуть до симуляційних пасток. Такий підхід трансформує мережу в мінне поле: будь-яка спроба зловмисника використати знайдені дані для розвідки чи ескалації привілеїв призводить до взаємодії з пасткою та негайного виявлення. Використання адаптивних алгоритмів дозволяє генерувати приманки, що не відрізняються від легітимних активів, роблячи середовище непрогнозованим для атакуючого та змушуючи його помилятися [10].

1.2 Роль симуляційного моделювання у виявленні та протидії кіберзагрозам

Визначення реального рівня захищеності інформаційних систем тривалий час базувалося на статичних детермінованих методиках, таких як сканування вразливостей, аудит конфігурацій та перевірка на відповідність нормативним вимогам (Compliance). Однак в умовах сучасної кібервійни, що характеризується високою динамікою зміни векторів атак та зростанням складності інструментарію зловмисників (зокрема, використання поліморфного коду), традиційні підходи демонструють критичну недостатність. Вони здатні констатувати наявність потенційної вразливості, проте не дають відповіді на питання щодо можливості її реальної експлуатації в конкретному операційному середовищі з урахуванням наявних засобів захисту. Саме в цьому контексті фундаментальну роль відіграє симуляційне моделювання, яке трансформує процес забезпечення кібербезпеки з площини теоретичних припущень у площину емпіричної верифікації та доказової безпеки.

Центральне місце у процесі проактивного виявлення загроз посідає математичне моделювання сценаріїв атак, яке реалізується через побудову графів атак (Attack Graphs) (рис. 1.5) та дерев атак (Attack Trees) (рис. 1.6). Цей підхід дозволяє формалізувати інформаційну систему у вигляді орієнтованого графа, де вершини репрезентують активи мережі та їхні стани безпеки, а ребра — можливі дії зловмисника або експлойти, що призводять до зміни стану системи. На відміну від лінійних звітів сканерів вразливостей, які розглядають кожну проблему ізольовано, графи атак дозволяють виявляти складні, багатоходові сценарії проникнення (Attack Paths). Симуляція на основі графів дозволяє змоделювати ситуацію, коли сукупність незначних вразливостей (наприклад, слабка політика паролів на тестовому сервері та непропатчена вразливість підвищення привілеїв на внутрішньому контролері домену) створює критичний вектор атаки, який неможливо виявити при покомпонентному аналізі. Застосування імовірнісних методів, зокрема

байєсівських мереж, у симуляційних моделях дозволяє розраховувати ймовірність успішної реалізації загрози для кожного вузла, пріоритезуючи заходи захисту на основі реального ризику, а не гіпотетичної тяжкості вразливості CVSS.

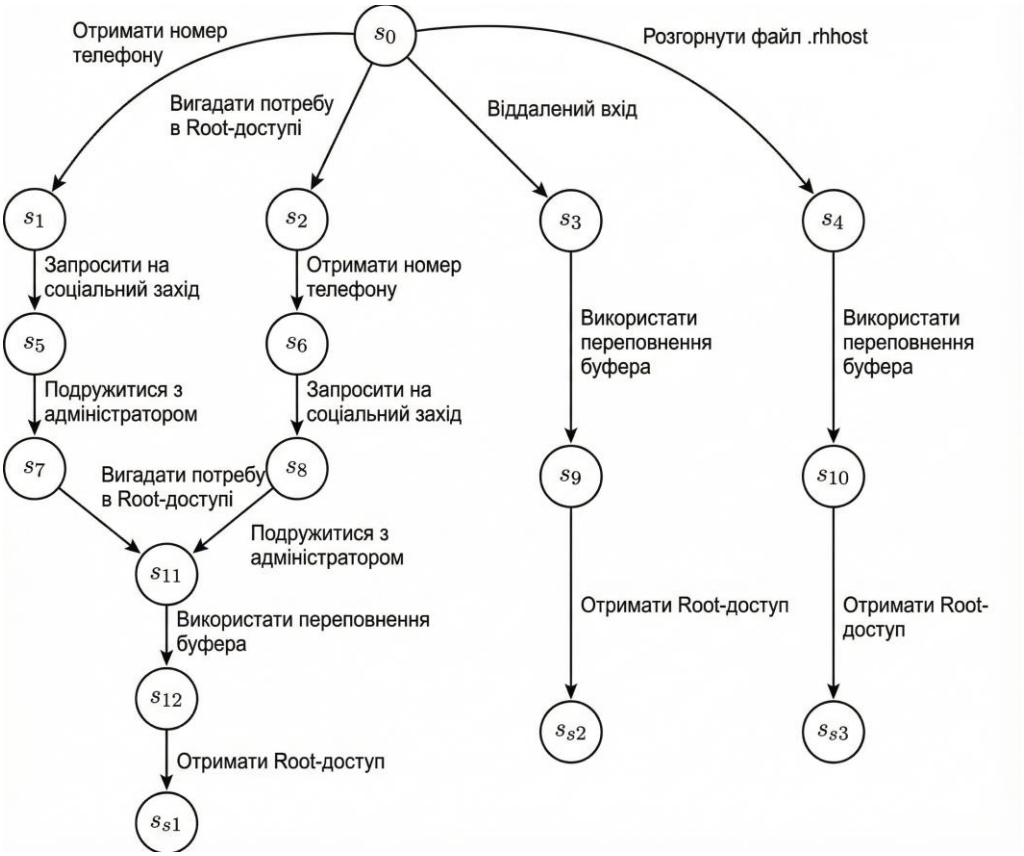

Рис. 1.5. Приклад графу атаки

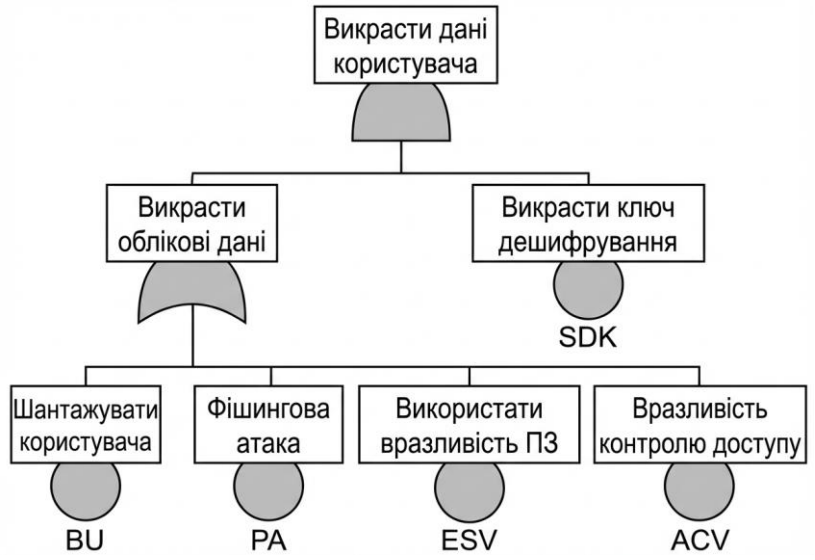

Рис. 1.6. Приклад дерева атаки

Окрім структурного моделювання мережі, симуляційні технології є безальтернативним інструментом для поведінкового аналізу невідомого програмного забезпечення. У сфері протидії та аналізу шкідливого програмного забезпечення (Malware Analysis) відбувається перехід від сигнатурного пошуку до динамічної детонації в ізольованих середовищах — «пісочницях» (Sandboxing). Сигнатурний метод виявлення ШПЗ ґрунтується на порівнянні файла, його геш-відбитку, з відомими зразками, недоліком таких систем є затримка при реакції на нові загрози. Сучасні симуляційні платформи не просто виконують підозрілий файл, а емулюють повноцінну взаємодію користувача з системою (рухи мишею, натискання клавіш, імітація мережевих затримок), щоб спровокувати шкідливе ПЗ на активні дії. Це необхідно для протидії технікам ухилення (evasion techniques), коли вірус аналізує середовище і припиняє шкідливу активність, виявивши ознаки віртуалізації. Симуляція дозволяє безпечно спостерігати за системними викликами (API calls), змінами в реєстрі та мережевою активністю зразка, формуючи його поведінковий профіль для подальшого блокування на рівні мережевих екранів та EDR-систем [11].

У сучасній парадигмі кібербезпеки платформи симуляції атак (Breach and Attack Simulation — BAS) виступають фундаментальним елементом стратегії активного захисту, дозволяючи організаціям перейти від теоретичної оцінки ризиків до емпіричної верифікації стійкості інфраструктури. Ця технологія забезпечує можливість безпечного відтворення повного життєвого циклу кібератаки (Cyber Kill Chain) у контрольованому середовищі — від початкової розвідки та доставки пейлоаду до етапів закріплення в системі, горизонтального переміщення (Lateral Movement) та ексфільтрації даних. Роль BAS полягає у проведенні автоматизованих, повторюваних «стрес-тестів» засобів захисту, що базуються на актуальних тактиках та техніках фреймворку MITRE ATT&CK. Ринок BAS-рішень пропонує диверсифікований інструментарій для вирішення цих завдань. Пропрієтарні платформи, такі як SafeBreach та AttackIQ, надають організаціям доступ до обширних бібліотек загроз та потужних аналітичних модулів, що дозволяє симулювати складні

мультивекторні атаки з мінімальними витратами часу на налаштування. Натомість, open-source фреймворки, зокрема MITRE Caldera та Atomic Red Team, забезпечують високу гнучкість та розширюваність, дозволяючи командам безпеки адаптувати сценарії під специфічну архітектуру мережі або унікальні моделі загроз [12].

Функціонування цих систем дозволяє виявити критичні «сліпі зони» в моніторингу та хибні налаштування політик блокування, які залишаються непоміченими при стандартному скануванні вразливостей. Якщо симульована атака проходить крізь периметр захисту без генерування алерту в SIEM-системі, це слугує прямим індикатором необхідності доопрацювання правил кореляції подій. Таким чином, імплементація BAS трансформує аудит безпеки з дискретної події (щорічного пентесту) на безперервний процес вдосконалення (Continuous Security Validation), надаючи командам захисту об'єктивні метрики для оптимізації протоколів реагування та пріоритезації інвестицій у засоби кібербезепеки.Ще один вектор застосування симуляційних технологій стосується підготовки даних для систем штучного інтелекту. Сучасні алгоритми виявлення аномалій (Anomaly Detection) потребують великих обсягів навчальних вибірок, що містять приклади шкідливої активності. Отримання таких даних з реальних інцидентів є складним, етично суперечливим та ризикованим завданням. Симуляційні середовища виступають генераторами синтетичних даних, створюючи терабайти трафіку з ознаками різноманітних атак — від масованих DDoS до складних ін’єкцій коду та спроб підбору паролів. Це дозволяє тренувати нейромережі на виявлення патернів поведінки зловмисників у контрольованих умовах, значно підвищуючи точність алгоритмів детекції та знижуючи рівень помилкових спрацьовувань (False Positives) у реальних умовах експлуатації [13].

Нарешті, симуляційне моделювання відіграє вирішальну роль у підготовці найбільш критичного елемента системи захисту — «людського фактору», зокрема операторів центрів моніторингу безпеки (SOC) та груп реагування на інциденти (CSIRT). Проведення кібернавчань на базі віртуальних

полігонів (Cyber Ranges) виходить за межі перевірки суто технічних навичок, дозволяючи комплексно оцінити ефективність організаційних процедур та злагодженість командної роботи. У високореалістичному середовищі полігону, яке емулює не лише атакуючі дії, а й легітимний трафік та поведінку користувачів, відтворюється психологічний тиск, невизначеність («туман війни») та жорсткі часові обмеження, притаманні реальним кризовим ситуаціям. Такий підхід дозволяє трансформувати теоретичні знання персоналу у стійкі практичні навички, виявляючи при цьому критичні недоліки в сценаріях реагування (Playbooks), вузькі місця в комунікації між підрозділами та прогалини в компетенціях аналітиків. Таким чином, інтеграція симуляційних технологій забезпечує реалізацію холістичного підходу до кібербезпеки (тріада «Люди-Процеси-Технології»), об'єднуючи прогнозування векторів атак, технічну валідацію засобів захисту та тренування персоналу в єдину, адаптивну систему оборони, здатну до самовдосконалення.

1.3 Нормативні вимоги та стандарти тестування систем захисту

Інтеграція симуляційних технологій у процеси забезпечення інформаційної безпеки вимагає суворої нормативно-правової регламентації, оскільки інструментарій, що використовується для моделювання кібератак, технічно ідентичний засобам, які застосовують реальні зловмисники. Правова природа проведення симуляційних заходів, таких як тести на проникнення (Penetration Testing) або навчання Red Teaming, базується на чіткому розмежуванні між санкціонованим аудитом безпеки та неправомірним втручанням у роботу автоматизованих систем. У міжнародній та національній практиці сформувалася багаторівнева система стандартів, яка не лише легітимізує використання симуляційних середовищ, а й визначає методологію їх проведення, критерії оцінки результатів та вимоги до кваліфікації персоналу. Перехід від формального виконання вимог (compliance) до реальної оцінки ефективності захисту через симуляцію закріплено у низці фундаментальних нормативних документів.

На рівні міжнародної стандартизації базовим документом, що регулює управління інформаційною безпекою, є сімейство стандартів ISO/IEC 27000. Зокрема, стандарт ISO/IEC 27001 (вимоги до Систем управління інформаційною безпекою – СУІБ) та ISO/IEC 27002 (практичні правила) містять контроль A.12.6.1 «Управління технічними вразливостями», який зобов’язує організації отримувати інформацію про технічні вразливості використовуваних інформаційних систем та оцінювати відповідні ризики. Однак, більш пізні редакції стандартів та доповнення до них зміщують акцент з пасивного моніторингу на активне тестування. Особливе значення має стандарт ISO/IEC 27005 «Управління ризиками інформаційної безпеки», який рекомендує використовувати сценарний підхід для оцінки ймовірності реалізації загроз. Симуляційне моделювання в цьому контексті виступає інструментом верифікації обраних сценаріїв ризику, дозволяючи емпіричним шляхом підтвердити або спростувати припущення щодо можливості

експлуатації конкретних вразливостей в інфраструктурі організації. Сімейство стандартів затверджено в українських нормативно-правових актах [15].

Найбільш деталізованим методологічним базисом для проведення технічних симуляцій є спеціальні публікації Національного інституту стандартів і технологій США (NIST). Ключовим документом у цій сфері є NIST SP 800-115 «Technical Guide to Information Security Testing and Assessment». Цей стандарт визначає таксономію методів тестування, чітко розмежовуючи сканування вразливостей, тестування на проникнення та симуляцію дій зловмисника. Згідно з NIST SP 800-115, тестування безпеки не повинно обмежуватися перевіркою конфігурацій; воно має включати активні дії з експлуатації вразливостей для визначення реального впливу на бізнес-процеси. Крім того, стандарт NIST SP 800-53 (Security and Privacy Controls) у контролі CA-8 «Penetration Testing» встановлює імперативну вимогу щодо регулярного проведення незалежних симуляційних тестів для федеральних інформаційних систем, що стало де-факто стандартом і для корпоративного сектору.

Окремий пласт нормативних вимог стосується критичної інфраструктури та фінансового сектору, де ціна кіберінциденту є однією з найвищих. У Європейському Союзі набула поширення концепція Threat-Led Penetration Testing (TLPT) — тестування на проникнення, кероване даними розвідки про загрози. Цей підхід формалізовано у фреймворку TIBER-EU (Threat Intelligence-based Ethical Red Teaming), розробленому Європейським центральним банком. TIBER-EU вимагає від фінансових установ не просто проводити абстрактні пентести, а здійснювати симуляцію атак конкретних угруповань (APT-груп), які є актуальними для даного регіону та сектору. Сценарії симуляції розробляються на основі даних Threat Intelligence, що забезпечує максимальну реалістичність навчань [14]. Аналогічні вимоги містяться у британському стандарті CBEST та гонконгському iCAST. Ці нормативні акти перетворюють симуляцію з факультативної процедури на обов'язковий елемент операційної стійкості банківської системи.

У правовому полі України питання використання симуляційних технологій регулюється Законом України «Про основні засади забезпечення кібербезпеки України» та галузевими нормативними документами Держспецзв'язку (НД ТЗІ). Зокрема, законодавство визначає необхідність проведення аудиту захищеності об'єктів критичної інфраструктури. Важливим аспектом є Постанова НБУ № 95 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України», яка зобов'язує банки проводити регулярні зовнішні та внутрішні тестування на проникнення [16]. Легалізація дій «білих хакерів» під час симуляцій забезпечується підписанням детальних угод про рівень послуг та документу «Правила взаємодії» (Rules of Engagement — RoE). Цей документ є юридичним запобіжником, що визначає межі дозволених дій, перелік заборонених векторів атак (наприклад, атаки, що можуть призвести до відмови в обслуговуванні виробничих систем) та процедури екстреного зупинення симуляції.

Таким чином, сучасна нормативна база еволюціонує в напрямку обов'язкового впровадження симуляційних практик. Стандарти вимагають переходу від статичної оцінки відповідності («паперової безпеки») до динамічної верифікації стійкості систем через контрольовані, санкціоновані кібератаки. Це створює правовий фундамент для розгортання кіберполігонів та впровадження автоматизованих систем симуляції (BAS) як невід'ємної складової стратегії корпоративної безпеки.

Висновки до розділу 1

У першому розділі роботи здійснено комплексний аналіз теоретико-методологічних засад застосування симуляційних технологій у сфері кібербезпеки. За результатами дослідження зроблено наступні узагальнення:

Трансформація парадигми захисту. Встановлено, що в умовах еволюції кіберзагроз та зростання активності APT-груп, традиційні статичні моделі безпеки втрачають ефективність. Необхідним є перехід до динамічних методів захисту («Active Defense»), фундаментом яких виступає емпірична верифікація стійкості інфраструктури засобами моделювання.

Технологічна диференціація. Проведено чітке розмежування базових категорій створення штучних середовищ. Визначено, що віртуалізація (зокрема гіпервізори 1-го та 2-го типів) формує інфраструктурний базис для ізоляції процесів; емуляція забезпечує крос-платформний аналіз шкідливого ПЗ та IoT-пристроїв; а симуляція дозволяє моделювати поведінкові аспекти складних систем. Окреслено еволюцію засобів обману від пасивних ханіпотів до комплексних платформ Deception Technology, що реалізують концепцію «всюдисущого обману».

Роль у виявленні загроз. Доведено критичну важливість впровадження систем автоматизованої симуляції атак (BAS) та використання математичних моделей (графів та дерев атак). Ці інструменти дозволяють трансформувати аудит безпеки з дискретної події на процес безперервної валідації (Continuous Security Validation), виявляючи «сліпі зони» моніторингу та верифікуючи налаштування засобів захисту вздовж усього ланцюга Cyber Kill Chain.

Людський фактор. Обґрунтовано значення симуляційних полігонів (Cyber Ranges) для підготовки кадрів. Відтворення реалістичних сценаріїв атак в умовах психологічного тиску дозволяє виявити недоліки в організаційних процедурах та підвищити кваліфікацію SOC/CSIRT команд, забезпечуючи холістичний підхід до оборони.

Нормативна обов'язковість. Аналіз міжнародних стандартів (ISO/IEC 27000, NIST SP 800) та національного законодавства засвідчив, що використання симуляційних технологій (Penetration Testing, Red Teaming) більше не є факультативним, а стає імперативною вимогою для забезпечення нормативної відповідності та реальної операційної стійкості критичних інформаційних систем.

Таким чином, симуляційні технології є невід'ємною складовою сучасної архітектури кібербезпеки, що забезпечує можливість безпечного, контрольованого та доказового дослідження захищеності інформаційно-комунікаційних систем.

РОЗДІЛ 2
МЕТОДИ ТА ЗАСОБИ СТВОРЕННЯ СИМУЛЯЦІЙНИХ СЕРЕДОВИЩ

Теоретичне обґрунтування необхідності використання симуляційних технологій, ґрунтовно викладене у попередньому розділі, знаходить своє практичне втілення у широкому спектрі спеціалізованих програмно-апаратних рішень. Сучасний ринок засобів кібербезпеки пропонує розгалужений та високотехнологічний інструментарій, що дозволяє реалізувати перехід від абстрактних моделей загроз і математичних графів атак до їхньої технічної імплементації в контрольованому цифровому середовищі. Якщо теоретичні засади відповідають на концептуальне питання «чому» необхідно проводити симуляцію для забезпечення стійкості систем, то даний технологічний розділ фокусується на інженерному питанні «як» це реалізується на рівні мережевої архітектури, протоколів взаємодії, віртуалізації ресурсів та програмного коду. Важливість цього переходу зумовлена тим, що ефективність будь-якої стратегії захисту залежить не лише від обраної методології, а й від функціональних можливостей та обмежень конкретних інструментів, що застосовуються для її реалізації.

Спектр технологій, що підлягають розгляду, є гетерогенним, проте його можна структурувати за трьома ключовими векторами, які формують комплексний ешелон симуляційного захисту. Перший вектор — це засоби активної симуляції наступальних дій (BAS — Breach and Attack Simulation). Ці платформи дозволяють автоматизувати рутинні процеси тестування на проникнення, трансформуючи їх з періодичних аудитів у безперервний процес верифікації стійкості засобів захисту (Firewalls, WAF, EDR) в режимі 24/7, використовуючи актуальні сигнатури загроз. Другий вектор стосується розгортання масштабних інфраструктурних платформ — кіберполігонів (Cyber Ranges). Вони забезпечують створення високореалістичного віртуалізованого простору, де за допомогою гіпервізорів та генераторів синтетичного трафіку емулюється повноцінна робота підприємства для проведення безпечних

досліджень та тренувань персоналу (Blue/Red Teaming). Третій вектор представлений технологіями обману (Deception Technology), які інтегрують елементи симуляції безпосередньо у продуктивне середовище. На відміну від ізольованих полігонів, ці рішення створюють ілюзорний шар інфраструктури (пастки, приманки), спрямований на детекцію зловмисників через когнітивний вплив та маніпуляцію їхнім сприйняттям цілі [22,23].

У даному розділі проведено детальний огляд, класифікацію та порівняльний аналіз технологічних рішень для створення симуляційних середовищ різного призначення. Особливу увагу приділено архітектурі систем автоматизованої симуляції зламів, принципам оркестрації ресурсів на віртуальних полігонах, а також механізмам функціонування сучасних пасток високого рівня взаємодії. Метою розділу є систематизація наявного інструментарію, визначення його тактико-технічних характеристик та формулювання критеріїв ефективності для вирішення прикладних завдань кібербезпеки в умовах сучасного ландшафту загроз.

2.1 Моделювання сценаріїв кібератак та вразливостей (Attack Simulation)

Технології симуляції порушень та атак (Breach & Attack Simulation — BAS) визначаються як клас інструментів, що дозволяють підприємствам реалізувати стратегію безперервного та послідовного моделювання повного циклу кібератаки безпосередньо проти власної інфраструктури. Функціональні можливості цих рішень охоплюють відтворення широкого спектра загроз, включаючи дії внутрішніх зловмисників (insider threats), горизонтальне переміщення мережею (lateral movement) та несанкціоновану ексфільтрацію даних. Технічна реалізація таких симуляцій здійснюється із застосуванням програмних агентів, віртуальних машин та інших спеціалізованих засобів, що дозволяє безпечно перевіряти стійкість корпоративної системи захисту в умовах, максимально наближених до реальних.

Еволюційний перехід від реактивних моделей захисту до проактивних зумовив появу окремого класу технологічних рішень — систем симуляції порушень та атак (BAS — Breach and Attack Simulation). На відміну від традиційних сканерів вразливостей, які оперують статичними даними про версії програмного забезпечення та конфігурації, технологія BAS фокусується на динамічній верифікації реальної реакції ешелонованої системи захисту на спробу несанкціонованого втручання [25-27].

Необхідність інтеграції платформ Breach and Attack Simulation (BAS) у сучасну архітектуру кібербезпеки зумовлена низкою критичних факторів, що нівелюють обмеження традиційних методів аудиту:

- Безперервність верифікації (Continuous Security Validation): Забезпечення переходу від дискретних аудитів (Point-in-Time assessment), таких як періодичні пентести, до моделі постійного тестування в режимі 24/7. Це дозволяє оперативно виявляти «дрейф безпеки» (security drift) — поступову деградацію налаштувань захисту через зміни в інфраструктурі.

- Емпірична валідація засобів захисту: Можливість на практиці перевірити реальну ефективність наявного стеку технологій (NGFW, WAF, EDR, SIEM), виявляючи критичні розбіжності між декларованими можливостями вендорів та фактичними конфігураціями в середовищі замовника.
- Орієнтованість на актуальні загрози (Threat-Centric Approach): Використання сценаріїв, синхронізованих із глобальною матрицею MITRE ATT&CK, що дозволяє оцінити резистентність організації до специфічних тактик, технік та процедур (TTPs), які використовують активні на даний момент кіберугруповання (APT).
- Оптимізація інвестицій та ресурсів: Надання об'єктивних, вимірюваних метрик для пріоритезації бюджету на кібербезпеку та підвищення ефективності роботи SOC-команд, фокусуючи їхні зусилля на усуненні підтверджених векторів атак та покращенні показників реагування (MTTD/MTTR).

Методологія BAS базується на таких етапах життєвого циклу (рис. 2.1) моделювання атаки:

- Сканування активу
- Використання активу
- Повторення попередніх кроків для іншого ресурсу

Рисунок 2.1. Життєвий цикл BAS

Архітектурна реалізація більшості комерційних BAS-платформ (зокрема, Cymulate, AttackIQ, XM Cyber) базується на гібридній клієнт-серверній моделі, що дозволяє проводити тестування розподіленої інфраструктури. Структурно такі системи складаються з двох ключових компонентів:

- Центр управління та аналітики (C2 Server/Management Console): Забезпечує оркестрацію сценаріїв, вибір векторів атак (наприклад, Email Gateway, Web Gateway, Endpoint) та консолідацію звітів.
- Агенти симуляції (Simulation Agents): Легковагові програмні модулі або віртуальні сутності, що розгортаються у критичних сегментах мережі (User VLAN, Server Farm, DMZ). Вони виконують роль як умовного «атакуючого», так і «жертви».

Фундаментальною відмінністю BAS від інструментів для реальних кібератак є дотримання принципу «безпечного виконання» (Safe-by-design) [30-31]. Агенти не здійснюють деструктивних дій, таких як незворотне шифрування даних чи ексфільтрація конфіденційної інформації. Механізм симуляції базується на обміні між агентами спеціально маркованим трафіком, який містить сигнатури відомих експлойтів, пейлоадів шкідливого ПЗ або патерни команд управління ботнетами (C&C traffic). Метою такої взаємодії є емпірична перевірка налаштувань засобів безпеки: якщо агент-отримувач успішно

декомпілює та зберігає файл із сигнатурою WannaCry без реакції з боку антивірусу або EDR-системи, BAS фіксує «сліпу зону» в захисті.

Функціонування сучасних засобів симуляції базується на інтеграції з глобальними базами знань про кіберзагрози, де стандартом де-факто виступає матриця MITRE ATT&CK. Використання цього фреймворку дозволяє структурувати симуляцію не як хаотичний набір тестів, а як логічно пов'язаний ланцюжок тактик і технік (TTPs — Tactics, Techniques, and Procedures). Це уможливлює перехід до моделювання поведінки конкретних загроз (Threat-Centric Approach): організації можуть автоматично запускати сценарії (Playbooks), що емулюють дії специфічних APT-груп, актуальних для їхнього сектору, перевіряючи стійкість проти автентичних методів закріплення та бічного переміщення [32,36].

Окремий сегмент в екосистемі займають інструменти емуляції супротивника з відкритим кодом (Open Source Adversary Emulation), які надають гнучкість для кастомізації сценаріїв внутрішніми командами, які імітують хакерські атаки (Red Team):

- MITRE CALDERA: Фреймворк, побудований на базі інтелектуального автоматизованого планувальника. Система не просто виконує скрипти, а динамічно обирає наступний крок атаки залежно від успіху попереднього, моделюючи поведінку адаптивного супротивника, який змінює тактику при зустрічі з перешкодами.
- Atomic Red Team: Бібліотека «атомарних» тестів, прив'язаних до конкретних технік MITRE. Кожен тест є ізольованим скриптом, що імітує окрему шкідливу дію (наприклад, дамп облікових записів). Це дозволяє реалізувати концепцію модульного тестування (Unit Testing) для SIEM-систем, швидко перевіряючи, чи генеруються сповіщення на конкретні аномалії.

У сукупності, розглянуті технології трансформують методологію валідації безпеки, забезпечуючи фундаментальний перехід від дискретного аудиту до безперервного циклу покращення захищеності. Впровадження BAS-

платформ та інструментів емуляції супротивника дозволяє замінити статичні перевірки на динамічну верифікацію стійкості інфраструктури в режимі 24/7, базуючись на актуальних даних про поведінку кіберзлочинців (Threat Intelligence). Такий підхід не лише автоматизує рутинні процеси тестування, але й надає можливість емпірично оцінити реальну ефективність налаштувань засобів захисту проти тактик матриці MITRE ATT&CK, перетворюючи кібербезпеку з «чорної скриньки» на прозорий процес із вимірюваними показниками ефективності та чітким розумінням залишкових ризиків [54,57,59].

2.2 Огляд програмно-апаратних платформ для розгортання кіберполігонів (Cyber Ranges)

Симуляція може ефективно використовуватися для розуміння природи атак та відпрацювання різноманітних сценаріїв. З цією метою на національному та інституційному рівнях створено спеціальні підрозділи для проведення навчань і тренувань із кібербезпеки. Наприклад, Міністерство внутрішньої безпеки США заснувало Національну програму кібернавчань та планування для підтримки планів реагування на інциденти за допомогою стратегічних тренувань. Аналогічні функції виконує Національний центр кібербезпеки Великої Британії. Об'єднаний центр передових технологій з кібербезпеки НАТО відповідає за організацію спільних навчань, що охоплюють як технічні, так і стратегічні аспекти кібербезпеки.

Зазначені установи організовують багато відомих навчальних заходів, які включають елементи симуляції. Штабні кібернавчання (tabletop exercise) під назвою Waking Shark II залучили близько 220 учасників з урядових установ, банків та фінансових організацій Великої Британії. У ході навчань моделювався збій на оптовому ринку з метою аналізу наслідків кібератак та відпрацювання каналів комунікації між компаніями. Міністерство внутрішньої безпеки США з 2006 року проводить аналогічні, але більш масштабні навчання під назвою Cyber Storm. Згідно з офіційним звітом, у останньому заході (Cyber Storm VI) взяло участь широке коло представників федеральних, регіональних та місцевих органів влади, а також приватного сектору. Метою навчань заявлено підвищення готовності до кіберзагроз та вдосконалення процедур реагування для оновлення відповідних планів. До прикладу, НАТО проводить кібернавчання Locked Shields (CCDCOE, 2019) щорічно, починаючи з 2010 року. У Locked Shields сині команди повинні захищати задану (емульовану) ІКТ-інфраструктуру від атак, організованих червоною командою. Емульовані ІКТ-інфраструктури, що використовуються в Locked Shields, складаються

приблизно з чотирьох тисяч віртуалізованих систем та виконуються у спеціальному кіберполігоні [22,23].

Такі масштабні гіпотетичні сценарії забезпечують учасникам цінний навчальний досвід. Проте організація зборів такої кількості людей часто є складною, а подібні масштабні заходи не підходять для багатьох підприємств малого та середнього бізнесу. Інструменти для самостійного навчання є критично важливими для заповнення цієї прогалини. Британський інструмент «Exercise in a Box» є чудовим прикладом вирішення цієї потреби. Він фокусується на організаційних практиках реагування на гіпотетичні кіберінциденти [39].

Альтернативним методом навчання є ігрові симуляції. Сучасні навчальні ігри включають CyberProtect, що використовується Міністерством оборони США, та CyberCIEGE, що застосовується ВМС США. Такі ігрові тренування зосереджені на забезпеченні інформаційної безпеки та розумінні причинно-наслідкових зв'язків. Існують також системи, що забезпечують навчання через змагання. Університет Каліфорнії в Санта-Барбарі проводить міжнародні змагання Capture the Flag (iCTF), а Інститут SANS організовує NetWars, що надає дослідникам можливість вивчати поведінку атак у безпечному середовищі. Платформа CyberNEXS використовується для проведення змагань із кіберзахисту. Змагання iCTF орієнтовані переважно на студентів університетів, хоча участь не обмежується лише ними. NetWars та CyberNEXS залучають також учнів старших класів. Навчання та залучення якомога ширшої аудиторії до питань кіберобізнаності та безпеки є метою Національної ініціативи США з освіти в галузі кібербезпеки. Симуляції та змагання слугують підтримкою для таких важливих ініціатив.

Критично важливим аспектом функціонування кіберполігону є забезпечення реалістичності мережевої взаємодії, що досягається шляхом сегментації інфраструктури на функціональні зони. Стандартна топологія полігону передбачає наявність «Синьої зони» (Blue Zone), яка імітує корпоративну мережу об'єкта захисту з типовими сервісами (Active Directory,

поштові сервери, бази даних, SCADA-системи [44]), та «Червоної зони» (Red Zone), звідки здійснюється атака. Проте, ключовим елементом, що відрізняє професійний полігон від статичного макета, є «Сіра зона» (Gray Zone) або імітація Інтернету. У цій зоні розгортаються емулятори зовнішніх DNS-серверів, соціальних мереж, новинних порталів та репозиторіїв коду. Це дозволяє реалізувати сценарії OSINT (розвідки на основі відкритих джерел) та атак типу Drive-by, коли інфікування відбувається через відвідування скомпрометованого веб-ресурсу. Для керування розгортанням цих складних топологій широко застосовуються підходи «Інфраструктура як код» (IaC), зокрема інструменти Terraform та Ansible, які дозволяють розгортати ідентичні копії тренувальних середовищ за лічені хвилини [39-43].

Окремим технологічним викликом при створенні симуляційного середовища є наповнення його синтетичним трафіком, оскільки «тиха» мережа є аномальною і дозволяє захисникам занадто легко виявляти дії атакуючих. Для створення фонового шуму (Background Noise) використовуються промислові генератори трафіку, такі як Cisco TRex, Ostinato або Ixia. Ці інструменти здатні генерувати гігабіти легітимного трафіку (HTTP, SMTP, SQL-запити), що емулює роботу тисяч віртуальних користувачів. Більш просунуті системи використовують ботів, що імітують поведінку людини: відкривають файли, переглядають веб-сторінки, вводять логіни та паролі. Це створює ефект «туману війни», змушуючи команди захисту (Blue Teams) шукати ознаки атаки серед масиву легітимних подій, відсіюючи хибні спрацювання (False Positives) [45].

На ринку платформ для розгортання кіберполігонів спостерігається поділ на рішення для мережевого моделювання та комплексні тренувальні системи. До першої групи належать емулятори GNS3 та EVE-NG (Emulated Virtual Environment Next Generation). Ці платформи дозволяють завантажувати реальні образи мережевого обладнання (Cisco, Juniper, Palo Alto) та будувати складні маршрутизовані мережі. Вони є стандартом де-факто для підготовки мережевих інженерів, проте мають обмежені можливості щодо гейміфікації процесу та

автоматичного підрахунку балів (Scoring). Для масового навчання персоналу та проведення змагань (CTF) використовуються платформи контейнерної віртуалізації (на базі Docker/Kubernetes) або спеціалізовані комерційні рішення (наприклад, Cyberbit Range, Silensec), які надають готовий інтерфейс для моніторингу прогресу учасників, автоматизованого запуску сценаріїв атак та формування звітів за результатами навчань [46,47]. Вибір конкретної платформи залежить від цільового призначення полігону: для глибокого дослідження мережевих протоколів доцільніше використовувати EVE-NG, тоді як для відпрацювання злагодженості дій SOC-команд необхідні потужності хмарних оркестраторів.

У сучасній практиці розгортання тренувальних середовищ виділяють два основні підходи до архітектурної реалізації кіберполігонів. Перший полягає у використанні готових комерційних платформ класу «під ключ» (Turnkey solutions), які пропонують інтегровану екосистему з автоматизованою системою оцінювання, професійною техпідтримкою та бібліотеками попередньо розроблених сценаріїв, що дозволяє мінімізувати час на введення в експлуатацію. Альтернативним вектором є побудова кастомізованих рішень на базі інструментарію з відкритим вихідним кодом (Open Source). Такий підхід, хоч і вимагає значної експертизи для інтеграції розрізнених компонентів віртуалізації та оркестрації, забезпечує повну відсутність ліцензійних витрат та надає архітекторам системи необмежену гнучкість у моделюванні специфічних інфраструктурних топологій, які не завжди доступні у пропрієтарних продуктах.

Практична реалізація концепції симуляційного навчання вимагає розгортання спеціалізованих програмно-апаратних комплексів — кіберполігонів (Cyber Ranges), які забезпечують створення високореалістичних віртуальних середовищ. На відміну від простих лабораторних стендів, кіберполігон є складною екосистемою, що інтегрує засоби віртуалізації, оркестрації ресурсів, генерації трафіку та автоматизованого оцінювання дій користувачів. Архітектурний фундамент сучасних полігонів базується на використанні гіпервізорів першого типу (KVM, VMware ESXi) та хмарних

операційних систем, таких як OpenStack. Саме OpenStack найчастіше виступає стандартом для побудови приватних хмар кіберполігонів, дозволяючи через API динамічно створювати ізольовані тенанти (проекти) для різних команд, керувати віртуальними мережами (SDN — Software Defined Networking) та забезпечувати масштабування інфраструктури до тисяч віртуальних машин. Типові архітектури таких платформ комбінують в собі засоби симуляції, емуляції та віртуалізаці [53].

Симуляція та емуляція (рішення на базі хоста) (рис. 2.2) передбачає використання моделі, віртуального екземпляра, для відтворення складного середовища на основі поведінки реальних елементів. Емуляція — це процес, коли кіберполігони функціонують на виділеній фізичній інфраструктурі. Популярними прикладами симуляції є Simulink для моделювання та аналізу багатодоменних систем; Cisco Packet Tracer (PT); Cisco Modeling Lab (CML), раніше відомий як VIRL; NS2 та NS3; а також симулятори дискретних подій OMNet++. Популярними прикладами емуляції є Mininet, GNS3, Emulab та QEMU як тестовий майданчик для мережевої емуляції.

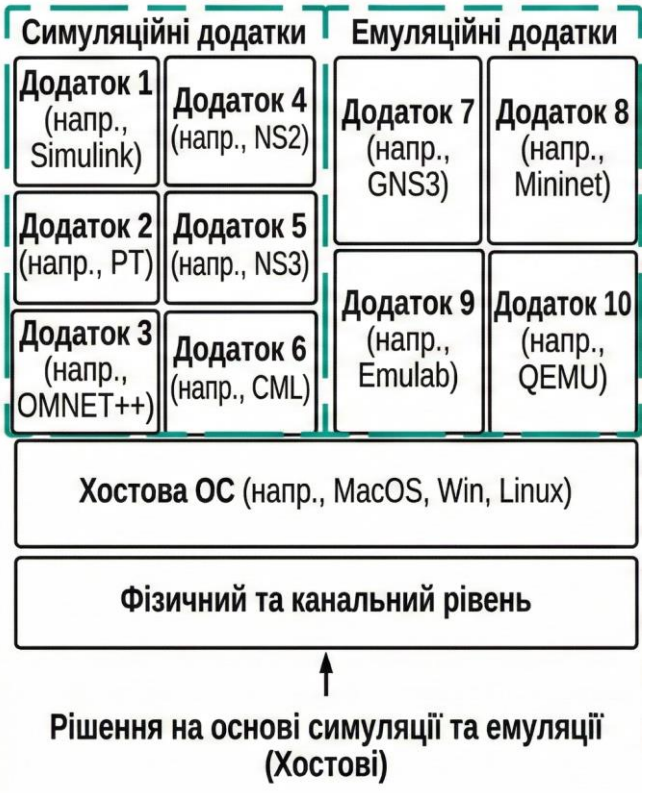

Рисунок 2.2. Структура та засоби засновані на симуляції та емуляції

Традиційна віртуалізація (рис. 2.3) досягається за допомогою віртуальних машин (ВМ) із реальною ОС [55, 56], що емулюється гіпервізором, який контролює весь доступ до базового фізичного обладнання. Існує два типи гіпервізорів :

- Тип 1 (або «bare-metal», або нативний) взаємодіє безпосередньо з базовими фізичними ресурсами, повністю замінюючи традиційну ОС (наприклад, MacOS, Windows та Linux). Популярними прикладами є VSphere, ESXi, Vagrant, Hyper-V та XenServer (нині відомий як Citrix Hypervisor);
- Тип 2 працює як додаток поверх існуючої ОС (MacOS, Windows або Linux). Він використовується на кінцевих пристроях для запуску альтернативних ОС, при цьому для доступу та координації базових апаратних ресурсів використовується хостова ОС. Популярними прикладами є VirtualBox, Fusion та Workstation.

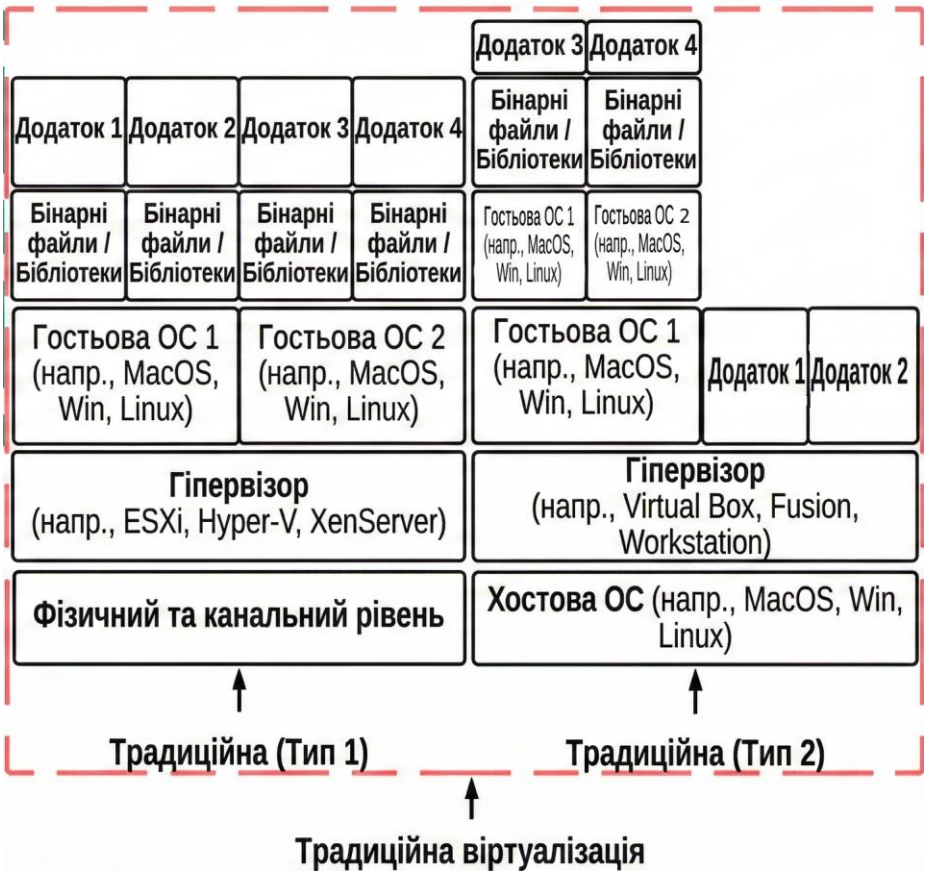

Рисунок 2.3. Структура та засоби засновані на традиційній віртуалізації

Контейнерна віртуалізація (рис. 2.4) використовує структуру контейнерів як рішення у випадках, коли виникають проблеми з традиційною віртуалізацією, такі як високі витрати на обслуговування та потреба у потужному обладнанні. Популярними прикладами є Docker, налаштований як «Платформа як послуга» (Platform as a service, PaaS); OpenStack, який може бути розгорнутий як «Інфраструктура як послуга» (Infrastructure as a service, IaaS); LXC; та OpenVZ.

Рисунок 2.4. Структура та засоби засновані на симуляції та емуляції

2.3 Технології обману зловмисників (Deception Technology) та архітектура пасток

Окремим, технологічно складним класом симуляційних рішень в екосистемі кібербезпеки є засоби активного захисту, стратегічною метою яких є зміна асиметрії кіберпротиборства на користь захисника. Якщо традиційні засоби захисту (IDS/IPS, Firewall) оперують бінарною логікою «дозволити/блокувати», то технології обману (Deception Technology) спрямовані на дезорієнтацію супротивника, збільшення часу його перебування в мережі (Dwell Time) під контролем та підвищення вартості атаки.

Ключовим елементом архітектури спільний інтерфейс, що виступає єдиною точкою входу для всіх суб'єктів та приховує наявність захисних механізмів. Система здійснює непомітну сегрегацію трафіку, в якій дії, що ідентифікуються як неавторизовані, не викликають повідомлення про відмову в доступі; замість цього активність приховано перенаправляється до ізольованої системи-пастки. Це дозволяє не лише захистити критичні активи від компрометації, але й дезорієнтувати атакуючого, змушуючи його витрачати ресурси на взаємодію з фальшивим середовищем, що дає змогу безпечно вивчати його тактики та інструменти [17].

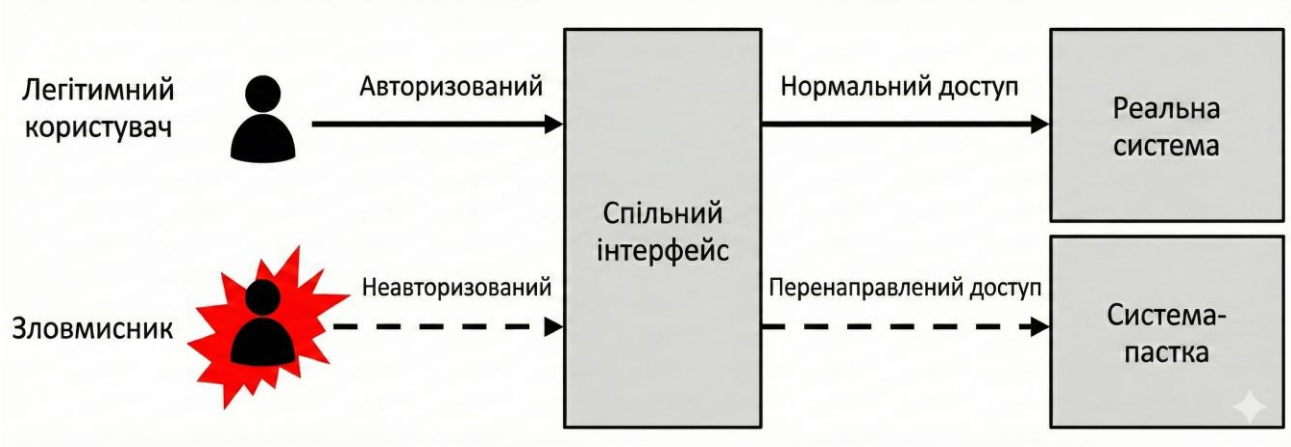

Рисунок 2.5. Концептуальна схема використання обману зловмисників

Технічна еволюція цих засобів пройшла шлях від ізольованих серверів-пасток (Honeypots) до комплексних розподілених платформ обману зловмисників (Distributed Deception Platforms — DDP), які інтегрують елементи симуляції безпосередньо в операційні системи кінцевих точок та хмарну інфраструктуру [18]. Суть роботи таких систем полягає у наступному:

- Створення фальшивого середовища: Розгортання обманнихз активів (фальшиві сервери, бази даних, облікові дані), які імітують реальні елементи всередині корпоративної мережі.
- Заманювання зловмисників: Активні зловмисники, шукаючи цінні цілі, взаємодіють із цими пастками, помилково вважаючи, що знайшли реальні системи.
- Генерація високоточних сповіщень: Оскільки пастки не мають реальної виробничої цінності, будь-яка активність у їхніх межах позначається як підозріла, що забезпечує чіткі попередження з низьким рівнем помилкових спрацьовувань.
- Збір даних кіберрозвідки (Threat Intelligence): Фіксують TTP зловмисників (тактики, техніки та процедури — як вони переміщуються, які інструменти використовують) для глибшого аналізу та проактивного захисту.
- Відволікання та затримка: Відвертають увагу зловмисників від реальних продуктивних систем, виграючи час для реагування команд безпеки.

Ключовими перевагами їх використання є:

- Раннє виявлення: Дозволяє виявити зловмисників на початкових етапах проникнення.
- Зниження кількості помилкових спрацьовувань: На пастках відбувається мінімальна легітимна активність, що робить сповіщення високонадійними.
- Глибока аналітика: Надає розуміння методів атак, що використовуються в реальних умовах.

- Інтеграція: Взаємодіє з інструментами EDR, NDR, SOAR та SIEM для автоматизації процесів реагування.

На рівні програмної реалізації класичні пастки (Honeypot, ханіпот) диференціюються за ступенем взаємодії зі зловмисником, що визначає глибину отримуваних даних та рівень ризику для інфраструктури:

- Системи низького рівня взаємодії (Low-interaction): Програмні рішення, такі як Dionaea, Cowrie або HoneyTrap, функціонують як емулятори мережевого стеку та сервісів. Вони не надають зловмиснику доступу до реального командного інтерпретатора (shell), а лише скриптово відтворюють діалог за протоколами SSH, Telnet, FTP, SMB чи HTTP. Їхня архітектура базується на кінцевих автоматах (state machines), які видають заготовлені відповіді на стандартні запити. Головна перевага — безпека (зловмисник не може захопити емулятор) та простота розгортання, проте вони неефективні проти складних атак, що вимагають нестандартної логіки виконання.
- Системи середнього рівня взаємодії (Medium-interaction): Забезпечують розширену емуляцію сервісів, дозволяючи зловмиснику частково взаємодіяти з системою (наприклад, завантажувати файли на емульований FTP-сервер або виконувати базові команди в пісочниці). Прикладом є SSH-Honeypot Kippo, який симулює файлову систему, дозволяючи аналізувати, які саме команди вводить зловмисник після «успішної» авторизації.
- Системи високого рівня взаємодії (High-interaction): Базуються на повноцінних, реальних операційних системах зі стандартним набором сервісів. Тут активність зловмисника не обмежується скриптами. Для моніторингу таких систем використовуються просунуті методи інтроспекції, зокрема технологія VMI (Virtual Machine Introspection). На відміну від встановлення агентів моніторингу всередині ОС (які можуть бути виявлені та вимкнені руткітами), VMI дозволяє аналізувати стан

віртуальної машини з рівня гіпервізора. Аналізатор (наприклад, на базі бібліотеки LibVMI) безпосередньо зчитує регістри процесора, сторінки пам'яті та події введення-виведення гостьової ОС. Це забезпечує «невидимий» моніторинг (agentless monitoring), дозволяючи фіксувати поведінку складних загроз рівня ядра (Kernel-mode rootkits), які залишаються непомітними для традиційних антивірусів [33].

Таблиця 2.1

Порівняння характеристик ханіпотів різних за ступенем взаємодії зі зловмисником

Критерій порівняння	**Системи низького рівня взаємодії (Low-interaction)**	**Системи середнього рівня взаємодії (Medium-interaction)**	**Системи високого рівня взаємодії (High-interaction)**
Архітектура та принцип роботи	Емулятори мережевого стеку та сервісів. Базуються на кінцевих автоматах (state machines).	Забезпечують розширену емуляцію сервісів та симуляцію файлової системи (пісочниця).	Базуються на повноцінних, реальних операційних системах зі стандартним набором сервісів.
Рівень взаємодії зі зловмисником	Обмежений скриптовим відтворенням діалогу (SSH, Telnet, FTP, SMB, HTTP). Доступ до реального інтерпретатора (shell) відсутній.	Дозволяє часткову взаємодію: завантаження файлів, виконання базових команд у пісочниці.	Повна взаємодія з реальною ОС, активність не обмежується скриптами.
Методи моніторингу	Реєстрація стандартних запитів та відповідей згідно з протоколами.	Аналіз введених команд після «успішної» авторизації.	Просунута інтроспекція (VMI) з рівня гіпервізора (зчитування регістрів процесора, пам'яті, подій вводу-виводу).

Продовження табл. 2.1

Ключові особливості та можливості	Видають заготовлені відповіді на запити. Безпечні (неможливо захопити емулятор) та прості у розгортанні.	Дозволяють аналізувати поведінку зловмисника в емульованому середовищі.	«Невидимий» моніторинг (agentless), здатність виявляти складні загрози рівня ядра (Kernel-mode rootkits).
Обмеження	Неефективні проти складних атак, що вимагають нестандартної логіки виконання.	Обмежені можливостями емульованого середовища (пісочниці).	Вимагають складніших методів моніторингу (VMI), оскільки агенти всередині ОС можуть бути виявлені.
Приклади рішень	Dionaea, Cowrie, HoneyTrap	SSH-Honeypot Kippo	Рішення на базі бібліотеки LibVMI

Перевагою пасток типу Honeypot є це надзвичайна простота концепції, що дає їм деякі дуже потужні переваги:

- Ханіпоти збирають невеликі обсяги інформації. Замість того, щоб реєструвати один ГБ даних на день, вони можуть реєструвати лише один МБ даних на день. Замість того, щоб генерувати 10 000 сповіщень на день, вони можуть генерувати лише 10 сповіщень на день. Пам’ятайте, що ханіпоти фіксують лише погану активність; будь-яка взаємодія з з ханіпотами, найімовірніше, є несанкціонованою або зловмисною діяльністю. Таким чином, ханіпоти зменшують шум, збираючи лише невеликі набори даних, але інформацію високої цінності, оскільки це лише погані хлопці. Це означає, що набагато легше (і дешевше) аналізувати дані, які збирають ханіпоти, і отримувати з них цінні дані.
- Ханіпоти розроблені для фіксації всього, що їм кидають, включаючи інструменти чи тактики, яких ніколи раніше не було.

- Ханіпоти потребують мінімальних ресурсів, вони фіксують лише зловмисну активність.
- На відміну від більшості технологій безпеки (таких як системи виявлення вторгнень), ханіпоти добре працюють у зашифрованому середовищі або середовищі IPv6. Незалежно від того, як зловмисники взаємодіють з ханіпотами, вони виявлять і фіксуватимуть це.
- Ханіпоти можуть збирати глибоку інформацію, з якою мало які інші технології, якщо взагалі якісь, можуть зрівнятися [17].

Ефективне використання технології Honeypot базується на безперервному ітеративному циклі, що адаптує пастку до зміни тактик зловмисників. Цей процес розпочинається з етапу дослідження, де аналізуються потенційні загрози для визначення, на кого саме орієнтована пастка. На основі отриманих даних створюється приманки, яка має виглядати максимально цінним та легітимним для обраної цілі. Наступним кроком є реалістичне розгортання ханіпота в інфраструктурі, що часто вимагає залучення компетентних вендорів для зниження складності інтеграції. Завершується та водночас перезапускається цикл етапом моніторингу та коригування: система збирає дані про атаки в реальному часі, дозволяючи захисникам вивчати тенденції та модифікувати параметри приманки для підвищення її ефективності [18].

Рисунок 2.6. Схема життєвого циклу ханіпота (приманки)

Сучасна архітектура систем Deception Technology докорінно відрізняється від класичних пасток принципом «проекції» та «всюдисущого обману» (Ubiquitous Deception). Замість пасивного очікування підключення до окремого сервера, ці платформи автоматизовано розповсюджують на реальних робочих станціях (Endpoints) тисячі фальшивих артефактів — «принад» (Lures/Breadcrumbs), які ведуть до ізольованих серверів-пасток (Decoys).

Технічна реалізація принад базується на глибокому розумінні тактик горизонтального переміщення (Lateral Movement):

- Endpoint Deception: Агенти обману впроваджують фальшиві дані безпосередньо у пам'ять та файлову систему користувача. Наприклад, для протидії інструментам дампінгу облікових даних (типу Mimikatz), Deception-агент ін’єктує фальшиві хеші паролів та квитки Kerberos у адресний простір процесу lsass.exe. При спробі зловмисника екстрагувати облікові дані, він отримує валідний на вигляд, але фальшивий хеш. Будь-яка спроба використання цього хешу (Pass-the-Hash) для авторизації на будь-якому ресурсі мережі миттєво генерує високопріоритетний алерт, оскільки легітимні користувачі ніколи не використовують ці фейкові дані.
- Active Directory Deception: Оскільки компрометація контролера домену є головною ціллю більшості атак, технології обману створюють «тіньовий» шар у Active Directory. Це включає створення фальшивих облікових записів адміністраторів, сервісних акаунтів (Service Accounts) із привабливими SPN (Service Principal Names) для виявлення атак типу Kerberoasting, а також реєстрацію неіснуючих комп'ютерів у DNS. Такі об'єкти моніторяться в реальному часі: будь-який запит до них (наприклад, спроба перерахування членів фейкової групи «Domain Admins») сигналізує про етап розвідки.
- Application & Data Deception: Створення фальшивих конфігураційних файлів, записів історії RDP-клієнтів, збережених сесій у терміналах

(PuTTY, WinSCP) та історії браузерів. Ключовою вимогою до таких принад є динамічна адаптивність (Dynamic Deception): система аналізує контекст реального хоста (ім'я, підмережа, встановлене ПЗ) і генерує принади, що органічно вписуються в оточення. Якщо робоча станція належить бухгалтеру, система створить принаду у вигляді посилання на «Financial_Server_Backup», а не на «IT_Admin_Portal».

Окремим вектором технічної реалізації є використання «медових токенів» (Honeytokens). Це цифрові маркери, які не мають легітимного застосування, але чий доступ або використання сигналізує про витік.

- Файлові маяки: Спеціально сформовані документи (Word, PDF, Excel) з вбудованими пікселями відстеження або макросами. При відкритті такого файлу на комп'ютері зловмисника (навіть за межами корпоративної мережі), документ ініціює вихідний HTTP/DNS-запит до сервера управління, передаючи метадані про IP-адресу атакуючого та версію його ПЗ.
- Бази даних: Створення фальшивих записів у реальних таблицях баз даних. Налаштування тригерів на операцію SELECT для цих рядків дозволяє виявити SQL-ін'єкції або дії інсайдерів, які намагаються вивантажити повний дамп бази.
- Хмарні токени: Розміщення неактивних API-ключів AWS або Azure у конфігураційних файлах розробників. Спроба використання цих ключів для доступу до хмарної інфраструктури одразу блокується Cloud-провайдером з генерацією сповіщення.

Також Deception Technology демонструє високу ефективність у протидії програмам-вимагачам (Ransomware). Системи розміщують на мережевих дисках спеціальні «жертовні» файли-принади, які постійно моніторяться. Оскільки віруси-шифрувальники зазвичай сканують диски та шифрують файли в алфавітному порядку або за розширеннями, початок операції запису у файл-принаду (наприклад, 000_Backup.docx) дозволяє системі захисту детектувати

атаку на ранній стадії та автоматично розірвати з'єднання з інфікованим хостом ще до того, як буде зашифровано критичні дані.

Ефективність Deception-платформ значно зростає при інтеграції з екосистемою SOAR (Security Orchestration, Automation and Response), EDR та мережевими шлюзами (NAC). Це дозволяє реалізувати сценарії автоматичного стримування: як тільки спрацьовує принада, IP-адреса джерела атаки автоматично ізолюється в карантинний VLAN, блокується на рівні порту комутатора або процес, що ініціював звернення до пастки, «заморожується» EDR-агентом для подальшого криміналістичного аналізу. Таким чином, технології обману замикають цикл кібербезпеки, перетворюючи кожну спробу атакуючого зробити крок у мережі на тригер для системи захисту [34,35].

Висновки до розділу 2

У другому розділі проведено детальний аналіз технологічного інструментарію, що забезпечує функціонування симуляційних середовищ у кібербезпеці.

Автоматизація верифікації захисту: Технології BAS (Breach and Attack Simulation) змінили підхід до тестування безпеки, дозволивши перейти від періодичних аудитів до безперервної перевірки стійкості інфраструктури. Використання безпечних агентів та інтеграція з матрицею MITRE ATT&CK дозволяє емпірично оцінювати ефективність налаштувань засобів захисту проти актуальних тактик зловмисників.

Інфраструктурна складність полігонів: Сучасні кіберполігони (Cyber Ranges) представляють собою складні програмно-апаратні комплекси, що поєднують технології віртуалізації, хмарної оркестрації та генерації синтетичного трафіку. Вони дозволяють створювати гіперреалістичні моделі мереж, що включають не лише корпоративні сервіси, а й емуляцію зовнішнього Інтернет-середовища, що є критичним для повноцінного відпрацювання сценаріїв реагування.

Еволюція технологій обману: Аналіз засобів Deception Technology продемонстрував їхню трансформацію з пасивних пасток у проактивні системи захисту кінцевих точок. Технічна реалізація через ін'єкцію фальшивих даних у пам'ять процесів та файлову систему дозволяє нівелювати перевагу зловмисника у прихованості, перетворюючи інфраструктуру на вороже середовище для несанкціонованої активності.

Загалом, розглянуті технології формують цілісний стек рішень для побудови адаптивної системи кібербезпеки, де симуляція виступає як інструментом навчання, так і засобом активної протидії.

РОЗДІЛ 3
ВПРОВАДЖЕННЯ ТА ПЕРСПЕКТИВИ РОЗВИТКУ СИМУЛЯЦІЙНИХ СИСТЕМ

Ефективність функціонування сучасних систем захисту інформації визначається не лише тактико-технічними характеристиками окремих засобів безпеки, а й здатністю організації інтегрувати їх у єдину, керовану екосистему. Впровадження симуляційних технологій — від автоматизованих платформ BAS (Breach and Attack Simulation) до комплексних цифрових полігонів — є складним інженерно-організаційним завданням, що вимагає фундаментальної перебудови процесів управління ризиками. Це не просто інсталяція програмного забезпечення, а перехід до нової парадигми «доказової безпеки», де будь-яке архітектурне рішення перевіряється емпіричним шляхом.

У цьому розділі розглядається методологія імплементації симуляційних систем у наявну IT-інфраструктуру підприємства. Процес впровадження декомпозовано на логічні етапи: від попереднього аудиту та розгортання агентської мережі до операціоналізації результатів тестування в рамках процесів SOC (Security Operations Center). Особливу увагу приділено проблематиці вимірювання ефективності (KPI), оскільки відсутність чітких метрик унеможливлює оцінку окупності інвестицій (ROI). Завершується розділ аналізом стратегічних перспектив розвитку галузі, де ключовими драйверами змін виступають конвергенція з технологіями цифрових двійників (Digital Twins), застосування генеративного штучного інтелекту для моделювання адаптивних загроз та концепція Security Chaos Engineering.

3.1 Етапи розгортання симуляційних платформ в інфраструктурі організації

Впровадження симуляційних рішень у корпоративне середовище є багатофакторним процесом, який вимагає суворої регламентації та узгодження з бізнес-пріоритетами організації. Методологічно цей процес доцільно розділити на чотири послідовні фази: підготовчо-аналітичну, архітектурно-технічну, операційну інтеграцію та фазу безперервного вдосконалення (рис. 3.1).

Рис. 3.1. Фази імплементації симуляційних рішень

На підготовчо-аналітичній фазі критично важливим є моделювання профілю загроз (Threat Modeling), моделі порушника, специфічних для конкретної галузі. Недоцільно впроваджувати абсолютно всі можливі засоби, без проведення необхідних досліджень. На основі проведеного аналізу необхідно побудувати матрицю ризиків, і спираючись на прийняту політику керування ризиками і технічну, фінансову, адміністративну можливість скласти Технічне завдання, що відображатиме справді необхідні спроможності та засоби, зокрема підготовку положень про використання впроваджуваних систем. Так, до прикладу, не має сенсу розглядати одразу всі існуючі вектори атак; натомість необхідно сфокусуватися на найбільш ймовірних сценаріях. Для фінансової установи пріоритетними будуть атаки на процесинг (SWIFT) та соціальна інженерія, тоді як для об'єктів критичної інфраструктури (SCADA/ICS) — атаки на протоколи промислової автоматизації. На цьому етапі

формується «Матриця покриття» (Coverage Matrix), яка визначає, які саме сегменти мережі та бізнес-процеси підпадають симуляційному тестуванню.

Архітектурно-технічна фаза передбачає безпосереднє розгортання програмно-апаратних комплексів відповідно до затвердженого Технічного завдання. Ключовим пріоритетом тут є дотримання принципу ізоляції та безпеки інфраструктури.

- Для кіберполігонів та пісочниць: Здійснюється розгортання середовища віртуалізації. Критично важливим є налаштування мережевої сегментації (VLAN чи інші способи мережевої сегментації чи ізоляції), що унеможливлює вихід шкідливого ПЗ, яке детонує в пісочниці, у продуктивну мережу організації . Створюються «золоті образи» (Golden Images) віртуальних машин, що імітують типові робочі станції співробітників з актуальним набором офісного ПЗ.
- Для систем обману (Honeypots/Deception): Відбувається розміщення пасток у різних, попередньо визначених на підготовчо-аналітичному етапі та описаних у Технічному завданні сегментах мережі (DMZ, внутрішні сервери, користувацькі підмережі). Паралельно може впроваджується технологія «хлібних крихт» (breadcrumbs) — на реальних робочих станціях розміщуються фальшиві облікові дані, токени або посилання, які ведуть зловмисника до пасток [34].
- Для BAS-платформ: Інсталюються агенти симуляції на кінцевих точках та серверах. Налаштовуються виключення в антивірусних засобах (AV/EDR) для самих агентів, щоб дозволити їм виконувати емуляцію, але не для тестових атак, які ці засоби повинні виявляти.

Фаза операційної інтеграції спрямована на впровадження функціоналу впровадженого інструментарію в бізнес-процеси організації, до прикладу включення ханіпотів в екосистему моніторингу та реагування (SOC), впровадження практичних занять на кіберполігонах в програму регулярних навчань для співробітників організації, впровадження автоматичного дослідження підозрілих вкладень на поштовому шлюзі електронної пошти

детонуючи їх у середовищі пісочниці. Симуляційні платформи не повинні існувати у вакуумі; їх дані мають збагачувати загальну картину безпеки [57]. Ці дії можна згрупувати у три основні категорії:

- Налаштування потоків даних: Забезпечується передача логів від ханіпотів, звітів пісочниць та результатів BAS-тестів до централізованої системи SIEM або платформи SOAR.
- Кореляція подій: Розробляються правила кореляції, які дозволяють відрізняти навчальні інциденти від реальних, або ж, навпаки, використовувати спрацювання пасток як індикатор компрометації з найвищим пріоритетом (High Fidelity Alert).
- Навчання персоналу: Проводяться тренінги для аналітиків SOC щодо інтерпретації даних, отриманих від нових систем. Персонал повинен розуміти, як виглядає звіт про детонацію malware у пісочниці та як реагувати на активність у сегменті ханіпотів.

Фінальною фазою є безперервне вдосконалення (Continuous Validation). Вона передбачає перехід від разових тестів до режиму роботи 24/7 адже впровадження симуляційних платформ — це не разова дія, а циклічний процес. Фаза забезпечує адаптацію системи захисту до змін ландшафту загроз. До прикладу, на цьому етапі впроваджуються механізми автоматичного запуску тестів при будь-яких змінах в інфраструктурі (Change Management): зміна правил на міжмережевому екрані або оновлення версії ОС автоматично тригерить запуск відповідного набору тестів («Smoke Testing» для безпеки), щоб переконатися, що зміни не утворили нових дірок у захисті тощо. На даному етапі здійснюються:

- Аналіз ефективності (KPIs): Оцінка метрик, таких як час виявлення (MTTD) та час реагування (MTTR) під час симуляцій.
- Оновлення сценаріїв: Регулярна актуалізація бібліотек атак у BAS-системах та оновлення профілів ханіпотів відповідно до нових технік, що з'являються у базі MITRE ATT&CK.

- Масштабування: Розширення покриття симуляційними засобами на нові філії, хмарні середовища або бізнес-додатки по мірі розвитку організації.

Підсумовуючи, слід зазначити, що дотримання запропонованої етапності дозволяє трансформувати впровадження симуляційних технологій зі складного інженерного виклику в керований та прогнозований бізнес-процес. Такий структурований підхід не лише мінімізує операційні ризики, пов'язані з «дружнім вогнем» у продуктивному середовищі, а й виступає гарантом раціонального використання ресурсів організації. Чітка кореляція між модельованим профілем загроз та технічним завданням унеможливлює надлишкові витрати на інструментарій, який не відповідає реальним ризикам компанії, забезпечуючи тим самим максимальний коефіцієнт повернення інвестицій (ROI). Крім того, документування кожного етапу — від затвердження правил взаємодії до фіксації метрик успіху — створює необхідний рівень прозорості для всіх стейкхолдерів, перетворюючи кібербезпеку з «чорної скриньки» на зрозумілу, вимірювану та інтегровану бізнес-функцію.

3.2 Оцінка ефективності використання впроваджених симуляційних технологій

Проблема оцінки ефективності інвестицій у кібербезпеку (ROI) є однією з найгостріших у галузі. Традиційні метрики, що базуються на кількості відбитих атак, є малоінформативними, оскільки не враховують складність загроз та якість реагування. Впровадження симуляційних технологій дозволяє перейти до системи об'єктивних, вимірюваних показників (KPI), які можна розділити на технічні (для оцінки засобів захисту) та операційні (для оцінки персоналу).

Ефективність кожного класу симуляційних рішень вимагає застосування унікального набору метрик, що відображають специфіку їхнього функціонального призначення позаяк метрики ефективності кіберполігону відрізнятимуться від метрик ефективності ханіпотів.

Оцінка ефективності середовищ ізольованого виконання («Пісочниць»), для таких систем динамічного аналізу (Sandboxes) головним критерієм є баланс між глибиною аналізу та впливом на бізнес-процеси (затримкою трафіку) [52]. Ключові показники включають:

- Коефіцієнт успішної детонації (Detonation Rate): Відсоток зразків, які успішно запустилися та продемонстрували шкідливу поведінку у віртуальному середовищі. Низький показник може свідчити про застарілість образів гостьових ОС або успішне застосування вірусами технік ухилення (evasion techniques).
- Стійкість до технік ухилення (Anti-Evasion Efficacy): Здатність пісочниці виявляти спроби шкідливого ПЗ визначити віртуальне середовище (перевірка наявності специфічних драйверів, відсутність рухів мишею тощо).
- Час аналізу (Analysis Latency): Середній час, необхідний для винесення вердикту. Для потокових пісочниць, що працюють у режимі блокування (inline), цей показник є критичним для User Experience (UX).

- Якість індикаторів компрометації (IoC Quality): Кількість та релевантність витягнутих артефактів (IP-адреси C2-серверів, хеші файлів, зміни в реєстрі), які можуть бути автоматично імпортовані в системи захисту периметра.

Оцінка ефективності інфраструктури кіберполігонів (Cyber Ranges) зумовлюється метою функціонування самого кіберполігону, скільки основною метою кіберполігонів є підготовка «людського фактору», метрики тут фокусуються на вимірюванні компетенцій команд SOC/CSIRT чи звичайних користувачів під час тренувань з кіберобізнаності чи з розпізнання фішингу та ефективності процесів [38,39]. Основними KPI будуть такі, що стосуються підготовлених команд:

- Час виявлення (MTTD — Mean Time to Detect): Інтервал часу між запуском симуляції атаки на полігоні та моментом створення першого інциденту в SIEM-системі аналітиком.
- Час реагування (MTTR — Mean Time to Respond): Час, витрачений командою на локалізацію загрози та відновлення працездатності сервісів після виявлення. Скорочення MTTR у динаміці навчань є головним індикатором зростання кваліфікації.
- Коефіцієнт покриття сценаріїв (Scenario Coverage Rate): Відсоток успішно виявлених та відбитих технік з матриці MITRE ATT&CK під час навчань.
- Відповідність плейбукам (Playbook Adherence): Якісний показник, що оцінює, наскільки точно дії команди відповідали затвердженим процедурам реагування. Відхилення вказують на необхідність перегляду інструкцій або додаткового навчання.

Оцінити ефективність технологій обману (Honeypots/Deception) складно, оскільки специфіка ханіпотів полягає в тому, що вони не повинні генерувати трафік подій безпеки у нормальному стані безпеки системи, тож його ефективність можливо виміряти лише у ході атаки або під час проходження пентестингу. Такими показниками можуть бути:

- Співвідношення сигнал/шум (Signal-to-Noise Ratio): Ефективність ханіпота визначається відсутністю помилкових спрацьовувань (False Positives). Ідеальний показник прагне до 100% точності («High Fidelity Alerts»), оскільки легітимні користувачі не повинні взаємодіяти з приманками.
- Час утримання зловмисника (Attacker Retention Time): Тривалість взаємодії атакуючого з фальшивою системою. Чим вищий цей показник, тим більше ресурсів витрачає зловмисник марно і тим більше даних про його тактику (TTPs) встигають зібрати захисники.
- Кількість зібраних унікальних загроз (Unique Intelligence Yield): Обсяг нових, раніше невідомих індикаторів (наприклад, 0-day експлойтів або нових IP-адрес ботнетів), отриманих завдяки аналізу активності в пастці.
- Коефіцієнт відволікання (Diversion Rate): Співвідношення атак, спрямованих на Deception-інфраструктуру, до загальної кількості спроб проникнення в мережу.

Впровадження та регулярний моніторинг визначених показників дозволяє трансформувати функцію кібербезпеки з традиційної «витратної статті» бюджету в прозорий, керований бізнес-процес. Завдяки цьому кожна інвестиція в симуляційні технології отримує чітке економічне обґрунтування, що базується не на гіпотетичних припущеннях, а на вимірюваному підвищенні стійкості інфраструктури та скороченні часу реакції на інциденти. Більше того, перехід до системи кількісних метрик створює спільний комунікаційний простір між технічними фахівцями та топ-менеджментом, дозволяючи транслювати складні технічні загрози в площину зрозумілих бізнес-ризиків. Це відкриває шлях до реалізації концепції доказової безпеки (Evidence-Based Security).

3.3 Перспективи розвитку: цифрові двійники (Digital Twins) та використання ШІ в симуляціях

Напрями подальшого розвитку симуляційних технологій визначаються загальними трендами Індустрії 4.0, зокрема конвергенцією фізичного та цифрового світів, а також експоненційним зростанням можливостей штучного інтелекту.

Концепція Cyber Digital Twins (Цифрові двійники) Еволюція кіберполігонів рухається в напрямку створення високоточних цифрових двійників організації. Якщо традиційний полігон є узагальненою моделлю, то Digital Twin — це динамічна репліка реальної інфраструктури, яка синхронізується з «оригіналом» у режимі реального часу, отримуючи дані телеметрії, конфігурації мережевого обладнання та версії ПЗ. Це відкриває шлях до предиктивного моделювання безпеки (Predictive Security). Перед впровадженням будь-яких змін (патчів, нових правил файрволу, змін у топології) адміністратори можуть протестувати їх на цифровому двійнику, піддавши його масованій атаці. Це особливо критично для систем промислового інтернету речей (IIoT) та критичної інфраструктури, де сканування працюючих систем може призвести до технологічних аварій. Цифровий двійник дозволяє проводити деструктивні тести (Chaos Engineering), перевіряючи відмовостійкість системи, не ризикуючи зупинкою реального виробництва.

Штучний інтелект та AI Red Teaming Інтеграція ШІ трансформує роль «атакуючої сторони» в симуляціях. Традиційні скрипти мають обмежену логіку і діють за заздалегідь визначеним алгоритмом. На зміну їм приходять автономні агенти на базі навчання з підкріпленням (Reinforcement Learning). Такий AI-агент не просто виконує команди, а має цільову функцію (наприклад, «отримати доступ до бази даних») і самостійно шукає шляхи її досягнення, адаптуючись до дій захисту. Якщо один порт заблоковано, AI-агент спробує інший вектор, змінить сигнатуру пейлоаду або використає техніку обфускації,

навчаючись на своїх помилках. Це дозволяє реалізувати концепцію «перманентного пентесту», де система піддається безперервним атакам з боку надлюдського інтелекту, що змушує захист постійно еволюціонувати [9,11].

Security Chaos Engineering Перспективним напрямом є адаптація методології Chaos Engineering до завдань кібербезпеки що передбачає введення контрольованих збоїв у систему безпеки: випадкове відключення сегмента мережевого екрану, деактивація агента EDR на критичному сервері або емуляція компрометації облікового запису адміністратора. Метою таких симуляцій є перевірка того, чи здатна система самостійно виявити аномалію та відновити безпечний стан (Self-healing systems) [52].

Таким чином, майбутнє симуляційних технологій лежить у площині повної автоматизації та інтелектуалізації процесів, де роль людини зміщується від ручного тестування до стратегічного управління параметрами автономних систем захисту та нападу.

Висновки до розділу 3

У третьому розділі роботи здійснено комплексний аналіз методології практичної імплементації симуляційних систем у наявну IT-інфраструктуру підприємства. За результатами проведеного дослідження сформульовано наступні узагальнення:

Системність та процесна орієнтованість впровадження. Обґрунтовано, що інтеграція симуляційних технологій (BAS, кіберполігони, Honeypots) не може розглядатися як точкове технічне завдання, а є складним інженерно-організаційним процесом, що вимагає дотримання повного життєвого циклу. Запропонована чотирифазна модель — від підготовчо-аналітичного етапу та архітектурної реалізації до операційної інтеграції та циклу безперервного вдосконалення — виступає необхідним фундаментом для успішного проекту. Такий підхід дозволяє мінімізувати ризики впливу на бізнес-процеси («friendly fire»), забезпечити відповідність налаштувань реальному профілю загроз організації та гарантувати безшовну інтеграцію нових інструментів в екосистему SOC, уникаючи створення ізольованих систем безпеки.

Вимірюваність результатів та економічне обґрунтування. Доведено, що перехід до сучасної парадигми «доказової безпеки» (Evidence-Based Security) можливий виключно за умови запровадження системи об'єктивних метрик. У роботі систематизовано специфічні KPI для різних класів систем: технічні показники для «пісочниць» (рівень детонації, стійкість до ухилення) та операційні метрики для кіберполігонів і ханіпотів (MTTD, MTTR, Signal-to-Noise Ratio). Встановлено, що використання цих показників вирішує фундаментальну проблему галузі — оцінку повернення інвестицій (ROI). Це дозволяє трансформувати кібербезпеку з витратної функції у прозорий, керований бізнес-процес, де рішення про закупівлю засобів захисту базуються на емпіричних даних про їхню ефективність, а не на маркетингових обіцянках вендорів.

Стратегічні перспективи та технологічна конвергенція. Аналіз тенденцій розвитку галузі засвідчив, що майбутнє симуляційних технологій лежить у площині глибокої інтеграції з концепціями Індустрії 4.0. Впровадження цифрових двійників (Digital Twins) дозволить реалізувати предиктивне моделювання безпеки, переносячи тестування вразливостей з продуктивного середовища у віртуальну репліку. Водночас, використання автономних AI-агентів для Red Teaming та застосування методології Security Chaos Engineering забезпечить перехід до повної автоматизації процесів виявлення та самовідновлення систем (Self-healing systems). Це дозволить організаціям не лише реагувати на інциденти, а й проактивно формувати стійкість до загроз, що еволюціонують швидше, ніж здатна реагувати людина.

Таким чином, імплементація симуляційних платформ є критично необхідним етапом еволюційної зрілості системи захисту сучасної організації, що забезпечує перехід від реактивного «гасіння пожеж» до проактивного управління кіберстійкістю на основі даних.

ВИСНОВКИ

У магістерській кваліфікаційній роботі здійснено системне та комплексне дослідження теоретичних, технологічних і практичних аспектів застосування симуляційних методів у сфері кібербезпеки. На основі проведеного аналізу наукової літератури, нормативно-правової бази, архітектури сучасних програмно-апаратних комплексів та методології їх впровадження отримано наступні наукові та практичні результати:

1. Обґрунтовано зміни парадигми кіберзахисту, у ході дослідження встановлено, що сучасний ландшафт кіберзагроз характеризується критичним зростанням асиметрії між можливостями зловмисників та захисників. Традиційні реактивні моделі безпеки, що базуються на статичному периметральному захисті та сигнатурному аналізі, втратили свою ефективність в умовах поширення APT-атак (Advanced Persistent Threats), поліморфного шкідливого програмного забезпечення та технік «living-off-the-land». Доведено, що стратегічною відповіддю на ці виклики є перехід до концепції «Active Defense» (Активного захисту) та «Evidence-Based Security» (Доказової безпеки). Фундаментом цієї нової парадигми виступають симуляційні технології, які дозволяють змістити фокус з пасивного очікування інцидентів на проактивне виявлення вразливостей архітектури та верифікацію стійкості інфраструктури в умовах, наближених до реальних бойових дій.

2. Систематизовано понятійно-категоріальний апарат, провівши критичний аналіз та чітку диференціацію ключових термінів, які часто помилково ототожнюються у фаховій літературі: «віртуалізація», «емуляція» та «симуляція». Визначено, що віртуалізація формує інфраструктурний базис для ізольованого виконання коду («пісочниці»), забезпечуючи масштабованість ресурсів. Емуляція є критично важливою для відтворення функціональності специфічних апаратних архітектур (зокрема IoT, SCADA, legacy-систем), що дозволяє аналізувати загрози для обладнання, яке неможливо віртуалізувати стандартними засобами. Симуляція фокусується на сценарному моделюванні

поведінки складних систем, мережевого трафіку та соціотехнічних взаємодій. Така класифікація має важливе практичне значення, оскільки дозволяє архітекторам систем безпеки коректно обирати інструментарій залежно від поставлених завдань: від глибокого аналізу шкідливого ПЗ до проведення масштабних кібернавчань.

3. Проведено аналіз еволюції технологічного інструментарію. Детально досліджено три ключові вектори розвитку симуляційних платформ, які формують сучасну екосистему активного захисту.

Встановлено, що технології BAS (Breach and Attack Simulation) революціонізували процес аудиту безпеки, дозволивши перейти від дискретних, розтягнутих у часі тестів на проникнення (Penetration Testing) до безперервної (24/7) автоматизованої валідації. Інтеграція BAS-агентів із глобальною матрицею загроз MITRE ATT&CK дозволяє організаціям емпірично перевіряти ефективність налаштувань засобів захисту (NGFW, EDR, SIEM) проти актуальних тактик і технік кіберзлочинців, оперативно виявляючи «дрейф безпеки» (security drift).

Визначено, що сучасні кіберполігони (Cyber Ranges) трансформувалися зі статичних лабораторних стендів у високотехнологічні оркестровані середовища, які поєднують віртуалізацію, емуляцію Інтернету («Сіра зона») та генерацію синтетичного трафіку. Вони відіграють подвійну роль: як платформа для «стрес-тестування» критичної інфраструктури без ризику для продуктивних систем, та як єдиний ефективний інструмент для формування практичних навичок команд реагування (Blue Teams) в умовах психологічного тиску та часових обмежень.

Досліджено трансформацію засобів обману зловмисників (Deception Technology) від класичних пасивних ханіпотів (Honeypots) до комплексних платформ розподіленого обману (Distributed Deception Platforms — DDP). Сучасні рішення реалізують принцип «всюдисущого обману» (Ubiquitous Deception), автоматизовано розповсюджуючи фальшиві артефакти (облікові дані, токени, записи реєстру) безпосередньо на робочі станції користувачів. Це

дозволяє нівелювати перевагу зловмисника у прихованості, ефективно детектуючи атаки на етапах розвідки та горизонтального переміщення.

4. Розробка методології впровадження У роботі обґрунтовано, що імплементація симуляційних технологій є складним інженерно-організаційним процесом, який вимагає системного підходу. Розроблено та запропоновано модель впровадження симуляційних засобів у інфраструктуру організації, що структурно розділена на чотири фази:

Підготовчо-аналітична фаза: Включає моделювання загроз (Threat Modeling) для визначення актуальних векторів атак та формування Технічного завдання. Це дозволяє уникнути надлишкових витрат на захист від нерелевантних загроз.

Архітектурно-технічна фаза: Передбачає розгортання компонентів системи з дотриманням принципів ізоляції та безпеки (наприклад, налаштування VMI-моніторингу, сегментація мережі).

Операційна інтеграція: Критично важливий етап, на якому симуляційні платформи інтегруються в процеси SOC. Забезпечується кореляція подій із SIEM-системою, налаштування автоматичного реагування через SOAR та навчання персоналу інтерпретації нових типів алертів.

Фаза безперервного вдосконалення: Забезпечує адаптацію сценаріїв симуляції до змін у ландшафті загроз та інфраструктурі підприємства.

5. Вирішення проблеми оцінки ефективності (ROI) Одним із ключових практичних результатів роботи є вирішення проблеми оцінки повернення інвестицій у кібербезпеку. Доведено, що перехід до вимірюваної безпеки можливий через впровадження системи KPI (Key Performance Indicators), специфічних для симуляційних технологій:

Технічні метрики: Коефіцієнт успішної детонації в пісочницях, стійкість до технік ухилення, рівень покриття матриці MITRE ATT&CK.

Операційні метрики: Середній час виявлення (MTTD), середній час реагування (MTTR), співвідношення сигнал/шум (Signal-to-Noise Ratio). Використання цих показників дозволяє трансформувати кібербезпеку з

витратної функції («black box») у прозорий бізнес-процес, де управлінські рішення про закупівлю засобів захисту базуються на емпіричних даних, а не на гіпотетичних припущеннях.

6. Стратегічні перспективи розвитку У підсумковій частині роботи окреслено вектори подальшого розвитку симуляційних технологій у контексті Індустрії 4.0:

Цифрові двійники (Digital Twins): Прогнозується перехід до предиктивного моделювання безпеки на основі високоточних цифрових копій інфраструктури, що дозволить тестувати вплив вразливостей та патчів без жодного ризику для виробничих процесів.

Штучний інтелект (AI Red Teaming): Визначено тенденцію до використання автономних AI-агентів, здатних реалізувати адаптивні сценарії атак, навчаючись у процесі злому. Це вимагатиме від систем захисту переходу до повної автоматизації процесів реагування.

Security Chaos Engineering: Перспективним напрямом є впровадження практики контрольованих збоїв для перевірки здатності систем до самовідновлення (Self-healing).

Результати кваліфікаційної роботи переконливо свідчать, що симуляційні технології вже не є нішевим інструментом для вузькоспеціалізованих досліджень, а стають критично необхідним компонентом архітектури корпоративної безпеки. Їх системне впровадження дозволяє організаціям реалізувати замкнений цикл управління кіберстійкістю: від виявлення слабких місць через автоматизовану симуляцію до активного заплутування зловмисника та безперервного підвищення кваліфікації персоналу. Це забезпечує якісний стрибок у забезпеченні інформаційної безпеки, гарантуючи готовність до протидії найсучаснішим кіберзагрозам.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. S. A. Sharaf, M.A.A. Al-qaness, M.A. Alghamdi, A.S. Alqa-htani, A.M. Alshahrani, “Advanced mathematical modeling of mitigating security threats in smart grids through deep ensemble model,” Sci. Rep., vol. 14, no. 23069, Oct. 2024. DOI: 10.1038/s41598-024-74733-6. URL: https://www.nature.com/articles/s41598-024-74733-6.

2. M. Homaei, Ó. Mogollón-Gutiérrez, J. Carlos Sancho, M. Ávila & A. Caro, “A review of digital twins and their application in cybersecurity based on artificial intelligence,” Artif. Intell. Rev., vol. 57, no. 201, Jul. 2024. URL: https://link.springer.com/article/10.1007/s10462-024-10805-3.

3. Держспецзв’язку, «Огляд кіберзагроз та стратегій захисту в 2025 році: досвід CERT-UA». URL: https://cip.gov.ua/ua/news/cyber-threat-overview-and-defense-strategies-in-2025-cert-ua-s-experience .

4. Kothamali, Parameshwar Reddy & Banik, Subrata. (2022). Limitations of Signature-Based Threat Detection. URL: https://www.researchgate.net/publication/388494583_Limitations_of_Signature-Based_Threat_Detection.

5. Zhou, W.; Shen, S.; Liu, P. IoT Firmware Emulation and Its Security Application in Fuzzing: A Critical Revisit. Future Internet 2025, 17, 19. https://doi.org/10.3390/fi17010019

6. Ivan Horniichuk, Mykhailo Shelelo, A. Mykytiuk, Volodymyr Onishchenko, “Information technology for orchestration of the cybersecurity training situation center cyber range virtual environment,” Information Technology and Security, 2024. URL: https://its.iszzi.kpi.ua/article/view/316257

7. Шаповалова О. О. Модель потенційного порушника інформаційної безпеки у цифровому світі / О. О. Шаповалова, Б. В. Луговий // Collection of Scientific Papers with the Proceedings of the 6th International Scientific and Practical Conference «Evolving Science: Theories, Discoveries and Practical Outcomes»

(December 15-17, 2025, Zurich, Switzerland). European Open Science Space, 2025. - P. 206-212. URL: https://repository.hneu.edu.ua/handle/123456789/38238

8. Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Goeke, L., Hildebrandt, T., Tsakirakis, G., Oikonomou, F., Leftheriotis, G., & Koshutanski, H. (2020). Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees. Applied Sciences, 10(16), 5702. https://doi.org/10.3390/app10165702

9. Gallard, Jérome & lèbre, Adrien & Vallee, Geoffroy & Morin, Christine & Gallard, Pascal & Scott, Stephen. (2009). Refinement Proposal of the Goldberg's Theory. 853-865. URL: https://www.researchgate.net/publication/227167839_Refinement_Proposal_of_the_Goldberg's_Theory

10. Andrushchak, I., Kosheliuk, V., & Veremiy, I. (2025). Cybersecurity deception technologies: integrating cowrie and ELK Stack to detect network attacks. International Science Journal of Engineering & Agriculture, 4(6), 1–14. https://doi.org/10.46299/j.isjea.20250406.01

11. Debas, E., Alhumam, N., & Riad, K. (2023). Unveiling the dynamic landscape of malware sandboxing: A comprehensive review. URL: https://www.preprints.org/frontend/manuscript/dc43fb6ec3efd33de28eb5db1ec045d1/download_pub#page=2.63

12. Sánchez-Matas, A., Ruiz, P. E., Díaz-López, D., Gómez, A. L. P., Nespoli, P., & Pérez, G. M. (2025). Simulating Cyberattacks through a Breach Attack Simulation (BAS) Platform empowered by Security Chaos Engineering (SCE). URL: https://arxiv.org/abs/2508.03882

13. Ibrahimli, Javad & Burgu, Batu & Karadeniz, Kerem. (2025). AI-Driven Detection of Network Traffic Anomalies: A Case Study with OMNeT++. URL: https://www.researchgate.net/publication/393445813_AI-Driven_Detection_of_Network_Traffic_Anomalies_A_Case_Study_with_OMNeT

14. EU TIBER FRAMEWORK. URL: https://www.ecb.europa.eu/press/pubbydate/html/index.en.html?search_term=tiber%20eu%20framework

15. Державне підприємство "Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості", Наказ від 16.10.2019 № 312 Про прийняття та скасування національних стандартів, прийняття поправок до національних стандартів. URL: https://zakon.rada.gov.ua/rada/show/v0312774-19#Text

16. Національний банк України, Постанова № 95 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України». URL: https://zakon.rada.gov.ua/laws/show/v0095500-17#Text

17. Latha, K. & Gowsalya, B. & Kannega, B.. (2014). Procuring the Dropbox Using Honey Encryption Technique. Applied Mechanics and Materials. 573. 523-528. URL: https://www.researchgate.net/publication/272035606_Procuring_the_Dropbox_Using_Honey_Encryption_Technique

18. Edward Amoroso, CEO, TAG Cyber, An introduction to deception technology. URL: https://www.helpnetsecurity.com/2018/12/06/introduction-deception-technology/

19. H. Kavak, J. J. Padilla, D. Vernon-Bido, S. Diallo, R. Gore, S. Shetty, “Simulation for cybersecurity: state of the art and future directions,” J. Cybersecur., vol. 7, no. 1, 2021. URL: https://www.researchgate.net/publication/350057399_Simulation_for_cybersecurity_state_of_the_art_and_future_directions

20. J. Lee, M. D. Sung, I. K. Kim, “Technological trends in cyber attack simulations,” 2020. URL: https://www.semanticscholar.org/paper/Technological-Trends-in-Cyber-Attack-Simulations-Lee-Sung/cb269ff460b1bcc7c5ab4e5da695dbead2389155

21. L. Serena, G. D’Angelo, S. Ferretti, M. Marzolla, “Simulation in cybersecurity: understanding techniques, applications, and goals,” ArXiv, Aug. 2025. URL: https://www.researchgate.net/publication/394426778_Simulation_in_Cybersecurity_Understanding_Techniques_Applications_and_Goals

22. M. Yamin, B. Katt, “Use of cyber attack and defense agents in cyber ranges: a case study,” Comput. Secur., vol. 124, Aug. 2022. URL: https://www.sciencedirect.com/science/article/abs/pii/S0167404822002644

23. M. Yamin, B. Katt, “Modeling and executing cyber security exercise scenarios in cyber ranges,” Comput. Secur., vol. 111, Feb. 2022. URL: https://www.researchgate.net/publication/358499436_Modeling_and_Executing_Cyber_Security_Exercise_Scenarios_in_Cyber_Ranges

24. M. Yamin, B. Katt, M. Nowostawski, “Serious games as a tool to model attack and defense scenarios for cyber-security exercises,” Comput. Secur., vol. 110, Nov. 2021. URL: https://www.researchgate.net/publication/354043076_Serious_Games_as_a_Tool_to_Model_Attack_and_Defense_Scenarios_for_Cyber-Security_Exercises

25. D. Gernhardt, S. Groš, G. Gledec, “Innovating cyber defense with tactical simulators for management-level incident response,” Information, vol. 16, no. 5, May 2025. URL: https://www.mdpi.com/2078-2489/16/5/398

26. D.-W. Kim, G.-Y. Sin, K. Kim, J. Kang, S.-Y. Im, M.-M. Han, “Network traffic synthesis and simulation framework for cybersecurity exercise systems,” Computers, Mater. Continua, vol. 78, no. 1, 2024. URL: https://www.researchgate.net/publication/383192160_Network_Traffic_Synthesis_and_Simulation_Framework_for_Cybersecurity_Exercise_Systems

27. X. Wei, L. Chen, S. Li, M. Zeng, “Research on cyber security attack and defence strategy simulation in a virtual network environment,” 2025. URL: https://www.semanticscholar.org/paper/Research-on-cyber-security-attack-and-defence-in-a-Wei-Chen/09b085874fb47bbbcc0261bb7be2bdf8fc70f4a0

28. D. Tymoshchuk, V. Yatskiv, V. Tymoshchuk, N. Yatskiv, “Interactive cybersecurity training system based on simulation environments,” Measuring and Computing Devices in Technological Processes, no. 4(80), 2024. URL: https://www.researchgate.net/publication/386545861_INTERACTIVE_CYBERSECURITY_TRAINING_SYSTEM_BASED_ON_SIMULATION_ENVIRONMENTS

29. Chandratre, Prof & Bhosale, Satyam & Kamble, Mayank & Kamthe, Mitesh. (2025). Cybercrescendo: Interactive Cybersecurity Virtual Lab for Real-Time Attack Simulation and Hands-On Defense Training. International Journal of Advanced Research in Science, Communication and Technology. 346-353. 10.48175/IJARSCT-25058.
URL: https://www.researchgate.net/publication/390637019_Cybercrescendo_Interactive_Cybersecurity_Virtual_Lab_for_Real-Time_Attack_Simulation_and_Hands-On_Defense_Training

30. D.-H. Lee, C.-M. Kim, H.-S. Song, Y.-H. Lee, W. Chung, “Simulation-based cybersecurity testing and evaluation method for connected car V2X application using virtual machine,” Sensors, vol. 23, no. 3, Jan. 2023. URL: https://www.mdpi.com/1424-8220/23/3/1421

31. T. Khiaonarong, K. Korpinen, E. Islam, “Using simulations for cyber stress testing exercises,” IMF Working Paper, May 2025. URL: https://www.imf.org/en/publications/wp/issues/2025/05/02/using-simulations-for-cyber-stress-testing-exercises-566489

32. Mazaher Kianpour, Ulrik Franke, The use of simulations in economic cybersecurity decision-making, Journal of Cybersecurity, Volume 11, Issue 1, 2025, tyaf003, URL: https://doi.org/10.1093/cybsec/tyaf003

33. A. Javadpour, F. Ja’fari, T. Taleb, M. Shojafar, C. Benzaïd, “A comprehensive survey on cyber deception techniques to improve honeypot performance,” Comput. Secur., vol. 138, Mar. 2024. URL: https://oulurepo.oulu.fi/bitstream/handle/10024/48484/nbnfioulu-202403262445.pdf?sequence=1&isAllowed=y

34. L. Zhang, V. Thing, “Three decades of deception techniques in active cyber defense – retrospect and outlook,” Comput. Secur., vol. 108, Apr. 2021. URL: https://www.researchgate.net/publication/350750138_Three_Decades_of_Deception_Techniques_in_Active_Cyber_Defense_-_Retrospect_and_Outlook

35. M. Kouremetis, D. Lawrence, R. Alford, et al., “Mirage: cyber deception against autonomous cyber attacks in emulation and simulation,” Ann. Telecommun., 2024. URL: https://link.springer.com/article/10.1007/s12243-024-01018-4

36. A. Jaber, L. Fritsch, “Towards AI-powered cybersecurity attack modeling with simulation tools: review of attack simulators,” 2022. URL: https://www.researchgate.net/publication/364436495_Towards_AI-powered_Cybersecurity_Attack_Modeling_with_Simulation_Tools_Review_of_Attack_Simulators

37. D. Cabuya-Padilla, D. Díaz López, J. Martínez-Páez, L. Hernández, C. Castañeda Marroquín, “SERDUX-MARCIM: maritime cyberattack simulation using dynamic modeling, compartmental models in epidemiology and agent-based modeling,” Int. J. Inf. Secur., May 2025. URL: https://link.springer.com/article/10.1007/s10207-025-00985-6

38. D. J. Condori-Churata, Y. N. Laqui-Huilahuaña, J. E. Huerta-Barrantes, et al., “Bridging theory and practice: a hybrid malware detection system with 3D propagation visualization for cybersecurity training,” J. Posthumanism, vol. 5, no. 9, 2025. URL: https://posthumanism.co.uk/jp/article/view/3335

39. Nestoras Chouliaras, G. Kittes, I. Kantzavelou, L. Maglaras, G. Pantziou, M. Ferrag, “Cyber ranges and security testbeds: Scenarios, functions, tools and architecture,” Comput. Secur., 2019. URL: https://www.sciencedirect.com/science/article/abs/pii/S0167404819301804

40. Muhammad Mudassar Yamin, Basel Katt, Vasileios Gkioulos, “Cyber ranges and testbeds: Scenarios, functions, tools and architecture,” Comput. Secur., 2019. URL: https://www.sciencedirect.com/science/article/abs/pii/S0167404819301804

41. Nestoras Chouliaras, G. Kittes, I. Kantzavelou, L. Maglaras, G. Pantziou, M. Ferrag, “Cyber Ranges and TestBeds for Education, Training, and Research,” Appl. Sci., 2021. URL: https://www.mdpi.com/2076-3417/11/4/1809

42. Maria Leitner, Maximilian Frank, Wolfgang Hotwagner, Gregor Langner, O. Maurhart, Timea Pahi, Lenhard Reuter, Florian Skopik, Paul Smith, M. Warum,

"AIT Cyber Range: Flexible cyber security environment for exercises, training and research," Proc. Eur. Interdiscip. Cybersecurity Conf., 2020. URL: https://www.skopik.at/ait/2020_eicc.pdf

43. Komal Vekaria, Prasad Calyam, Songjie Wang, Ramya Payyavula, Matthew Rockey, Nafis Ahmed, "Cyber Range for research-inspired learning of 'attack defense by pretense' principle and practice," IEEE Trans. Learn. Technol., 2021. URL: https://ieeexplore.ieee.org/abstract/document/9463747

44. T. Cruz, P. Simões, "Down the rabbit hole: Fostering active learning through guided exploration of a SCADA cyber range," Appl. Sci., 2021. URL: Down the Rabbit Hole: Fostering Active Learning through Guided Exploration of a SCADA Cyber Range

45. Manos Vasilakis, Konstantinos Karampidis, Manolis G. Tampouratzis, Athanasios Malamos, S. Panagiotakis, G. Papadourakis, "Enhancing Industry 4.0 cybersecurity training through cyber range platform," Proc. 5th Int. Conf. Electronic Engineering, Information Technology & Education, 2024. URL: https://www.researchgate.net/publication/383796872_Enhancing_Industry_40_Cybersecurity_Training_through_Cyber_Range_Platform

46. Muhammad Ali Hamza, Usama Ejaz, Hyun-chul Kim, "Cyber5Gym: An integrated framework for 5G cybersecurity training," Electronics, 2024. URL: https://www.mdpi.com/2079-9292/13/5/888

47. P. Nespoli, Mariano Albaladejo-González, J. Ruipérez-Valiente, Joaquin Garcia-Alfaro, "SCORPION Cyber Range: Fully customizable cyberexercises, gamification and learning analytics to train cybersecurity competencies," 2024. URL: https://arxiv.org/abs/2401.12594

48. Sanggyu Shin, Y. Seto, "CyExec – Training platform for cybersecurity education based on a virtual environment," Int. J. Learn. Technol. Learn. Environ., 2020. URL: https://www.iaiai.org/journals/index.php/IJLTLE/article/view/517/427

49. D. Bergin, "Cyber-attack and defense simulation framework," J. Defense Model. Simul., 2015. DOI:10.1109/LCN.2009.5355149

50. Dmytro Tymoshchuk, Vasyl Yatskiv, Vitaliy Tymoshchuk, N. Yatskiv, “Interactive cybersecurity training system based on simulation environments,” Measuring and Computing Devices in Technological Processes, 2024. URL: https://www.researchgate.net/publication/387669672_Interactive_cybersecurity_training_system_based_on_simulation_environments

51. Likhith G, S. M, “Adaptive cyber defense: Realistic SOC workflow implementation,” Int. J. Res. Appl. Sci. Eng. Technol., 2025. URL: https://www.ijraset.com/research-paper/adaptive-cyber-defense-realistic-soc-workflow-implementation

52. Muhammad Mudassar Yamin, Ehtesham Hashmi, Mohib Ullah, Basel Katt, “Applications of LLMs for generating cyber security exercise scenarios,” IEEE Access, 2024. URL: https://www.researchgate.net/publication/378490305_Applications_of_LLMs_for_Generating_Cyber_Security_Exercise_Scenarios

53. M. Yamin, Basel Katt, “Modelling attack and defense scenarios on federated cyber ranges,” Proc. 2025 IEEE Int. Conf. Cyber Security and Resilience, 2025. URL: https://www.researchgate.net/publication/394982307_Modelling_Attack_and_Defense_Scenarios_on_Federated_Cyber_Ranges

54. Michael Lanier, Yevgeniy Vorobeychik, “CyGym: A Simulation-Based Game-Theoretic Analysis Framework for Cybersecurity,” arXiv, 2025. URL: https://arxiv.org/abs/2506.21688

55. Menelaos N. Katsantonis, A. Manikas, I. Mavridis, D. Gritzalis, “Cyber range design framework for cyber security education and training,” Int. J. Inf. Secur., 2023. URL: https://www.researchgate.net/publication/369361219_Cyber_range_design_framework_for_cyber_security_education_and_training

56. Elochukwu A. Ukwandu, M. B. Farah, Hanan Hindy, et al., “A Review of Cyber-Ranges and Test-Beds: Current and Future Trends,” Sensors, 2020. URL: https://www.mdpi.com/1424-8220/20/24/7148

57. Viktor Engström, Robert Lagerström, “Two decades of cyberattack simulations: A systematic literature review,” Comput. Secur., 2022. URL: https://www.researchgate.net/publication/359087597_Two_Decades_of_Cyberattack_Simulations_A_Systematic_Literature_Review

58. Lillemets, P., Jawad, N., Kashi, J., Sabah, A., & Dragoni, N. (2025). A Systematic Review of Cyber Range Taxonomies: Trends, Gaps, and a Proposed Taxonomy. Future Internet. URL: https://doi.org/10.3390/fi17060259.

59. Stytz, M., & Banks, S. (2020). Future challenges for cyber simulation. The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, 17, 47 - 49. URL: https://doi.org/10.1177/1548512919879816.

60. Noponen, S., Parssinen, J., & Salonen, J. (2022). Cybersecurity of Cyber Ranges: Threats and Mitigations. International Journal for Information Security Research. URL: https://doi.org/10.20533/ijisr.2042.4639.2022.0117.