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: “ТЕХНОЛОГІЇ СИМУЛЯЦІЙНОГО НАВЧАННЯ ЯК ЗАСІБ ПІДВИЩЕННЯ ПРАКТИЧНОЇ СПРЯМОВАНОСТІ ПІДГОТОВКИ ФАХІВЦІВ ІЗ КІБЕРБЕЗПЕКИ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

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

_____ Владислав УШАКОВ
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав(ла): здобувач(ка) вищої освіти гр. УБД-42

Владислав УШАКОВ
Ім’я, ПРІЗВИЩЕ

Керівник: Тетяна МУЖАНОВА
к. держ. упр., доцент Ім’я, ПРІЗВИЩЕ

Рецензент:
Ім’я, ПРІЗВИЩЕ

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Ушакову Владиславу Андрійовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Технології симуляційного навчання як засіб підвищення практичної спрямованості підготовки фахівців із кібербезпеки”,
керівник кваліфікаційної роботи Мужанова Тетяна Михайлівна, к.держ.упр., доцент,
(ПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “20“ лютого 2026 р. №51.

2. Строк подання кваліфікаційної роботи “12” травня 2026 р.

3. Вихідні дані до кваліфікаційної роботи: *забезпечення кібербезпеки, практично-орієнтоване навчання фахівців з кібербезпеки, симуляційні технології навчання з кібербезпеки.*

4. Перелік питань, які мають бути розроблені:

4.1. З’ясувати роль симуляційних технологій навчання у практичній підготовці кіберфахівців.

4.2. Проаналізувати види симуляційних технологій навчання з кібербезпеки.

4.3. Дослідити рішення для симуляційного навчання кіберфахівців і розробити рекомендації щодо їхнього застосування.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “05“ березня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2026	
2.	Збір та аналіз літератури.	30.03.2026	
3.	Встановлення ролі симуляційних технологій навчання у практичній підготовці кіберфахівців.	08.04.2026	
4.	Аналіз видів симуляційних технологій навчання з кібербезпеки.	15.04.2026	
5.	Дослідження рішень для симуляційного навчання кіберфахівців і розробка рекомендацій щодо їх застосування.	22.04.2026	
6.	Формулювання висновків за результатами проведеного дослідження.	29.04.2026	
7.	Оформлення роботи.	06.05.2026	
8.	Оформлення презентації.	11.05.2026	
9.	Отримання рецензії на роботу.	10.06.2026	
10.	Захист в ДЕК.	__.06.2026	

Здобувач вищої освіти _____ Владислав УШАКОВ
(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 бакалавра

Направляється здобувач Ушаков В.А. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Технології симуляційного навчання як засіб підвищення практичної спрямованості підготовки фахівців із кібербезпеки"

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач УШАКОВ Владислав у кваліфікаційній роботі з'ясував роль і переваги симуляційних технологій навчання у практичній підготовці кіберфахівців; проаналізував види симуляційних технологій навчання з кібербезпеки; дослідив рішення для симуляційного навчання кіберфахівців і розробив рекомендації щодо їхнього застосування.

УШАКОВ Владислав показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, успішно використав різні методи наукового дослідження, проявив себе як відповідальний і організований виконавець. Результати дослідження апробовані на конференції "Стратегії кіберстійкості: управління ризиками та безперервність бізнесу" 25 лютого 2026 року.

Все це дозволяє оцінити кваліфікаційну роботу здобувача УШАКОВА Владислава на позитивну оцінку та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

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

"____" _____ 2026 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Ушаков В.А. 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 бакалаврську роботу

здобувача вищої освіти УШАКОВА Владислава
на тему “Технології симуляційного навчання як засіб підвищення практичної спрямованості підготовки фахівців із кібербезпеки”

Актуальність. Як свідчить практика, традиційні методи навчання з кібербезпеки стають дедалі менш ефективними, а показники порушень внаслідок впливу людського чинника, зокрема й неналежної підготовки персоналу, залишаються високими. Так, згідно зі звітом Verizon 82% порушень кібербезпеки пов'язані з людським фактором. Водночас, симуляційні технології трансформують навчання в галузі кібербезпеки, забезпечуючи його практичну спрямованість і набуття досвіду реагування на інциденти кібербезпеки в контрольованому і безпечному середовищі.

З огляду на зазначене дослідження технологій симуляційного навчання як засіб підвищення практичної спрямованості підготовки фахівців із кібербезпеки є актуальним науковим завданням.

Позитивні сторони.

1. У роботі досліджено особливості використання симуляційних навчальних технологій в галузі кібербезпеки з акцентом на види і сценарії навчання, а також переваги практично-орієнтованих вправ для посилення кіберзахисту організації.

2. Кваліфікаційна робота оформлена згідно з вимогами. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків.

3. Автор опрацював значну джерельну базу: понад 50 публікацій, в тому числі англомовних, проаналізував ринок симуляційних онлайн-рішень для навчання в галузі кібербезпеки.

4. За результатами дослідження запропоновано рекомендації щодо ефективного застосування симуляційних технологій навчання в кібербезпеці.

Недоліки.

Доцільно було б приділити більше уваги питанням організації симуляційного навчання на корпоративному рівні, зокрема підбір форм і методів тренування, періодичність і охоплення всього персоналу.

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

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує позитивної оцінки, а здобувач УШАКОВ Владислав заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____ _____

підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню технологій симуляційного навчання як засобу підвищення практичної спрямованості підготовки фахівців із кібербезпеки. Робота складається зі вступу, трьох розділів, що містять 15 рисунків і 2 таблиці, висновків і списку використаних джерел із 52 найменувань. Загальний обсяг роботи становить 86 аркушів, з яких 5 аркушів займає список використаних джерел.

Метою роботи є дослідження технологій симуляційного навчання як засобу підвищення практичної спрямованості підготовки фахівців із кібербезпеки.

Об'єктом дослідження є засоби підвищення практичної спрямованості підготовки фахівців із кібербезпеки.

Предмет дослідження – технології симуляційного навчання як засіб підвищення практичної спрямованості підготовки фахівців із кібербезпеки.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, моделювання та прогнозування, узагальнення кращих практик навчання з кібербезпеки.

Як результат у роботі встановлено роль симуляційних технологій навчання у практичній підготовці кіберфахівців; проаналізовано види симуляційних технологій навчання з кібербезпеки; досліджено рішення для симуляційного навчання кіберфахівців і розроблено рекомендації щодо їхнього застосування.

Галузь застосування. Розроблені підходи можуть бути використані при плануванні та реалізації корпоративної системи навчання з кібербезпеки в контексті забезпечення його практичної спрямованості.

Ключові слова: ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ, ПРАКТИЧНО-ОРІЄНТОВАНЕ НАВЧАННЯ В ГАЛУЗІ КІБЕРБЕЗПЕКИ, СИМУЛЯЦІЙНІ ТЕХНОЛОГІЇ НАВЧАННЯ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ.

ABSTRACT

The qualification work is devoted to the study of simulation training technologies as a tool for improving the practical focus of cybersecurity specialists training. The work consists of an introduction, three chapters containing 15 figures and 2 tables, conclusions and the list of references containing 52 items. The total volume of the work is 86 pages, of which 4 pages are occupied by the list of references.

The purpose of the study is to study simulation training technologies as a tool for improving the practical focus of cybersecurity specialists training.

The object the study is tools for improving the practical focus of cybersecurity specialists training.

The subject of the study is simulation training technologies as a tool for improving the practical focus of cybersecurity specialists training.

Research methods. In order to solve the mentioned higher scientific task, the methods of analysis and synthesis, comparison, classification, forecasting, modeling, as well as generalization of best practices in cybersecurity training were used.

As a result, the work establishes the role of simulation training technologies in the practical training of cyber specialists; analyzes the types of simulation technologies for cybersecurity training; investigates solutions for simulation training of cyber specialists and develops recommendations for their application.

Field of application. The developed approaches can be used in planning and implementing a corporate cybersecurity training system in the context of ensuring its practical orientation.

Keywords: CYBER SECURITY, PRACTICAL TRAINING IN CYBER SECURITY, SIMULATION TECHNOLOGIES OF CYBER SECURITY SPECIALISTS TRAINING.

ЗМІСТ

ВСТУП 9
РОЗДІЛ 1 РОЛЬ СИМУЛЯЦІЙНИХ ТЕХНОЛОГІЙ НАВЧАННЯ У ПРАКТИЧНІЙ ПІДГОТОВЦІ КІБЕРФАХІВЦІВ 11
1.1 Напрями застосування симуляційних технологій у кібербезпеці 11
1.2 Переваги симуляційних методів навчання в галузі кібербезпеки 18
1.3 Основні види сценаріїв симуляційного навчання кіберфахівців 24
Висновки до розділу 1 32
РОЗДІЛ 2 ВИДИ СИМУЛЯЦІЙНИХ ТЕХНОЛОГІЙ НАВЧАННЯ З КІБЕРБЕЗПЕКИ 34
2.1 Штабні навчання з кібербезпеки 35
2.2 Навчання червоної команди 40
2.3 Змагання «Захоплення прапора» 46
2.4 Навчальні кіберполігони 51
Висновки до розділу 2 57
РОЗДІЛ 3 РІШЕННЯ ДЛЯ СИМУЛЯЦІЙНОГО НАВЧАННЯ КІБЕРФАХІВЦІВ І РЕКОМЕНДАЦІЇ ЩОДО ЇХНЬОГО ЗАСТОСУВАННЯ 59
3.1 Кращі симуляційні онлайн-платформи для навчання з кібербезпеки 59
3.2 Розробка симуляцій на основі ШІ для навчання кібербезпеці 66
3.3 Практичні рекомендації щодо ефективного застосування симуляційного навчання 72
Висновки до розділу 3 78
ВИСНОВКИ 80
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 82

ВСТУП

Актуальність теми. У сучасних умовах, коли вплив людського чинника на стан захищеності ІКС та інформаційних активів організації залишається традиційно високим, проведення ефективного навчання персоналу й кіберфахівців набуває життєво важливого значення. З огляду на те, що традиційні методи навчання з кібербезпеки стають дедалі менш ефективними і не задовольняють актуальних потреб і очікувань роботодавців, виникає нагальна потреба у використанні нових навчальних підходів. Насамперед слід розглянути симуляційні технології, які трансформують навчання в галузі кібербезпеки, забезпечуючи його практичну спрямованість і набуття працівниками досвіду реагування на кіберінциденти і командної роботи в контрольованому і безпечному середовищі.

З огляду на зазначене дослідження технологій симуляційного навчання як засобу підвищення практичної спрямованості підготовки фахівців із кібербезпеки є актуальним науковим завданням.

Мета роботи полягає у дослідженні технологій симуляційного навчання як засобу підвищення практичної спрямованості підготовки фахівців із кібербезпеки.

Об'єкт дослідження **–** засоби підвищення практичної спрямованості підготовки фахівців із кібербезпеки.

Предмет дослідження – технології симуляційного навчання як засіб підвищення практичної спрямованості підготовки фахівців із кібербезпеки.

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

1. Встановити роль симуляційних технологій навчання у практичній підготовці кіберфахівців.

2. Проаналізувати види симуляційних технологій навчання з кібербезпеки.

3. Дослідити рішення для симуляційного навчання кіберфахівців і розробити рекомендації щодо їхнього застосування.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння,

класифікації, моделювання та прогнозування, узагальнення кращих практик навчання з кібербезпеки.

Практичне значення одержаних результатів. Застосування напрацювань дослідження дасть змогу здійснити обґрунтований вибір методів та інструментів симуляційного моделювання як обов'язкового елемента корпоративної системи практично-спрямованого навчання з кібербезпеки організації з урахуванням потреб і можливостей організації.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції "Стратегії кіберстійкості: управління ризиками та безперервність бізнесу" 25 лютого 2026 року.

РОЗДІЛ 1
РОЛЬ СИМУЛЯЦІЙНИХ ТЕХНОЛОГІЙ НАВЧАННЯ У ПРАКТИЧНІЙ ПІДГОТОВЦІ КІБЕРФАХІВЦІВ

1.1 Напрями застосування симуляційних технологій у кібербезпеці

На нинішньому етапі розвитку симуляційні технології в кібербезпеці створюють безпечні віртуалізовані середовища для моделювання реальних атак, перевірки захисту й навчання персоналу без ризику для реальної інфраструктури. Ці інструменти дозволяють організаціям виявляти вразливості, тестувати реагування на інциденти й імітувати методи зловмисників у реальному часі. За результатами дослідження встановлено такі основні напрями використання симуляційних технологій у галузі кібербезпеки (Рис. 1.1)

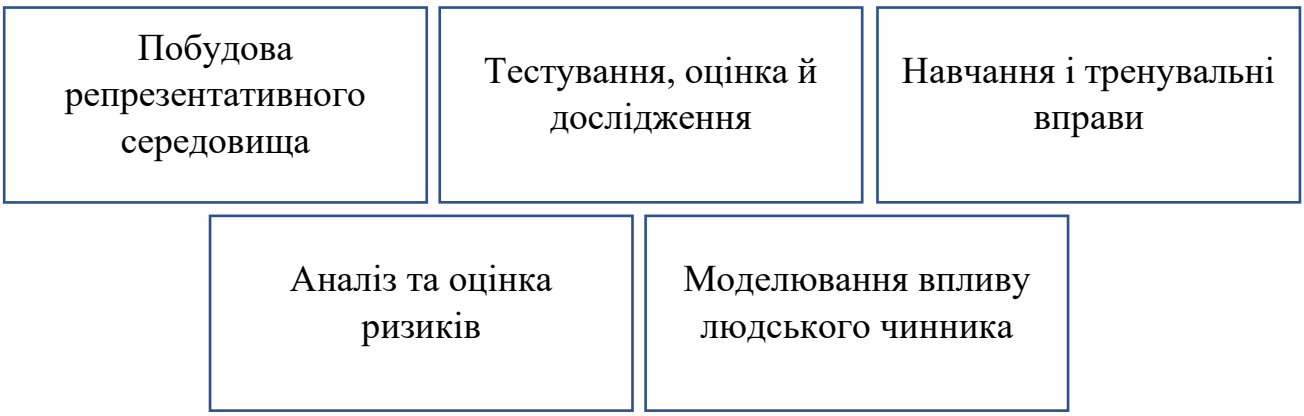

Рис. 1.1. Напрями використання симуляційних технологій у кібербезпеці

Побудова репрезентативного середовища стосується створення мереж та підключених систем як платформи для тестування. Програмні симулятори мереж та алгоритми мережевого трафіку можуть бути використані для тестування певних типів кібератак. Бібліотеки та інструменти для моделювання мереж з відкритим кодом та комерційні продукти використовуються для реалізації симуляційного мережевого середовища. Перші спроби мережевих симуляторів були розроблені в 1980-х роках переважно для тестування різних алгоритмів маршрутизації та планування [1].

Широке використання таких симульованих мереж стало можливим пізніше, коли обчислювальна потужність зросла, а кібератаки стали поширеними. Пізніші розробки були зразками надійного програмного забезпечення з відкритим кодом, здатного симулювати широкий спектр пристроїв, таких як дротові/бездротові комунікаційні мережі, сенсорні мережі та вбудовані мережі тощо. Нині існує багато інших варіантів мережевих симуляторів, які класифікуються за типом, режимом розгортання, мережевими порушеннями й підтримуваними протоколами. Мережеві симулятори зазвичай включають лише представлення пристроїв, технологій та зв'язку між ними, пропускаючи деякі критичні компоненти кіберсценарію.

Однак інші розробники запропонували застосовувати до побудови репрезентативного середовища «живий, віртуальний, конструктивний» (LVC) підхід, який охоплює живу (кібер) симуляцію, де реальні актори взаємодіють з фізичними системами реальних комп'ютерів, підключених до реальних і зазвичай ізольованих мереж; віртуальну (кібер) симуляцію, де реальні актори взаємодіють з емуляцією або симуляцією мереж, або емульовані чи симульовані актори взаємодіють з реальними та зазвичай ізольованими мережами; конструктивну (кібер) симуляцію, в якій симульовані або емульовані актори взаємодіють з емуляціями або симуляціями мереж [2].

Наприклад, був розроблений фреймворк LVC під назвою StealthNet для підтримки тестування, оцінки й навчання з використанням сценаріїв кібербезпеки. Розробка містить моделі поведінки користувачів, що представляють сині та червоні команди. Згідно з прикладом сценарію, який вони представляють, червоні сили виконують заздалегідь визначені дії в сценарії DDoS, однак, він не може адаптуватися до різних умов у динаміці.

Деякі з подальших розробок для кібернавчання та тестування, наприклад платформа LVC Emulytics від Sandia National Lab, передбачають механізми швидкої специфікації та розгортання мереж, підтримку протоколів для мережевих пристроїв, створення екземплярів мереж з великою кількістю вузлів і представлення дротового та бездротового зв'язку.

Загалом, використання великої кількості варіантів з відкритим кодом, симуляційні технології позитивно вплинути на декілька галузей кібербезпеки, серед яких тестування, оцінка та дослідження безпеки.

Тестування, оцінка та дослідження. Симуляційні можливості для дослідження, тестування й оцінки ситуації, ймовірно, використовуються найширше внаслідок швидкості і гнучкості експериментування. Типовими прикладами використання симуляцій за цим напрямом є оцінювання алгоритмів виявлення вторгнень, класифікація мережевих атак, визначення оптимального розміщення систем IDS/IPS у великих мережах, сегментація мережі для ускладнення отримання зловмисниками доступу до мережі, моделювання кібератак, методів захисту й наслідків, специфікація систем дискретних подій (DEVS) із системою навчання на основі знань для зловмисника та статистичним аналізатором для оцінки вразливостей.

Моделювання може класифікувати загрози, визначати механізми атаки, перевіряти механізми захисту та оцінювати наслідки [3].

Подальше вдосконалення таких розробок мало на меті розширення захисту «в ширину» шляхом поєднання систем IDS, обманних технологій і системи захисту від рухомих цілей (Moving Target Defense MTD). Системи обману, зокрема приманки «honeypots», які здаються реальними частинами мережі, впроваджуються для введення зловмисника в оману та вивчення його поведінки. MTD дозволяють захисникам автоматично змінювати поведінку, політики або конфігурації системи таким чином, щоб потенційні поверхні атаки динамічно переміщувалися.

Для оцінки впливу загроз і атак була розроблена агентно-орієнтована система симулювання - розподілений симулятор відмови в обслуговуванні (DDoSSIM), який здійснює оцінку різних механізмів DDoS-атак і захисту, сформованих програмними агентами. Крім цього завдяки симуляційним технологіям здійснювався аналіз стійкості мережі у разі DoS-атаки на мережу.

Іншими прикладами використання симуляцій є моделювання масштабних атак шляхом автоматичного налаштування хост-агентів на основі зразків

фонового трафіку та поточних моделей шкідливого трафіку; моделювання й імітація різних змін кіберекосистеми, таких як загрози та захисні стратегії; оцінювання впроваджених механізмів безпеки в інтелектуальних мережах, а також застосовності метрик на основі вимірювання даних трафіку.

Іншим аспектом є використання симуляцій для пошуку умов, за яких безпека може бути вразливою, тобто визначення комбінації вхідних факторів, які призводять до бажаного (або небажаного) результату.

Крім систем IDS, які є першою лінією кіберзахисту симуляцію використовують для моделювання поведінки шкідливих програм на основі моделей їхньої активності в різних мережах, зокрема безмасштабних, Wi-Fi та інтелектуальних мережах. Тут симуляційні дослідження дозволяють безпечно тестувати реальне або гіпотетичне поширення шкідливого ПЗ і оцінювати потенційні заходи щодо пом'якшення наслідків.

В останні роки симуляційні технології дають можливість досліджувати та розуміти потенційні сценарії та перевіряти їх на відповідність існуючим системам виявлення, а також проводити навчальні вправи й аналіз ризиків. Останнім часом таке генерування синтетичних даних також спирається на мережі загальної змагальності.

Основні практичні приклади використання симуляційних технологій для тестування, оцінка та дослідження показані на рис. 1.2 [1].

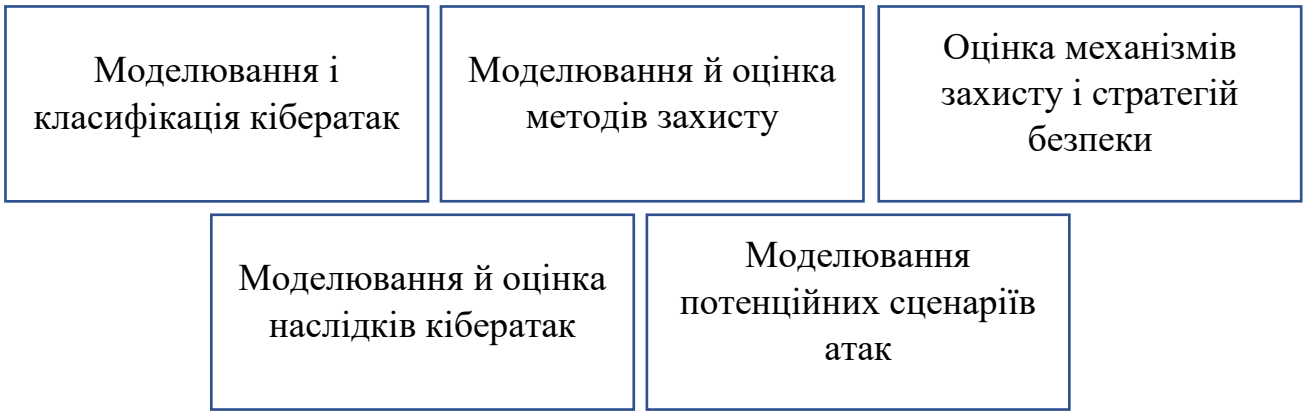

Рис. 1.2. Основні кейси використання симуляційних технологій для тестування, оцінки та дослідження

Аналіз та оцінка ризиків. Як зазначалося раніше, метою кібербезпеки є захист кіберпростору за допомогою превентивних заходів. Створення репрезентативного операційного середовища для тестування, оцінки та навчання проти потенційних атак і стратегічного захисту є важливим елементом. Однак розмір і масштаб потенційних кібератак роблять повну безпеку неможливою. Системи все ще піддаються ризикам, які можна проаналізувати та пом'якшити.

Аналіз ризиків – це функція, яка досліджує ймовірність негативного результату. При застосуванні цієї концепції до кібербезпеки, загрози зазвичай вимірюються за такими критеріями як: ймовірність типу атаки, ймовірність успіху атаки і збитків, пов'язаних з успішною атакою. Однак кількісна оцінка втрат не є простим завданням у кіберпросторі. Втрати залежать від часу, не проявляються, доки не буде виявлено порушення, і можуть зменшити майбутню цінність, наприклад, втрату інтелектуальної власності. Втрати можуть залежати від стороннього постачальника послуг, тобто взаємозалежності можуть створювати втрати для суб'єкта, який не був безпосередньо атакований. Існує кілька підходів до аналізу ризиків:

- оцінка ймовірності ризику (Probalbility Risk Assessment, PRA);
- аналіз дерева атак (Attack Tree Analysis, ATA);
- аналіз дерева відмов (Fault Tree Analysis, FTA);
- аналіз наслідків відмов (Failure Mode and Effects Analysis, FMEA).

PRA кількісно визначає ризики на основі статистичних ймовірностей. PRA має загальні етапи: ідентифікація, кількісна оцінка, оцінка та прийняття.

PRA є теоретично обґрунтованим підходом і застосовується в різних сценаріях, таких як DDoS-атаки на систему дистанційного навчання та втрати виробництва в електромережі. Моделювання Монте-Карло часто застосовується для приблизної оцінки втрати вартості. Незважаючи на ці переваги, PRA все ще стикається з кількома проблемами при застосуванні до кібербезпеки: не підтримуються історичні бази даних; дані безпеки зазвичай не поширюються, незважаючи на значну кількість порушень; існуючі дані важко аналізувати для великих, складних мереж [4].

З цією метою докладається безліч зусиль для заохочення та стимулювання стандартизації, використання та обміну даними кіберрозвідки. Для багатьох організацій рішення брати участь у програмах обміну кіберрозвідувальними даними стало ідеальним випадком для зусиль з теорії ігор.

Дерева атак забезпечують формальний засіб опису та аналізу безпеки систем на основі різних атак. Моделювання використовувалися як для створення, так і для оцінки дерев атак. Генерація дерева атак включає моделювання зловмисника та його запуск для імітації атак, які використовуються для генерації дерева. Оцінка дерев атак включає представлення системи за допомогою відповідної методики та проведення методу Монте-Карло.

FTA використовує систематичне зворотне міркування для визначення ймовірностей, а FMEA використовує прямо-індуктивний підхід для того ж самого. Ці методи досліджують лише одну помилку.

Зовсім недавно дослідники використовували симулювання для аналізу ризиків у складних та взаємозалежних системах, зокрема для оцінки каскадних ефектів атаки на ланцюг постачань, вивчення впливу атаки (і подальшого захисту) на критичну інфраструктуру, аналізу та оцінки систем контролю безпеки та збору даних (SCADA), моделювання процесу експлуатації вразливостей для визначення масштабу наслідків [1].

Відомим прикладом є застосування теоретико-ігрового підходу до управління ризиками кібербезпеки за допомогою гри кібербезпеки (CSG), яка використовує моделі для опису системи, середовища загроз і можливостей захисника, який призначається для подальшого інформування осіб, які приймають рішення, про прийнятні принципи проектування безпеки, цілеспрямовані покращення, економічно ефективні інвестиції у зниження ризиків та засади розгортання засобів захисту.

Різноманіття видів і різні показники ймовірності атак, а також каскадний ефект взаємозалежностей ускладнюють оцінку ризиків у кібербезпеці. Це ще більше ускладнюється людським чинником: від недбалого і скомпрометованого користувача до рішучого зловмисника, від рядового працівника до

кваліфікованого кіберфахівця, кожен з яких нерідко відіграє ключову роль у належному використанні або зловживанні у кіберпросторі.

Людський чинник у кібербезпеці. Окремо слід звернути увагу на можливості використання симуляційних технологій у контексті подолання негативного впливу на кібербезпеку людського чинника. Зловмисники, аналітики кібербезпеки (CSA), системні адміністратори та пересічні користувачі системи взаємодіють, формуючи кіберпростір сьогодні. Тому кожного з них необхідно враховувати при забезпеченні кібербезпеки. Зловмисники можуть бути «скрипт-кідді», державними хакерами, організованими злочинними групами, інсайдерами, аматорами, хактивістами, легітимними тестувальниками на проникнення або терористами. Їхня роль у кіберпросторі визначається їхніми навичками, знаннями, ресурсами, доступом та мотивами.

Незважаючи на те, що технології покращили захист ІКС, він все ще сильно залежить від того, хто опікується системами і має до них доступ.

Дії людини, зокрема її злочинна поведінка, значно рідше ставали об’єктом симулювання у порівнянні з симуляціями мережевих вторгнень та інших форм кібератак. Ранні моделі містили заздалегідь задані, статичні шаблони, яким мали слідувати агенти зловмисника. Ці моделі зрештою поступилися місцем ігровим та когнітивним моделям, які забезпечують корисну характеристику ініціації атаки, але ігнорують безліч інших соціальних контекстів: взаємодію користувачів, толерантність до ризику, соціальне навчання тощо [5].

Навіть новіші моделі сегментації мережі, такі як AVAIL, які покращують симуляції безпеки шляхом розвитку стратегій як зловмисника, так і захисника, не мають динамічного поведінкового компонента.

Водночас, відомими є симуляційні дослідження таких показників, як навмисні маркери, значущі помилки, підготовча поведінка, корельовані моделі використання, вербальна поведінка і риси особистості з метою передбачення, який суб’єкт може бути активною внутрішньою загрозою, а також факторів (розмір групи, рівень успішності атаки і можливості її реалізації), які

перетворюють схильного до порушень безпеки користувача на кібернападника. Крім цього об’єктом моделювання був процес скоєння злочину.

Хоча зловмисники намагаються знайти несанкціоновані способи використання системи, агенти з кібербезпеки повинні оцінювати інформацію, надану системами, щоб визначити рівень потенційного ризику. Саме повідомлення про ризик, засоби комунікації та процес прийняття індивідуальних рішень впливають на реакцію на ризик і сповіщення. Існує лише обмежена кількість моделей поведінки агентів з кібербезпеки, наприклад агентна модель для фіксації співпраці фахівців з кібербезпеки для обміну знаннями про виявлення атак. Модель симулює ефективність співпраці у збільшенні кількості вирішених сповіщень.

Проблеми користувачів не є широко розробленими у симуляційних технологіях кібербезпеки. Серед відомих прикладів слід згадати програмну модель користувачів як суб’єктів з набором притаманних кожному переконань, бажань і намірів (belief, desire, intention - BDI), які виконують свої рутинні завдання і комунікують один з одним. Деякі симуляційні моделі кібератак дозволяють зафіксувати стійкість користувача, зміни в моделях комунікації та їх вплив на виконання завдань.

Знову ж таки, цей когнітивний підхід фіксує людину як раціонального суб’єкта прийняття рішень, залишаючи поза увагою поведінкові складнощі, які можуть бути більш показовими при розгляді таких ситуацій, як атаки соціальної інженерії [6].

1.2 Переваги симуляційних методів навчання в галузі кібербезпеки

Як свідчить практика, традиційні методи навчання з кібербезпеки стають дедалі менш ефективними. Оскільки організації стикаються зі складними атаками, що поєднують технічні експлойти із соціальною інженерією, лише теоретичних знань недостатньо для підготовки команд безпеки до реальних сценаріїв. Згідно зі звітом IBM, компанії, які регулярно проводять симуляції

безпеки, мають на 35% нижчі витрати, пов’язані з порушеннями даних, порівняно з тими, хто не проводить таких програм [7].

З’ясуємо, чому традиційне навчання з кібербезпеки не відповідає сучасним потребам і очікуванням галузі.

Протягом десятиліть організації покладалися на програми обізнаності з безпеки, спрямовані на дотримання нормативних вимог: щорічне відеонавчання, перевірка знання політик і періодичні тести на виявлення фішингових атак. Хоча ці методи формують базове розуміння персоналу з питань кібербезпеки, вони не розвивають критичного мислення і навичок адаптивного реагування, необхідних під час реальних інцидентів безпеки.

Про наявні недоліки традиційної системи навчання кіберпрофесіоналів однозначно свідчить статистика:

– 82% порушень кібербезпеки пов'язані з людським фактором, згідно зі звітом Verizon про розслідування витоків даних;

– тільки 16% фахівців з кібербезпеки вважають, що їхні організації достатньо ефективні у виявленні інцидентів безпеки;

– організації, які регулярно використовують симуляційні методи безпеки скорочують час реагування на інциденти на 75% [8].

Ці цифри підтверджують зростаючий розрив між теоретичними знаннями з безпеки та їхнім практичним застосуванням. Хоча більшість працівників можуть визначити поширені вектори атак під час тестування, їм важко розпізнати й реагувати на ці загрози в реалістичних сценаріях, де наявні контекст і стресові чинники.

Симуляційні технології трансформують навчання в галузі кібербезпеки, запускаючи механізми експериментального навчання – процесу навчання через досвід і самопізнання. Коли учасники беруть участь у реалістичних сценаріях безпеки, вони розвивають контекстне розуміння, тобто вчаться розпізнавати, як атаки розгортаються в конкретному середовищі; м'язову пам'ять через автоматизацію початкових дій реагування шляхом повторення; адаптивне

мислення шляхом розвитку здатності реагування на нові загрози; навички співпраці й координації дій реагування між командами [9].

Завдяки навчанню з використанням симуляційних технологій працівники знайомляться з контрольованими і безпечними версіями реальних кібератак, зокрема фішингом, вішингом, смішингом, діпфейками та іншими тактиками соціальної інженерії, – для оцінювання й посилення власної реакції.

Симуляції надають керівникам з інформаційної безпеки, менеджерам сфер корпоративного управління, управління ризиками й забезпечення нормативної відповідності, а також посадовим особам, які відповідають за впровадження програм підвищення обізнаності й навчання з кібербезпеки, реальні показники ризиків внаслідок поведінки персоналу, які традиційне статичне навчання не може отримати. Симуляційні технології дозволяють встановити, які помилки роблять працівники, як швидко вони ескалюють інциденти, які робочі процеси найбільш вразливі до розкриття конфіденційної інформації. Завдяки сучасним інструментам для симуляції фішингу, які розроблені на основі поведінкової аналітики, можна встановити спосіб мислення, реагування і прийняття рішень кожного працівника [10].

Оскільки кіберзлочинці активно впроваджують автоматизацію, фішинг, згенерований ШІ, та все більш таргетовані методи соціальної інженерії, організаціям потрібне навчання з кібербезпеки, яке адаптується так само швидко і відповідає низці вимог.

Швидкість і наближеність до реальності. Як свідчить практика, зловмисники виконують багаторазове повторення кібернападів швидше, ніж оновлюється більшість навчальних програм. Нові фішингові інструменти з'являються щодня, а механізми ШІ можуть генерувати тисячі персоналізованих приманок за лічені хвилини. Статичне навчання з підвищення обізнаності щодо безпеки просто не може встигнути реагувати в такому темпі.

Нещодавні галузеві дані показали, що понад 90% порушень кібербезпеки пов'язані з певною, часто новою формою соціальної інженерії [11], що підкреслює необхідність навчатися на актуальних векторах атак. У цьому

контексті симуляційне навчання має особливе значення, оскільки дозволяє змоделювати реальні атаки в контрольованому середовищі, відображаючи сучасні тактики, такі як діпфейковий вішинг, фішинг QR-кодів, робочі процеси збору облікових даних і плацдарми програм-вимагачів.

Акцент на формування практичних навичок. Сьогодні найбільш важливим результатом навчання є не інформування персоналу про кіберзагрози та методи реагування, а зміна або формування нових зразків поведінки в разі реалізації кібератаки.

На відміну від результатів тестування і рейтингів їх проходження, які не можуть дати уявлення про поведінку працівників під час реального інциденту, навчання на основі симуляції надає вимірне розуміння людського ризику, зокрема щодо частоти натискань на клавіші, частоти звітів, часу затримки, ризикованих моделей і конкретних типів атак, з якими стикається кожна команда.

Завдяки навчальним симуляція можна кількісно виміряти людську поведінку під час реагування на кіберзагрози, а отже й адаптувати методи навчання, покращити реагування на інциденти і відстежувати прогрес з часом.

Адаптивність до застосування в різних сферах. Слід відзначити, що кібератаки рідко спрямовані власне на сектор IT та захисту інформації. Сучасні фішингові кампанії націлені на команди з бухгалтерського обліку, діяльність помічників керівників і HR-менеджерів, привілейованих користувачів, процеси прийняття важливих фінансових рішень тощо. З огляду на це симуляції кіберзагроз мають бути специфічними для різних сфер, кожній з яких притаманні свої особливості. Адаптуючи симуляції до кожної функції, організації зміцнюють не лише свої технічні команди, а й усю корпоративну систему захисту персоналу [10].

Симуляційне навчання є актуальним і перспективним для використання в галузі кібербезпеки, оскільки воно має цілий ряд беззаперечних переваг для підприємств та організацій (Рис. 1.3).

Розглянемо основні з них.

Симуляційні навчальні технології забезпечують практичну спрямованість навчання й набуття досвіду реагування на інциденти кібербезпеки в контрольованому середовищі і дозволяють організаціям:

– покращувати знання і навички своїх працівників, які дізнаються про різні типи атак і процедури реагування через участь у симульованих сценаріях;

Рис. 1.3. Переваги симуляційних технологій навчання

– перевіряти готовність персоналу належним чином реагувати на кіберзагрози, зокрема надання швидкої і адекватної відповіді на загрози, дотримання планів, процедур і технологій реагування на кіберінциденти;

– зменшувати ризики кібератак, оскільки практикуючи в симульованому середовищі, працівники організації мають можливість помилятися і вчитися на власних помилках без реальних ризиків порушень кібербезпеки;

– забезпечувати безпечне та контрольоване середовище для людей, щоб експериментувати з різними методами та стратегіями кібербезпеки без ризиків, пов'язаних з реальними атаками;

– підвищувати мотивацію персоналу дотримуватися вимог кібербезпеки й усвідомити її пріоритетне значення для функціонування організації в результаті отримання ними досвіду хибних дій із серйозними для організації наслідками в умовах, максимально наближених до реальності [12].

Крім можливостей в безпечному та контрольованому середовищі набувати практичного досвіду роботи зі діючими в реальних умова сценаріями та технологіями, симуляційне навчання дозволяє тестувати корпоративні плани та процедури реагування на інциденти, виявляти будь-які слабкі місця або прогалини та вдосконалювати свої плани на основі результатів моделювання. Симуляції дозволяють організаціям краще дотримуватися передових галузевих практик, які вимагають від організацій проводити регулярні кібертренування.

Шляхом покращення практичної підготовки персоналу з кібербезпеки, симуляційні методи сприяють підвищенню загального рівня кібербезпеки в організації, зменшенню кіберризиків і кращій готовності до реальних інцидентів.

Встановлено, що симуляційне навчання, що базується на віртуальних, хмарних або автоматизованих інструментах моделювання, є для організацій більш економічно вигідним порівняно з іншими видами навчання з кібербезпеки, оскільки навчальні симулятори не вимагають використання фізичної інфраструктури або розгортання реальних систем і мереж.

Масштабованість є ще однією перевагою симуляційного навчання внаслідок можливостей легко розширювати програми для охоплення великих груп осіб або організацій, що робить їх прийнятним рішенням в умовах потенційного розширення обсягів діяльності організації або для задоволення ширшого спектру навчальних потреб.

Окремо слід відзначити ще низку переваг симуляційних методів навчання кіберфахівців. У симульованих навчальних середовищах організації можуть

відстежувати ефективність співробітників, вимірювати зрілість та виявляти прогалини в навичках для покращення свого стану безпеки [13].

Симуляції перевіряють здатність команди реагувати на кібератаку, що має вирішальне значення для зменшення її деструктивного впливу. За підсумками навчання можна оцінити, чи потребують члени команди додаткового навчання з реагування на кіберінциденти, іншим – запропонувати зміну підходів до реагування у разі атаки. Симуляційне навчання дозволяє розвивати практичні навички персоналу без психологічного дискомфорту і стресу, оскільки стажери можуть вчитися на помилках, не ризикуючи реальними даними чи інфраструктурою, що знижує тривожність та рівень стресу.

Важливим плюсом використання симуляцій кібератак у процесі навчання персоналу є забезпечення відповідності нормативним вимогам, які можуть застосовуватися в конкретній галузі. Так, організації, відповідальні за функціонування об'єктів критично важливої інфраструктури, зобов’язані регулярно перевіряти свої плани реагування на інциденти шляхом кібертренувань.

Таким чином, навчання кіберфахівців з використанням технологій симуляційного моделювання в кінцевому рахунку робить свій важливий внесок у покращення ефективності всієї системи кібербезпеки організації.

У технологічному контекст переваги симуляцій охоплюють можливості візуалізації атаки, а також процесів захисту інфраструктури дій захисників; тестування та усунення недоліків інтеграції нових систем та інструментів перед розгортанням; простота обслуговування і легкість оновлення програмного забезпечення для віртуального навчання, що гарантує постійний доступ до найактуальнішої інформації; відносна дешевизна і можливість масштабування відповідно до потреб; можливості легко повторити й відтворити навчання [13].

1.3 Основні види сценаріїв симуляційного навчання кіберфахівців

Дослідження джерел [14-17] показало, що найпоширенішими сценаріями кібератак для симуляційного навчання є:

– Симуляції соціальної інженерії та фішингу, спрямовані на людські вразливості, перевіряючи обізнаність співробітників та їх здатність виявляти

– Симуляції кінцевих точок та шкідливого програмного забезпечення, які перевіряють стійкість окремих пристроїв (ноутбуків, робочих станцій, серверів)

– Атаки на мережу та інфраструктуру з метою перевірки здатності мережі протистояти вторгненням та обмежувати пересування зловмисників.

– Розширені тактики симуляції, зокрема симуляція порушення й атаки (BAS) - автоматизовані інструменти, які постійно тестують засоби контролю безпеки на відповідність конкретним реальним тактикам (TTP).

Детальна інформація про види атак, які найчастіше стають основою симуляційного навчання показані в таблиці 1.1.

Таблиця 1.1.

Сценарії кібератак для симуляційного навчання

Вид атаки	Короткий опис
Симуляції соціальної інженерії	
Фішинг	Масові е-листи, щоб обманом змусити користувача перейти за шкідливими посиланнями або ввести облікові дані
Цільовий фішинг	Цільові атаки, спрямовані на конкретних осіб або відділи
Вейлінг	Високорівневий цільовий фішинг, спрямований на керівників вищої ланки
Компрометація ділової е-пошти	Зловмисники видають себе за високопосадовців, щоб ініціювати банківські перекази або витік даних
Вішинг (голосовий фішинг)	Шахрайські телефонні дзвінки, щоб обманом змусити працівників розкрити конфіденційну інформацію
Фішинг QR-кодів (квішинг)	Використання шкідливих QR-кодів для обходу традиційних фільтрів е-пошти

Продовження табл. 1.1.

Симуляції кінцевих точок і шкідливого ПЗ	
Розгортання програм-вимагачів	Симуляції шкідливого ПЗ, яке шифрує файли, з метою виявлення, ізоляції та відновлення резервних копій
Симулювання шкідливого ПЗ/вірусів	Розгортання безпечних, неруйнівних файлів для перевірки їх виявлення антивірусним ПЗ
Крадіжка облікових даних	Моделювання методів крадіжки облікових даних для входу зі скомпрометованої кінцевої точки
Рекламне ПЗ	Бомбардування систем небажаною рекламою для перевірки поведінки користувачів і безпеки браузера
Атаки на мережу та інфраструктуру	
Тактика бічного руху	Моделювання того, як зловмисники переміщуються мережею після отримання початкового доступу до тестової сегментації
DDoS-атаки	Затоплення систем, наприклад, трафіком з ботнетів, щоб спричинити простої
Підробка домену	Імітація легітимних, довірених доменів для перевірки фільтрів безпеки електронної пошти
Експлойти нульового дня	Тестування захисту від невідомих вразливостей до появи патчів
Просунуті тактики симуляції	
Симуляція порушень і атак (BAS)	Автоматизовані інструменти, які постійно тестують засоби контролю безпеки на відповідність конкретним реальним тактикам (TTP)
Червоні команди/тестування на проникнення	Етичні хакери активно намагаються проникнути в системи, щоб перевірити реакцію команди безпеки

З огляду на те, що близько третини всіх витоків даних пов'язані з фішингом, і майже 75% компаній у всьому світі щороку стикаються з фішинговими атаками, детальніше розглянемо можливості симуляційного навчання щодо виявлення та протидії атакам з використанням методів «виманювання» інформації та інших соціоінженерних тактик [14] (Рис. 1.4).

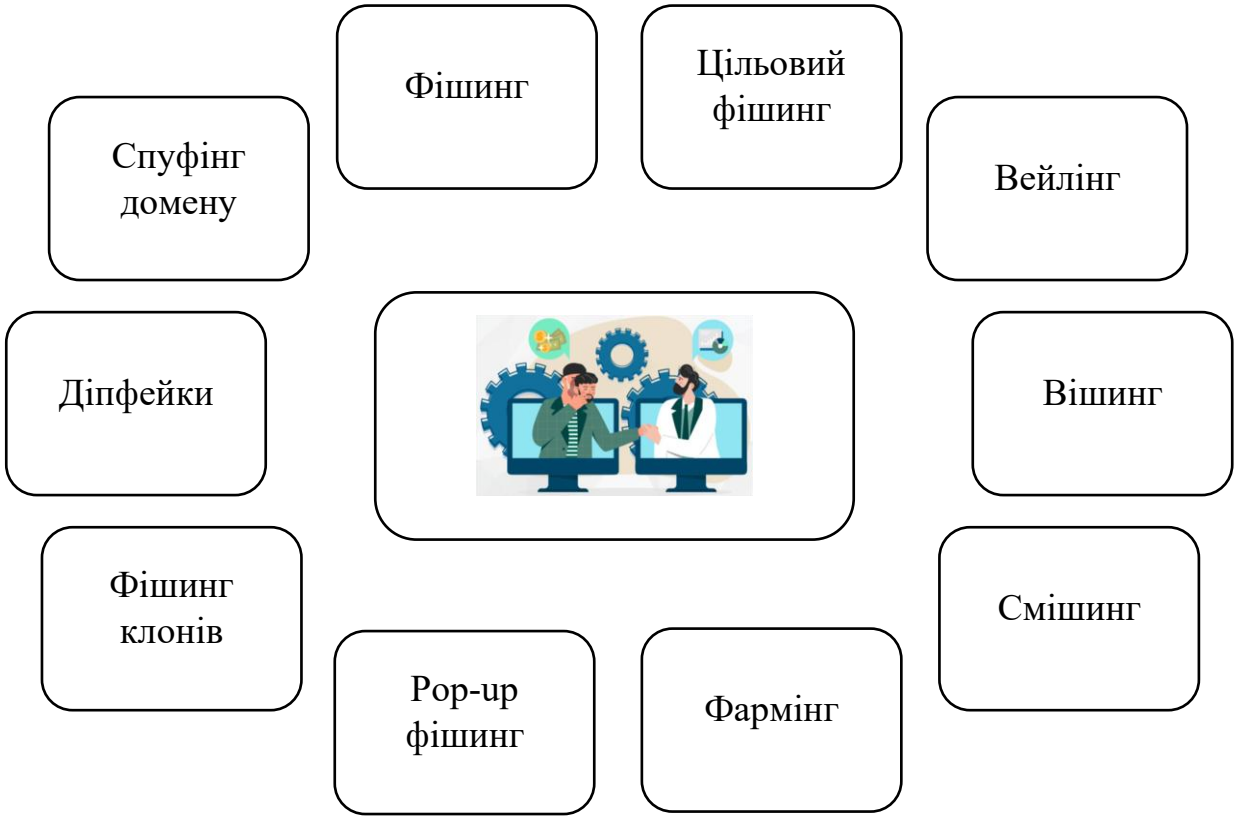

Рис. 1.4. Сценарії соціоінженерних атак для симуляційного навчання

Спуфінг домену – це одна з найпоширеніших тактика фішингових атак, оскільки понад 96% компаній страждають від різних типів спуфінгу домену [18]. Метою таких атак є введення в оману одержувачів електронної пошти, змушуючи їх повірити, що повідомлення надходить від законного відправника або організації. Підробка домену може охоплювати також підробку веб-сайтів.

У межах симуляційного навчання працівники мають насамперед знати відповідні політики, зокрема політику відправників (SPF) і DomainKeys IdentifiedMail (DKIM), а також навчитися розпізнавати ознаки підроблених електронних листів, зокрема розбіжності в адресах електронної пошти відправників, орфографічні та граматичні помилки, запити на конфіденційну інформацію або термінові заклики до дії тощо.

Важливим також є сформувати вміння ефективно й точно перевіряти особу відправника, а також вміст електронних листів на наявність ознак фішингу або видавання себе за іншу особу.

Цільовий фішинг (spear-phishing) - це цілеспрямована форма атаки, за якої зловмисники адаптують свої спроби фішингу до конкретних осіб або організацій. На відміну від традиційної фішингової загрози, цільовий фішинг передбачає ретельне дослідження, наприклад розвідку відкритих джерел OSINT, та налаштування під конкретну особу, щоб максимізувати ймовірність успіху. Потім зловмисники атакують жертву, використовуючи справжні імена і назви посад, щоб електронний лист виглядав справжнім.

Навчання для виявлення та реагування на такі атаки передбачає знання традиційних для фішингу ознак, перевірку адреси електронної пошти відправника, наприклад шляхом контакту із ймовірним відправником через відомий, надійний канал, а також виявлення неочікуваних запитів на конфіденційні дані або підозрілих посилань.

Вейлінг (Whailing) - форма фішингу, в якій кіберзлочинці цілеспрямовано атакують керівників та високопоставлених осіб, що приймають рішення, відомих як «кити». Атаки вейлінгу зазвичай характеризуються витонченістю, ретельним налаштуванням і увагою до деталей.

Атаки проти «китів» можуть мати різні форми, зокрема шахрайство з підробленими рахунками-фактурами, видавання зловмисником себе за посадову особу, крадіжка облікових даних.

Симуляції мають бути розроблені спеціально для керівників вищої ланки та пропонувати певну адаптацію контенту до конкретних ролей. Основними завданнями навчання є інформування топ-менеджменту про поширеність і потенційний вплив «китових» атак, формування культури «довіряй, але перевіряй», зокрема щодо високо ризикованих транзакцій і запитів, ініційованих електронною поштою.

Окремим напрямом симуляцій є рольові навчальні сесії, в рамках яких закріплюються навички виявлення фішингових спроб, шахрайських платіжних запитів і перевірки справжності фінансових транзакцій [17].

Вішинг (голосовий фішинг) – це атака, під час якої хакери обманом змушують працівників ділитися конфіденційною інформацією по телефону.

Подібно до традиційних фішингових шахрайств, що здійснюються електронною поштою, вішинг використовує методи соціальної інженерії для маніпулювання та зловживання довірою жертв.

Зазвичай зловмисники, що використовують вішинг, видають себе за працівників банків, щоб перевірити інформацію про рахунок і провести транзакцію або податкової служби.

Навчання на основі симуляцій має навчити працівників методам виявлення вішингу, зокрема перевірки номера відправника й оцінки номера абонента, який у разі голосової атаки відрізняється від звичайних, наприклад кодом іншої країни. У процесі симулювання атаки персонал заохочують недовірливо ставитися до неочікуваних і небажаних дзвінків, сумніватися в обґрунтованості запитів на конфіденційну інформацію, особливо коли абонент демонструє примусову або маніпулятивну поведінку, а також закріпити вимоги політик і процедур безпеки щодо обробки конфіденційної інформації по телефону.

Смішинг - це техніка, яка передбачає використання текстових повідомлень від нібито законних організацій (банків, державних установ) для обману працівників, щоб змусити їх розголосити конфіденційну інформацію, перейти за шкідливим посиланням чи завантажити на свій пристрій шкідливе ПЗ.

Ці повідомлення часто містять термінові запити, такі як попередження про призупинення дії облікового запису, запити на перевірку особистих даних або посилання на URL-адресу веб-сайту, яка здається автентичною.

Симуляційні вправи мають на меті навчити працівників способам розпізнавання підробних URL-адрес (префікси, номер відправника і вміст текстового повідомлення), перевірки справжності повідомлень, закріпити звички безпечного реагування на підозрілі повідомлення, зокрема уникнення натискання

на посилання або завантаження вкладень з невідомих джерел, утримання від розголошення конфіденційної інформації через текстові повідомлення й інформування про потенційні спроби смішингу фахівців з безпеки [15].

Фармінг - це вдосконалений тип кібератаки, який перенаправляє Інтернет-трафік з легітимних веб-сайтів на шахрайські без відома чи згоди користувача. На відміну від фішингових атак, які спираються на соціальну інженерію, фармінг працює на рівні DNS, маніпулюючи процесом розв'язання проблем, щоб перенаправити користувачів на шкідливі веб-сайти. Під час фармінгової атаки зловмисники клонують справжній веб-сайт і перенаправляють онлайн-трафік з автентичного веб-сайту на підроблений веб-сайт, щоб викрасти особисті дані. Це може бути зроблено за допомогою шахрайського посилання, надісланого електронною поштою, маніпуляції результатами пошукових систем або злому DNS домену.

У результаті симуляційного навчання працівники мають розібратися, як працює DNS, ознайомитися з потенційними вразливостями в інфраструктурі DNS і зловмисними методами маніпулювання роздільною здатністю DNS. У практичному вимірі мають бути формовані навички відрізняти підроблений веб-сайт від справжнього, виявляти підозрілі перенаправлення на веб-сайти або попередження веб-браузерів про недійсні сертифікати безпеки, перевіряти автентичність веб-сайтів перед введенням конфіденційної інформації.

Фішинг через спливаючі вікна (Pop-up Phishing) має на меті обманом спонукати користувачів поділитися конфіденційною інформацією або встановити шкідливе ПЗ через спливаючі вікна, які з'являються на їхніх екранах під час перегляду Інтернету. Під час фішингової атаки зі спливаючими вікнами хакери вкладають шкідливий код у спливаючі вікна або вікна підказок, які з'являються на веб-сайтах у браузері. Натискаючи на спливаюче вікно, особа автоматично встановлює шкідливу програму на свій комп’ютер. Крім цього, спливаючі вікна можуть використовуватися для збору облікових даних, імітуючи екран входу.

Симуляційне навчання має забезпечити закріплення у персоналу стійких безпечних практик використання програм для блокування реклами або розширення браузера, щоб запобігти появі шкідливої спливаючої реклами, уникнення натискання на підозрілі посилання або рекламу, перевірки URL-адрес веб-сайтів перед введенням конфіденційної інформації та обережної взаємодії зі спливаючими вікнами, зокрема, які запитують особисті або фінансові дані [16].

Фішинг клонів (Clone phishing) – атака, під час якої хакери використовують оригінальний електронний лист, надісланий з надійного джерела, а потім вносять до нього незначні зміни, такі як заміна справжніх посилань або вкладень шкідливими посиланнями або вкладеннями. Щойно користувач натискає на ці посилання, вірус або шкідливе ПЗ встановлюється на комп'ютер одержувача або починається спроба отримати облікові дані жертви.

Навчання з елементами симуляції передбачає опанування практиками виявлення клонованих веб-сайтів шляхом перевірки URL-адреси, виявлення невідповідностей або розбіжностей і перевірки легітимності сайту, а також стійкими звичками уникнення підозрілих посилань і завантаження вкладень.

Діпфейки - це підробні медіафайли (зображення, відео або аудіо), згенеровані за допомогою штучного інтелекту та глибокого навчання для введення в оману споживачів цієї інформації.

Статистика свідчить, що діпфейки показують вражаючі темпи розвитку впродовж останніх років. Кількість файлів з діпфейками різко зросла з 500 тис. у 2023 році до 8 млн. у 2025 році. Спроби шахрайства з використанням діпфейків зросли на 3000% у 2023 році, а зростання у Північній Америці склало 1740%. Клонування голосу є головним вектором атаки через свою дешевизну, швидкість і переконливість. Показник виявлення людиною підробок високоякісного відео становить лише 24,5%. Основними порушеннями із використанням діпфейків є шахрайство і крадіжка особистих даних у великих масштабах [19].

Незважаючи на те, що фахівці вважають найкращим захистом інструменти виявлення на основі штучного інтелекту і процедурні заходи безпеки, симуляційне навчання може сприяти покращенню показників виявлення таких

підробок шляхом симуляції сценарії діпфейків (термінові схвалення, зміни нарахування заробітної плати, запити на переказ коштів та ескалацію доступу), підготовки команд до перевірки запитів через безпечні канали, застосування позасмугової перевірки і розпізнавання ознак, які можуть бути неочевидними на перший погляд.

Висновки до розділу 1

У результаті дослідження встановлено, що симуляційні технології широко використовуються в кібербезпеці для різних цілей, зокрема моделювання реальних атак, перевірки систем захисту й навчання персоналу без ризику для реальної інфраструктури. Ці інструменти дозволяють організаціям виявляти вразливості, аналізувати й оцінювати ризики, тестувати реагування на інциденти й імітувати методи зловмисників у реальному часі, моделювати вплив людського чинника в режимі реального часу.

Масштаби застосування симуляцій для навчання кіберфахівців стрімко зростають, оскільки традиційні методи навчання з кібербезпеки стають дедалі менш ефективними, а симуляційне моделювання дозволяє організувати процес навчання через досвід і участь у реалістичних сценаріях безпеки в контрольованому й безпечному середовищі.

Встановлено, що найчастіше основою для симуляційного навчання є: атаки соціальної інженерії (різні вили фішингу, компрометація ділової е-пошти); атаки на кінцеві точки і впровадження шкідливого ПЗ (програми-вимагачі, крадіжка облікових даних); атаки на мережу та інфраструктуру (DDoS-атаки, експлойти нульового дня тощо); просунуті тактики симуляції (симуляція порушень і атак, робота червоних команд і тестування на проникнення).

Симуляційне навчання є актуальним і перспективним для використання в галузі кібербезпеки, оскільки має цілий ряд беззаперечних переваг для організації, зокрема доступ до реальних сценаріїв і технологій; експерименти в безпечному середовищі, перевірка готовності до кібератак, тестування планів

реагування на інциденти, кількісне оцінювання й аналітика; економічна вигідність; масштабованість рішень; забезпечення нормативної відповідності; формування ефективних кіберкоманд; впровадження кращих практик; розвиток культури кібербезпеки і, в підсумку, - покращення стану кібербезпеки організації.

У технологічному контексті переваги симуляційного підходу охоплюють: візуалізацію атак, процесів захисту інфраструктури і дій кіберкоманд; тестування й усунення несправностей; інтеграцію нових систем та інструментів перед розгортанням; просте обслуговування й оновлення програм для віртуального навчання, що гарантує постійний доступ до актуальної інформації; відносно невисоку вартість і можливість масштабування відповідно до потреб.

РОЗДІЛ 2
ВИДИ СИМУЛЯЦІЙНИХ ТЕХНОЛОГІЙ НАВЧАННЯ З КІБЕРБЕЗПЕКИ

Як відзначалося вище, традиційні методи навчання з кібербезпеки поступово втрачають свою актуальність у галузі кібербезпеки і стають дедалі менш затребуваними. Водночас, методи симуляційного навчання дозволяють організаціям забезпечити практичне спрямування підготовки кіберфахівців і відточування навиків командної роботи, відповідають викликам сучасного динамічного цифрового середовища і сприяють формуванню стійкої культури кібербезпеки організації.

Ще однією перевагою симуляційних методів є їхнє різноманіття з можливостями масштабування та вдосконалення у контексті розвитку технологій та ландшафту кіберзагроз. Так, у результаті дослідження встановлено наявність таких основних видів симуляційних методів навчання [20-21] (Рис. 2.1).

Рис. 2.1. Основні види методів симуляційного навчання

Розглянемо основні з них детальніше.

2.1 Штабні навчання з кібербезпеки

Штабні або «настільні», стендові, навчання на робочому місці (Tabletop exercise, TTX) базуються на обговоренні, де ключові зацікавлені сторони збираються разом, щоб імітувати реальний кіберінцидент. Метою такого навчання є перевірка плану реагування організації шляхом розгляду сценаріїв у середовищі низького рівня стресу.

На відміну від повномасштабних навчань, під час настільних навчань жодні реальні системи не зазнають впливу. Натомість учасники обговорюють свої ролі, дії та рішення, щоб зрозуміти, як план реагування організації на інциденти працюватиме в умовах потенційної кіберзагрози. Наприклад, Агентство з кібербезпеки та безпеки інфраструктури (CISA) надає детальні пакети настільних навчань для забезпечення готовності до кібербезпеки за такими напрямами: атаки програм-вимагачів, внутрішні загрози, фішинг і компрометація промислових систем управління (ICS) тощо [22].

Штабні навчання допомагають виявити прогалини в плануванні, уточнити ролі команди й покращити комунікацію, забезпечуючи готовність до реальної кібератаки. Метод настільних навчань передбачає використання заздалегідь визначених і часто гіпотетичних сценаріїв кібербезпеки, щоб допомогти учасникам обговорити, як вони реагуватимуть. Цей метод є спільним і нетехнічним, зосереджуючись на прийнятті рішень, процесах комунікації, а не на практичній діяльності. Учасникам зазвичай надається сценарій, такий як витік даних або атака програм-вимагачів, і їх просять крок за кроком описати свої дії, враховуючи ключові аспекти, такі як виявлення, стримування, пом'якшення наслідків та відновлення.

Метод є досить гнучким, що дозволяє адаптувати його до різних рівнів складності залежно від потреб організації та характеру загроз, які найчастіше викликають занепокоєння. Основною метою «настільного» навчання є оцінка ефективності плану реагування на інциденти організації і дозволяє:

– перевірити готовність команди до реагування на реальні кіберінциденти;

– виявити слабкі місця або прогалини в процесі реагування на інциденти, політиках або каналах зв'язку;

– покращити співпрацю і координацію між різними командами, включаючи ІТ-відділ, юридичний відділ, відділ зв'язків з громадськістю і керівництво;

– підвищити обізнаність про потенційні загрози й відповідні заходи реагування серед усіх учасників;

– розробити пункти дій для вдосконалення стратегій і процедур реагування на інциденти на основі отриманого досвіду [21].

Ключовими посадовими особами, які беруть участь у таких навчаннях зазвичай є: модератор, який відповідає за проведення навчання, керівництво сценарієм і забезпечення залучення всіх учасників; команда реагування на інциденти у складі технічного персоналу, який керуватиме прямим реагуванням на кіберінцидент; топ-менеджери та особи, що приймають рішення, у повноваження яких входить затвердження дій, управління ризиками і забезпечення відповідності цілям компанії; фахівців з юридичних питань і питань нормативної відповідності; представники ПР-відділу, які займаються зовнішніми комунікаціями і керують сприйняттям інциденту громадськістю; спостерігачі, зовнішні консультанти або команда внутрішнього аудиту, які відстежують хід навчання і надають зворотний зв'язок.

Загалом у штабних навчаннях мають брати участь представники всіх критичних сфер організації, які будуть залучені до реального кіберінциденту, зокрема команди з ІТ та кібербезпеки; топ-менеджмент і менеджери середнього рівня; юристи і комплаєнс-команди; фахівці з ПР та комунікації; представники відділи кадрів та фінансів тощо.

Тривалість штабного навчання може варіюватися залежно від складності сценарію та розміру організації. Зазвичай навчання за простішими сценаріями вимагають лише години часу, однак складніші або симулювання багатофазних інцидентів можуть тривати кілька годин.

Очікуваним результатом навчання на робочому місці є детальна оцінка того, наскільки добре організація підготовлена до кіберінциденту. Основні результати штабних навчань охоплюють виявлення прогалин у плані реагування з їх подальшим виправленням; розробка практичних рекомендацій для покращення стану кіберготовності, зокрема оновлення політик чи вдосконалення комунікаційних стратегій; покращення координації і чіткіше визначення ролей усіх членів команди; формалізація уроків за результатами навчання шляхом підготовки офіційного звіту з детальним описом висновків за результатами навчання і коригувальних заходів [22] (Рис. 2.2).

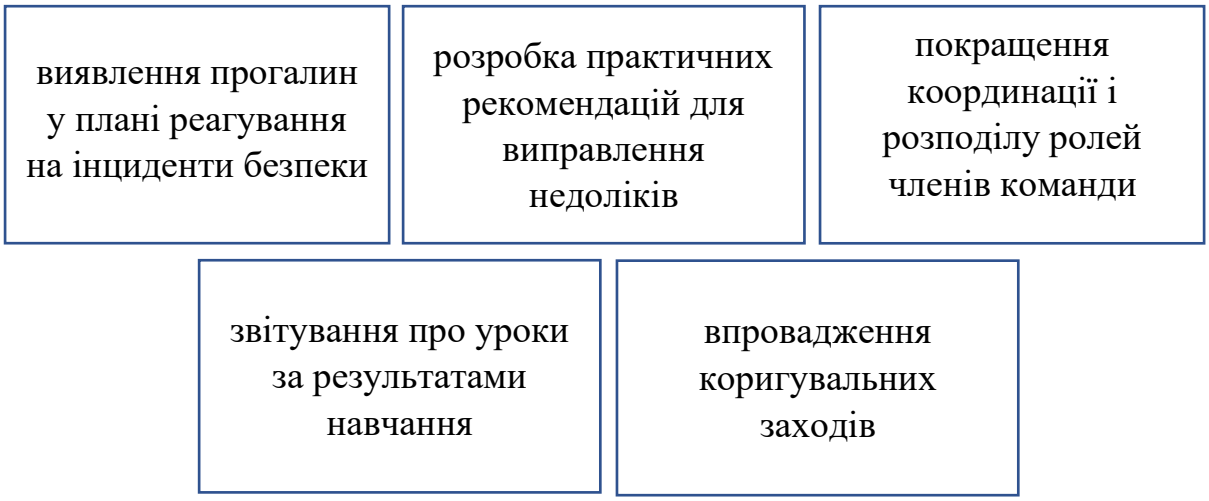

Рис. 2.2. Результати штабних навчань

Слід відзначити, що штабні навчання визначаються як важливий елемент системи забезпечення кібербезпеки (CSF) організації [23], а їх проведення рекомендується настановами щодо реагування на інциденти Національного інституту стандартів і технологій NIST [24]. Відповідно до зазначених документів навчання на робочому місці є частиною фази тестування та вдосконалення життєвого циклу реагування на інциденти й допомагають організаціям забезпечити ефективність і належне відпрацювання своїх можливостей реагування.

Проведення успішних «настільних» навчань вимагає розуміння керівних принципів реагування на інциденти NIST і дотримання алгоритму їх реалізації:

– підготовка, яка передбачає визначення мети, вибір реалістичного сценарію і збір необхідних матеріалів (короткі описи сценаріїв, контрольні списки реагування);

– залучення всіх ключових зацікавлених сторін розуміння ними своєї ролі та внеску в досягнення цілей навчання;

– симулювання, яке охоплює управління дискусією, заохочення співпраці й активної участі всіх учасників. Особливу роль відіграє модератор, який має залишатися нейтральним і дозволяти команді приймати рішення, водночас м'яко підштовхувати їх до усвідомлення критичних моментів навчання;

– підбиття підсумків для збору відгуків, обговорення отриманих уроків і визначення практичних коригувальних заходів [24].

Встановлено, що штабні навчання можуть бути адаптовані для вирішення широкого спектру сценаріїв і, відповідно, тестування різних аспектів можливостей реагування на інциденти організації. Основними варіантами використання штабних навчань у сфері кібербезпеки такі.

Моделювання атак програм-вимагачів, які сьогодні є зростаючою загрозою з часто критичними фінансовими втратами для організацій-жертв. «Настільне» навчання допомагає командам оцінити свою здатність виявляти кібератаку з метою здирництва, ізолювати уражені системи, спілкуватися із зацікавленими сторонами і приймати раціональне рішення щодо виплати викупу. Такі вправи також дозволяють організаціям відпрацювати свої плани відновлення, зокрема відновлення даних з резервних копій, і забезпечення безперервності бізнесу.

Тестування реагування на витік даних. З огляду на те, що витік даних може мати серйозні правові та репутаційні наслідки, моделювання таких ситуацій на робочому місці є необхідним. Практичне навчання на основі сценаріїв витоку даних дозволяє організаціям оцінити свою здатність швидко стримувати витік, оперативно інформувати постраждалі сторони й дотримуватися нормативних вимог. Крім цього, штабні вправи допомагають оцінити, як організація управляє зовнішніми комунікаціями для пом'якшення наслідків для зв'язків з громадськістю.

Реагування на експлойти нульового дня. Оскільки нові вразливості є невідомими до моменту експлуатації, реагування на такі інциденти вимагає адаптивності. Симуляційні навчання «настільного» типу щодо експлойтів нульового дня допомагають перевірити ефективність і злагодженість роботи команди у процесі реагування без заздалегідь визначених рішень. Цей сценарій підкреслює важливість швидкого виявлення, розвідки загроз і співпраці між командами в умовах невизначеності.

Виявлення та реагування на внутрішні загрози. З огляду на ключову роль людського чинника у реалізації кібератак, значення штабних навчань за цим напрямом зростає і дозволяє організації перевірити свою здатність виявляти незвичайну поведінку, запобігати несанкціонованому доступу до даних і реагувати на порушення внутрішньої безпеки. Цей сценарій підкреслює необхідність систем моніторингу та протоколів для захисту конфіденційної інформації зсередини.

Моделювання атаки на ланцюги постачання. Кібератаки на безпосередніх постачальників організації або постачальників наступних рівнів ланцюга постачань можуть швидко вплинути на діяльність організації. Симулювання атак на ланцюг постачань у штабному форматі моделює сценарій, коли зовнішній постачальник скомпрометований, дозволяючи організації відпрацювати, як реагувати, управляти відносинами з постачальниками і захищати свої системи від каскадних ефектів. Таким чином організація може перевірити стійкість ширшої організаційної екосистеми, а не лише внутрішнього захисту [21].

Підсумовуючи, слід відзначити, що практика підтверджує доцільність інвестування у симуляційні штабні кібернавчання, оскільки вони дозволяють скоротити час прийняття рішень, чітко визначити й розподілити ролі й обов'язки членів команди реагування, знизити потенційні витрати на відновлення після кіберінцидентів, посилити страхову й регуляторну позицію організації, переконатися в організаційній кіберстійкості й постійно вдосконалювати результати у забезпеченні захищеності організації від кіберзагроз [25].

2.2 Навчання червоної команди

В умовах постійного розширення й ускладнення важливим є перехід організацій від суто превентивного до проактивного підходу, сфокусованого на вдосконаленні механізмів виявлення та реагування на загрози. У таких випадках навчання «червоної команди» (Red teaming), які включають імітацію кібератак, спрямованих на виявлення прихованих вразливостей, є необхідним заходом.

Навчання червоної команди, яка грає роль потенційного нападника, є одним з основних способів тестування рівня кіберзахисту організації, покращення готовності й реагування корпоративних команд з кібербезпеки.

Навчання червоної команди на основі симуляційних технологій забезпечує досягнення таких основних цілей (Рис. 2.3).

Рис. 2.3. Цілі навчань червоної команди

На думку багатьох фахівців, основною метою навчань червоної команди є виявлення технічних і людських вразливостей організації, зокрема вразливості програмного забезпечення, застарілі налаштування системи і слабке управління паролями. Розуміння цих чинників допомагає ефективно розставляти пріоритети щодо виправлення та розподіляти ресурси.

Навчання червоної команди оцінюють ефективність плану реагування на інциденти в організації, за допомогою змодельованих реальних сценаріїв дозволяють актуалізувати прогалини в процесі відповіді на події кібербезпеки,

надати інформацію щодо його покращення для забезпечення своєчасного й ефективного реагування на реальні загрози.

Інформація, отримана в результаті атак, використовується для покращення існуючих протоколів безпеки і курсу нових стратегій, які в умовах динамічного середовища загроз мають постійно вдосконалюватися, підтримуючи загальний стан безпеки організації на належному рівні.

Навчання працівників щодо потенційних загроз й ознайомлення їх із передовим досвідом у кібербезпеці знижує ризик негативного впливу людського чинника й мінімізують ймовірність внутрішніх загроз. Навчання червоної команди сприяє створенню стійкої культури кібербезпеки організації, усвідомленню персоналом нагальної потреби у безпечній поведінці й реагуванні на кіберзагрози, забезпечуючи критичний рівень захисту від соціальної інженерії та інших атак, націлених на людину.

Регулярні навчання демонструють рівень дисципліни й дотримання вимог кібербезпеки, що допомагає організації відповідати нормативним зобов’язанням та успішно проходити аудити безпеки. Це допоможе не тільки уникнути порушень галузевих стандартів і юридичних норм, але сприятиме покращенню репутацію організації серед клієнтів і партнерів [26].

Як показало дослідження, навчання червоної команди охоплює кілька ключових кроків, кожен з яких є критично важливим для комплексної оцінки стану кібербезпеки й подальшої мінімізації ймовірностей реальних атак.

У процесі *планування* навчання червоної команди визначають обсяг і цілі навчання, правила взаємодії команди у середовищі, максимально наближеному до реальності. Крім цього, на етапі планування необхідно визначити переліки систем для тестування і типів атак для моделювання, завдяки чому забезпечується об'єднання командних зусиль в одному напрямку й підвищується ефективність навчання.

Етап *розвідка* складається зі збору інформації про організацію, зокрема мережеву архітектуру, персонал та види інформації, які необхідно захищати, щоб отримати повне уявлення про різні точки входу потенційного зловмисника.

Детальний збір розвідувальних даних буде також важливим для розробки ефективних сценаріїв атаки Таким чином організація може підвищити шанси виявлення слабких місць системи кіберзахисту, які червона команда в подальшому використає для симуляції вторгнення.

На етапі *експлуатації* червона команда на основі зібраної інформації намагається використати знайдену вразливість для порушення безпеки за допомогою різних методів, таких як фішинг, розгортання шкідливого ПЗ або проникнення в мережу. Команда нападу прагне реалізувати можливості несанкціонованого доступу до систем, щоб показати критичні слабкі місця.

Подальша *ескалація нападу* може охоплювати різні дії червоної команди, серед яких горизонтальне переміщення в мережі, ескалація привілеїв і організація витоку даних. Завдяки інструментам симулювання цей етап дає точне уявлення про шкоду, яку може завдати реальний зловмисник.

Звітність і аналіз передбачають документування і представлення результатів у детальних звітах, зокрема щодо виявлених вразливостей, використаних слабких місцях захисту, й рекомендаціях щодо коригування й покращення. На цьому етапі має забезпечуватися втілення отриманих за результатами навчання висновків у конкретні практичні дії [27].

Навчання «Червоної команди» мають різні переваги, серед яких:

– покращення рівня кібербезпеки внаслідок виявлення та використання вразливостей. Водночас, постійне вдосконалення окремих випадках забезпечує розвиток загального захисту організації у відповідь на нові загрози;

– удосконалення процесів реагування на інциденти, оскільки моделювання кібератак у симульованому середовищі сприяє швидкій та ефективній відповіді у подальших випадках реальних інцидентів. Така підготовка значно послаблює вплив, пов'язаний з фактичними порушеннями безпеки;

– підвищення рівня обізнаності персоналу про різні види потенційних загроз завдяки отриманню досвіду розпізнавання підозрілої діяльності та вжиття відповідних заходів у наближених до реальності умовах. Краща обізнаність має результатом зменшення кількості людських помилок;

– регулярні навчання червоної команди допомагають організації виконувати нормативні вимоги й успішно проходити аудити кібербезпеки, підтримуючи відповідність галузевим стандартам і правовим зобов'язанням, тим самим зменшуючи ризики витоків даних і санкцій [28].

У той час як навчання червоної команди зосереджені на імітації атак, навчання синьої команди (Blue team) пов’язані із забезпечення захисту. Розуміння різниці між ними на кожному кроці має першорядне значення для ефективного забезпечення кібербезпеки. У таблиці 2.1. представлене детальне порівняння підходів до навчання команд нападу та захисту [26].

Таблиця 2.1.

Порівняння підходів до навчання червоної і синьої команд

Критерій	Червона команда	Синя команда
мета	виявлення слабких місць та тестування захисту	захист від атак; посилення безпеки
склад команди	фахівці із впровадження наступальної стратегії	фахівці із реалізації оборонної безпеки
підхід	симуляція реальних атак	захист інфраструктури організації
фокус	наступальні стратегії та тактики	захисні стратегії та реагування на інциденти
результат	виявлення слабких місць і надання рекомендацій	посилення захисту й реагування на інциденти
частота	періодичне проведення	безперервний моніторинг і захист
інструменти та методи	пентестинг, соціальна інженерія та експлуатація	фаєрволи, системи IDS/IPS, реагування на інциденти

Отже, як видно з таблиці, навчання червоної команди – це симульовані кібератаки, призначені для виявлення слабких місць шляхом виконання наступальних методів та імітації дій реальних противників. У результаті навчань

команди нападу збирають цінну інформацію про зусилля щодо зміцнення захисту, яка допоможе організації краще підготуватися до виявлення і протидії загрозам, з якими вона може зіткнутися в реальному світі.

З іншого боку, навчання синьої команди мають оборонний характер, де внутрішньо призначені фахівці з IT та кібербезпеки взаємодіють із системами та намагаються захиститися від симульованих атак. Завдяки таким навчанням покращується здатність організації виявляти, реагувати та відновлюватися після інцидентів безпеки. Навчання синьої команди, зазвичай, є безперервними, забезпечуючи постійне оцінювання ефективності існуючих заходів безпеки.

У той час як навчання червоної команди є періодичними й вимагають менше співпраці з іншими, навчання синьої команди проводяться безперервно та є командною роботою. Обидва підходи мають свої переваги і є частинами загальної стратегії кібербезпеки організації. Об'єднання обох тактик сприятиме реалізації більш повної та надійної корпоративної стратегії безпеки.

Навчання фіолетової команди (Purple team) є інтеграцією зусиль обох вище згаданих команд з метою реалізації єдиної стратегії безпеки організації. Такий підхід забезпечує кращу координацію, за якої виявлена червоною командою вразливість, швидко виправляється синьою командою. Спільні зусилля завершуються створенням сильної позиції безпеки, де кожна команда навчається на тактиці та методах конкуруючої команди.

Отже, навчання фіолетової команди дозволяють організаціям випереджати кіберзагрози, що розвиваються, завдяки постійному процесу вдосконалення зі спільним навчанням. Цей інтегрований підхід допомагає забезпечити як проактивний, так і реактивний характер заходів безпеки, забезпечуючи більш збалансовану та ефективну стратегію захисту [29].

Типовими прикладами навчання червоної команди є:

– симулювання фішингу, в рамках якого червона команда може перевірити знання та реакцію працівників, визначити персонал, який потребує подальшого навчання за цим напрямом, і таким чином знизити ризики успішного фішингу в реальних умовах;

– тестування на проникнення, під час якого червона команда намагається проникнути в мережу організації з використанням різних методів проникнення, щоб виявити лазівки в мережевій безпеці, насамперед ті, які є критично важливими;

– атаки соціальної інженерії, які використовуються червоними командами для доступу до несанкціонованих зон і мають на меті перевірити ефективність фізичної безпеки та рівень пильності персоналу, виявити існуючі в системі захисту і, в результаті, встановити потреби в додатковому навчанні чи захисті;

– розгортання шкідливого ПЗ в контрольованому середовищі, що дозволяє оцінити можливості організації щодо виявлення та реагування на зловмисні програми з метою подальшого вдосконалення антивірусного захисту, ефективного виявлення і пом'якшення загроз шкідливого ПЗ.

Підводячи підсумки, варто відзначити, що для успішного проведення навчань усіх видів кіберкоманд критично важливими є ретельне планування та реалізація вправ, забезпечення достатніми ресурсами, а також максимальне охоплення тренуваннями усього причетного персоналу.

У цьому контексті ключове значення має підтримка топ-менеджменту, яка здатна подолати будь-який внутрішній опір. На організаційному рівні згода керівництва означає відданість організації кібербезпеці та гарантує наявність усіх необхідних ресурсів і організаційного супроводу для проведення ефективних навчань червоної команди.

Без кваліфікованої команди неможливо гарантувати успішність навчань з кібербезпеки. Організація може передати функції команди нападу на аутсорсинг або найняти професійних експертів з безпеки для створення своєї власної команди. Вони повинні мати багатий досвід і бути обізнаними про реалістичні загрози для конкретної організації, щоб забезпечити об’єктивну оцінку корпоративних засобів захисту.

Основоположним завданням є визначення чіткий цілей та обсягу навчання, зокрема визначення систем і видів атак, які будуть використані у ході

тренування. Такий підхід дозволить організувати навчання в рамках плану та з охопленням найбільш чутливих аспектів організаційної безпеки.

Важливим є регулярність проведення симуляційних навчань, забезпечення мінімального їх втручання у корпоративних систем і впливу на поточну діяльність організації. Крім цього доцільно ґрунтовно оцінити результати навчань і розробити детальний звіт з рекомендаціями щодо покращення заходів кібербезпеки організації та планів реагування на інциденти. Саме результати навчання можуть бути ефективно використані для прийняття рішень щодо майбутніх інвестицій та ініціатив у галузі кібербезпеки [26].

Завдяки навчанням червоної команди шляхом емуляції реальних кібератак організації можуть краще виявляти точки збоїв або вразливості, планувати процес реагування на реальні інциденти й оцінити його якість, покращити рівень кіберзахисту. Навчання червоної команди в рамках загальної стратегії безпеки є надзвичайно важливим для реалізації проактивного підходу до кіберзахисту організації в умовах розширення й ускладнення інформаційних загроз.

2.3 Змагання «Захоплення прапора»

Дедалі більш популярними в кібербезпеці є змагання типу «Захоплення прапора» (Capture the Flag, CTF), під час яких оцінюють навички і знання учасників у різних доменах кібербезпеки. Метою кожного завдання CTF є пошук прихованого файлу або фрагмента інформації («прапор») у цільовому середовищі. Вперше гра CTF була представлена на конференції з кібербезпеки DEF CON у 1996 році, після чого вона була прийнята в кіберіндустрії та академічних колах як засіб навчання, співпраці та змагання [30].

Згідно з дослідженням ENISA 2021 року, кількість заходів CTF у світі зросла більш ніж удвічі – з приблизно 80 у 2015 році до понад 200 у 2020 році [31]. Масштабні змагання, такі як Dragos CTF 2025, збирають близько 2 000 гравців з усього світу, з яких сформовано понад 1200 команд [32]. Хоча більшість змагань відбуваються онлайн, деякі заходи також проводяться локально по

всьому світу. У контексті нашого дослідження розглянемо можливості використання цього методу власне для навчання персоналу.

Встановлено, що змагання з кібербезпеки CTF проводяться у двох формах: вирішення завдань (Jeopardy-style) і захисту від атаки (Attack-defense).

Найпопулярнішим і найпоширенішим є змагання в стилі Jeopardy, де завдання класифікуються за різними областями. Вирішення завдання дає прапор, який учасник або команда надсилає для отримання балів. Тому чим більше завдань буде зроблено, тим кращим буде результат.

У цих змаганнях учасники вирішують завдання, пов'язані з багатьма темами, зокрема: веб-безпека, криптографія і стеганографія, зворотна інженерія, цифрова криміналістика, виявлення аномалій і вторгнень. Завдання вирішуються послідовно, і кожна ітерація зростає за складністю.

У форматі «захист від атаки» кожному учаснику або команді CTF надається власна віртуальна машина або мережа для захисту, кожна з яких має свої власні вразливості, що можуть бути використані іншими командами. Учасники мають знаходити та використовувати вразливості інших команд, одночасно захищаючи власну систему, виявляючи і виправляючи її слабкі місця [30]. Таким чином, основними завданнями учасників є захист вразливих систем і розробка експлойтів для атаки на своїх конкурентів. Під час змагань учасники заробляють бали за захист своїх сервісів та злом своїх опонентів.

Слід зазначити, що змагання CTF є важливим засобом набуття практичного досвіду й підвищення кваліфікації кіберфахівців через можливості:

– застосування теоретичних знань і розвиток практичних навичок у процесі вирішення реальних проблем у наближених до справжніх умовах;

– набуття реального досвіду роботи з інструментами й методами кібербезпеки в контрольованому середовищі без ризиків, де учасники можуть експериментувати без руйнівних наслідків;

– розвиток здатності до співпраці й командної роботи, оскільки CTF зазвичай вимагає від учасників об'єднання зусиль для вирішення складних, багатоетапних завдань;

– можливості нетворкінгу й рекрутингу, з огляду на те, що CTF є ідеальним способом для фахівців спілкуватися, навчатися один в одного й демонструвати свої здібності потенційним роботодавцям [31].

Щодня виявляються нові вектори атак, постійно відкриваються нові перспективи. Фахівці з кібербезпеки повинні реагувати інноваційними, креативними та нестандартними рішеннями у проактивний спосіб, а отже, постійно навчатися застосуванню нових інструментів, методологій і практик для протидії цим загрозам.

Навчаючись відповідати на актуальні кібервиклики у симульованому, а не реальному середовищі, організація може оцінити та розвинути практичні навички своїх кіберфахівців, підготувати свою команду й організацію загалом до зустрічі з реальними загрозами. Симулювання дозволяє кіберкоманді діяти на основі своїх знань, розробляти стратегії та використовувати технології на свою користь і при цьому взаємодіяти з іншими кіберпрофесіоналами, співпрацювати з експертами та використовувати нові технології для вирішення безпрецедентних проблем кібербезпеки.

Розглянемо основні категорії CTF (Рис 2.4).

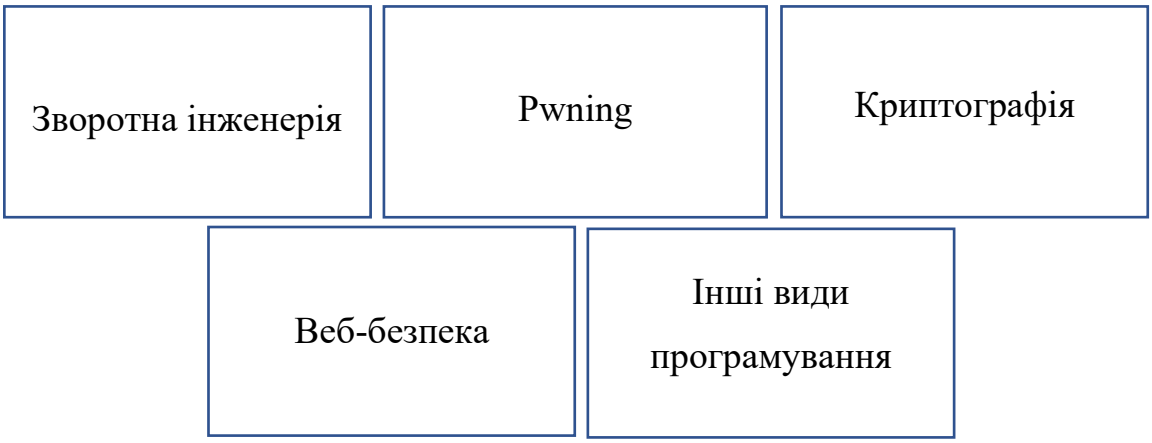

Рис. 2.4. Основні категорії CTF

Зворотна інженерія. У зворотному CTF учасникам надається виконуваний файл для перевірки вхідного рядка на основі алгоритму, а вони повинні знайти правильний ключ, який також служить цільовим прапорцем. На практиці може використовуватися будь-який метод зворотної інженерії, але загальна ідея полягає у визначенні того, як алгоритм відображає невідомий вхідний сигнал у

наданий вихідний рядок. Алгоритм може бути простим концептуальним прикладом алгоритму криптографії або процесом, який застосовує кілька різних перетворень до вхідних даних

Pwning. У змаганнях типу pwning учасники отримують виконуваний файл, IP-адресу та номер порту хост-сервера, на якому запущено програму/файл. Метою вправи є аналіз виконуваного файлу, виявлення вразливостей і використання програми для віддаленого виконання довільного коду на цільовому сервері. Успішна експлуатація часто передбачає зчитування певного файлу (наприклад, «файлу прапорців») на цільовому сервері.

Поширеними методами для цих експлойтів є переповнення буфера і впровадження коду або інші методи пошкодження пам'яті, такі як використання недоліків вивільнення або пошкодження динамічної пам’яті.

Криптографія. У криптографічному випробуванні надається зашифрований текст, а учасники мають розшифрувати його за допомогою криптографічних алгоритмів і математичних методів. Це випробування є складнішим, оскільки вимагає знань у предметній області, особливо в криптографії та математиці в кібербезпеці. Правильне розшифрування шифротексту генерує прапорець. Учасники заробляють бали залежно від швидкості розшифрування і рівня складності.

Веб-безпека. Учасникам надається URL-адреса веб-додатку або веб-сайту, який вони можуть використовувати за допомогою різних методів, зокрема SQL-ін'єкції, обхід засобів ідентифікації та доступу, міжсайтовий скриптинг (XSS) тощо. Ці випробування зазвичай зустрічаються в змаганнях CTF у стилі атаки та захисту. Від учасників очікується, що вони ідентифікуватимуть та захистять власні веб-додатки, атакуючи своїх конкурентів у режимі випробування на час.

Інші напрями. Завдання CTF можуть не мати попередньо визначеної категорії й охоплювати оптичне розпізнавання символів (OCR) для капчі, розв'язування лабіринтів, задачі оптимізації тощо. Учасники можуть заробляти бали за заздалегідь визначеними критеріями, такими як ефективність

використання часу, складність і оптимізація програми, а також проходження тестування [30, 33].

У контексті навчання з кібербезпеки заохочення участі персоналу в таких змаганнях може допомогти організації визначити, яке місце займають наявні фахівці в цьому спектрі, і як потрібно підвищити кваліфікацію робочої сили за допомогою залучення кваліфікованих спеціалістів за певними спеціалізаціями.

Оцінюючи з CTF у навчанні з кібербезпеки, слід відзначити, що змагання «Захоплення прапора» пропонують більше, ніж просто технічні вправи, але захопливий досвід, який розвиває реальні можливості. CTF як один із найефективніших способів отримати досвід без ризику виробничого середовища моделюють реальні середовища, де учасники повинні виявляти вразливості, використовувати слабкі місця та захищати системи. Вправи в рамках змагань є складними, але й цікавими. Вони забезпечують простір для тестування методів, випробування нових інструментів та підтримки професійного рівня.

Учасники CTF мають можливості відточити навички вирішення проблем: розв’язувати складні головоломки, критично мислити, змінювати стратегії та застосовувати креативні підходи для досягнення успіху. Сценарії CTF, які відображають сучасні тенденції в кіберзлочинності: від атак на ланцюги постачання до нових штамів шкідливого ПЗ, - дозволяють учасникам залишатися зацікавленими в мінливому ландшафті загроз.

З огляду на те, що CTF залучають широкий спектр учасників, від студентів до досвідчених аналітиків, змагання відкривають двері до спільноти професіоналів з кібербезпеки, де можна навчатися в інших, ділитися тактикою та розвивати свою репутацію. Крім того, рекрутери все частіше розглядають CTF як надійні показники кваліфікації, а високі результати у змаганнях можуть допомогти у працевлаштуванні, зокрема бути запрошеним на стажування, інтерв’ю або навіть отримати повноцінну посаду [30, 33, 34].

Водночас, слід відзначити, що проведення CTF пов’язане з низкою складнощів і викликів, зокрема традиційно вимагає значної інфраструктури: розміщення серверів, налаштування випробувань і забезпечення учасників

необхідними інструментами. Кіберфахівцям, які хочуть взяти участь у змаганнях, часто потрібні «хакерські» ноутбуки з попередньо встановленими утилітами, що створює логістичні труднощі.

Щоб подолати такі проблеми, деякі організації для проведення своїх CTF звертаються до платформ, спеціально створених для навчання безпеці на основі симуляційного моделювання – кіберполігонів. Використання кіберполігону для CTF також значно знижує поріг входу. Замість того, щоб з'являтися зі складним хакерським ноутбуком, будь-хто з комп'ютером та підключенням до Інтернету може увійти на платформу кіберполігону та розпочати змагання [34].

2.4 Навчальні кіберполігони

Дослідження показало, що ще одним популярним методом практично-орієнтованого навчання професіоналів з кібербезпеки є кіберполігон. Організації та окремі особи, які прагнуть отримати практичні знання й навички або підвищити кваліфікацію, нерідко стикаються з нестачею симульованих середовищ, подібних до тих, що існують у професійних сферах, таких як аерокосмічна галузь, бізнес або медицина. Професійне навчання в кібербезпеці стикається з численними викликами, зокрема такими як слабка реалістичність навчальних вправ, дотримання нормативних вимог під час тренувань, обмежені можливості навчальних платформ, недостатні гнучкість методів навчання, доступність навчальних середовищ і масштабованість моделей навчання [35].

Отже, кіберполігон – це інтерактивна симульована платформа, яка відтворює мережі, системи, інструменти та програми. Кіберполігони забезпечують безпечне та легальне середовище для набуття практичних кібернавичок і пропонують безпечні умови для розробки продуктів і тестування стану безпеки.

Кіберполігони відіграють вирішальну роль у сприянні та просуванні освіти, навчання та сертифікації в галузі кібербезпеки. Ці життєво важливі

інструменти можуть складатися з фактичного обладнання та програмного забезпечення або комбінації фізичних і віртуальних компонентів.

Розглянемо основні кейси використання кіберполігонів для освітніх цілей.

Насамперед таких платформ потребують організації, які мають на меті забезпечити навчання та безперервну освіту для фахівців з операцій безпеки, аналізу і криміналістики. Кіберполігони використовують також організації, які хочуть протестувати «ситуативні операції» для нових продуктів, випусків ПЗ та організаційної реструктуризації.

Окрему категорію становлять тренування на кіберполігоні для підтвердження кібернавичок при найманні й оцінюванні кандидатів на посади, пов'язані з кібербезпекою, або навчити діючих працівників для переведення на посади з кібербезпеки в організації.

Кіберполігони цікаві також для викладачів з кібербезпеки, які планують впровадити базові та поглиблені курси та навчальні програми з кібербезпеки.

Відповідно, цілі використання кіберполігонів в навчальних програмах і змаганнях також є відмінними. Основні з них показані на рисунку 2.5 [35-36].

Підвищення індивідуальних та командних знань і можливостей	Застосування знань і розвиток кібернавичок у безпечному середовищі	Забезпечення нормативної відповідності
Підготовка до іспитів або оцінювань з кібербезпеки	Оцінка заходів і стратегій, тестування нових процедур з кібербезпеки	Вивчення нових організаційних і технічних середовищ, протоколів

Рис. 2.5. Цілі використання кіберполігонів для навчання персоналу

Важливо зазначити, що ці цілі не є вичерпними, але можуть бути інтегрованими і передбачати вирішення різнопланових завдань.

На думку європейських фахівців, крім перелічених вище кіберполігони сприяють досягненню таких цілей як: розширення наукових досліджень нових методів виявлення та пом'якшення атак; посилення кіберстійкості організацій; безперервне проведення тренувань для перевірки корпоративних кіберможливостей; кризовий менеджмент для прогнозування наслідків кіберзагроз; відточення спроможностей кіберзахисту на основі гібридних сценаріїв і симуляційних технологій [37].

Розглянемо ключові характеристики кіберполігонів, які відіграють вирішальну роль у подоланні розриву в навичках кібербезпеки, зокрема технологічні компоненти типового кіберполігону.

Ключовим компонентом багатьох кіберполігонів є система управління навчанням (Range/Learning Management System, RLMS), яка охоплює стандартні функції традиційних систем управління навчанням (Learning Management System, LMS) і відмінні риси, притаманні власне кіберполігону.

Наведена на рисунку 2.6. діаграма зображує технологічні компоненти діапазону та виділяє різні характеристики RLMS [35].

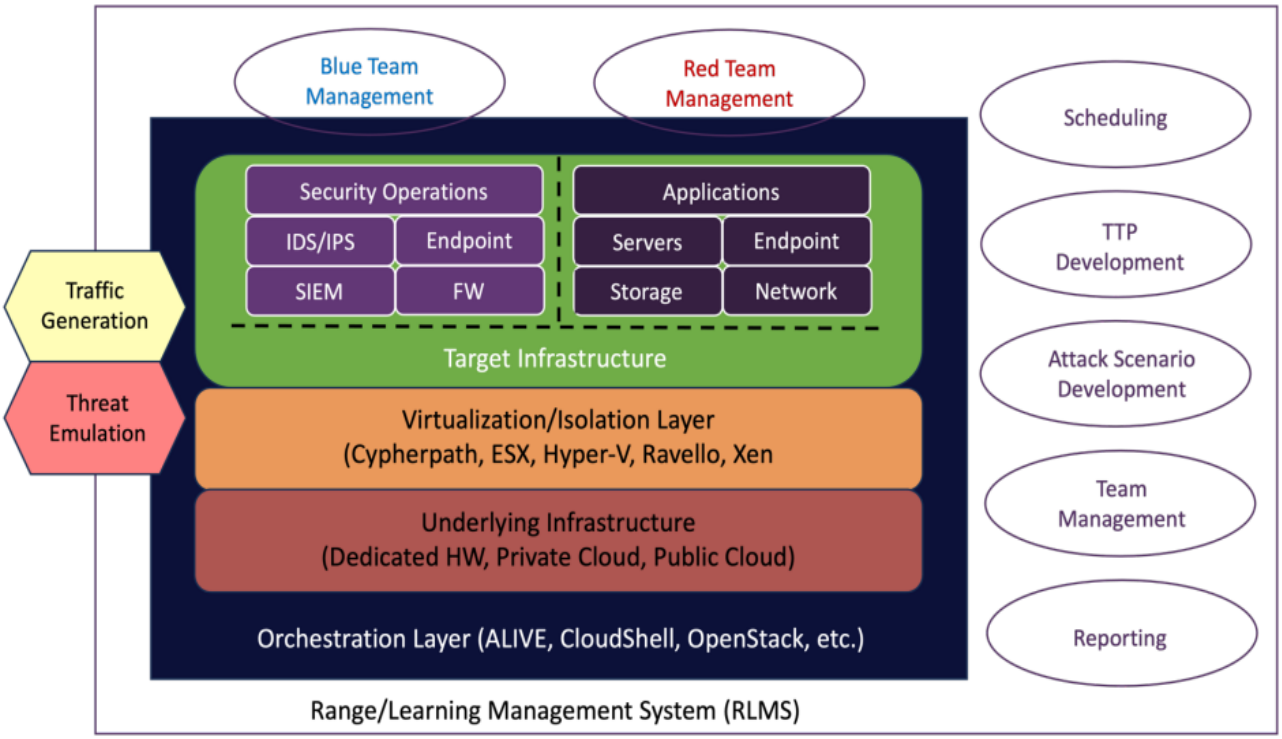

Рис. 2.6. Технологічні компоненти кіберполігона

Найнижчий рівень *оркестрації*, що підживлюється вхідними даними RLMS, об'єднує різні технологічні та сервісні компоненти кіберполігона. Деякі кіберполігони покладаються на внутрішньо розроблений рівень оркестрації, інші обирають комерційний продукт. Рівень оркестрації відіграє вирішальну роль в ефективності кіберполігонів, оскільки дозволяє інтегрувати базову інфраструктуру, рівень віртуалізації або ізоляції та цільову інфраструктуру. Крім того, цей рівень сприяє динамічній розширюваності кіберполігону, підтримуючи публічну або приватну хмару та виділені дротові інфраструктури.

Кожен кіберполігон спирається на *базову інфраструктуру*, що складається з мереж, серверів та сховищ. Хоча деякі виділені діапазони безпосередньо побудовані на фізичній інфраструктурі (такі як комутатори, маршрутизатори, міжмережеві екрани, кінцеві точки) у стеку, цей підхід часто є дорогим і слабо масштабованим.

Для вирішення проблем масштабованості, вартості та розширюваності, постачальників діапазонів часто переходять на програмно-визначену віртуальну інфраструктуру. Така інфраструктура суттєво впливає на реалістичність і точність кіберполігону. Під час вибору та використання інфраструктури важливим фактором є рівень підтримки, необхідний для застарілого обладнання або ПЗ, щоб задовольнити вимоги конкретного клієнта. Варто зазначити, що, хоча багато кіберполігонів не є суворо частиною базової інфраструктури, вони включають варіанти використання, які передбачають генерацію трафіку та емуляцію атак.

Більшість кіберполігонів використовують *віртуалізацію* для зменшення свого фізичного сліду. Існує два поширених підходи: рішення на основі гіпервізора та програмно-визначена інфраструктура. Незалежно від обраного методу віртуалізації, ступінь розмежування між базовою фізичною інфраструктурою та цільовою інфраструктурою впливає на реалістичність кіберполігону, оскільки може призвести до небажаних і непередбачуваних переривання або затримки.

Однак віртуалізація є важливою для створення економічно вигідних кіберполігонів, а також служить захисним бар'єром між цільовою інфраструктурою, яка може містити потенційні вектори атаки, і базовою інфраструктурою, яка може бути локальною, базуватися на публічній або приватній хмарі.

Цільова інфраструктура стосується симульованого середовища, в якому навчаються учасники. Залежно від конкретного випадку використання, цільова інфраструктура іноді може відтворювати фактичну IT- і безпекову інфраструктуру окремої особи в реальному світі. Розширені кіберполігони включають профілі комерційно доступних серверів, систем зберігання даних, кінцевих точок, програм і фаєрволів.

Коли учасники взаємодіють з кіберполігоном, RLMS генерує сценарії, які керують рівнем оркестрації у створенні цільової інфраструктури. Вони можуть включати специфічні для клієнта деталі конфігурації, такі як діапазони IP-адрес, інформація про маршрутизацію, стеки серверів і ПЗ кінцевих точок [35].

Слід відзначити, що основною характеристикою ефективного кіберполігона є *реалістичність*, тобто рівень точності, з яким кіберполігон відтворює реальний світ, що відіграє вирішальну роль у розробці прогнозованих операційних і навчальних результатів. Водночас, під час тренування певних навичок може бути корисним використовувати менш реалістичний сценарій для фокусування на опануванні самої навички.

Ще одним ключовим аспектом функціонування кіберполігону є можливості *отримання доступу* для участі в активних заходах. Двома міркуваннями щодо доступу є розташування та складність.

Оскільки розташування платформи може бути локальним чи хмарним рішенням, для всіх зацікавлених сторін важливо розуміти, як і коли вони можуть отримати доступ до технологій та додатків полігону, якими є обмеження пропускної здатності, а також вимоги до апаратного та програмного забезпечення для клієнтів. Іншим аспектом доступності є рівень складності

кіерполігону, оскільки всі учасники повинні мати чітке розуміння модулів, рівнів та інструментів, доступних на кожній платформі або системі.

Важливими рисами кіберполігону є *масштабованість і еластичність*. Масштабованість стосується здатності кіберполігону ефективно обслуговувати цільову групу користувачів. Еластичність, з іншого боку, стосується часу, необхідного для розширення ємності полігону для розміщення додаткових користувачів. В ідеалі, платформа має одночасно підтримувати всю свою потенційну групу користувачів та швидко збільшувати свою ємність на запит.

Кіберполігони, що покладаються на локальну апаратну інфраструктуру, стикаються з обмеженнями, що накладаються доступною оперативною пам'яттю та місцем на жорсткому диску. Натомість кіберполігони на базі публічних хмар зазвичай демонструють чудову масштабованість, за потреби використовуючи додаткові ресурси від хмарних постачальників. Вони також є більш еластичними за активного використання автоматизації й можливостей виділення системних ресурсів для додаткових користувачів.

Окрім комп’ютерної та сховищної інфраструктури, масштабування також вимагає достатньої пропускної здатності на стороні сервера, щоб обслуговувати великі обсяги доступу користувачів у періоди пікового навантаження.

Навчальні можливості, зокрема програми та результати навчання, що базуються на кіберполігоні, є центральними для всіх можливих випадків використання платформи й цілей зацікавлених сторін. Навчальні програми кіберполігону впроваджуються у двох формах: стандартна (попередньо розроблена) і спеціальна.

Попередньо розроблена навчальна програма містить навчальний план із низьким або середнім рівнем точності змісту, тестуванням та гейміфікацією, що забезпечує стандартизований шлях до завершення. З іншого боку, спеціальна навчальна програма є високо кастомізованою й адаптованою до конкретного клієнта, що часто вимагає постійного, інтегрованого та високоякісного експериментального простору.

Наступне важливе питання як для оператора, так і користувачів полігону полягає в тому, чи навчальні програми розроблені з *дотриманням нормативних вимог* і відповідають національному законодавству, галузевим рамкам і стандартам [35, 38].

Зменшення дефіциту робочої сили в галузі кібербезпеки та пом'якшення кіберзагроз для організацій та підприємств вимагає інноваційних і практичних підходів до навчання і підвищення кваліфікації діючих і потенційних фахівців з кібербезпеки. Хоча традиційні академічні методи та навчання на робочому місці залишаються важливими, їх більше не достатньо для задоволення зростаючого попиту на кваліфікованих працівників у сфері кібербезпеки.

Натомість рішення на основі симуляційних технологій, зокрема й навчання на кіберполігонах, дозволяють забезпечити якісну й ефективну, спрямовану на формування практичних навичок і досвіду в наближених до реальності і, в той же час безпечних умовах, підготовку висококваліфікованих професіоналів з кібербезпеки у відповідності з вимогами потенційних роботодавців.

Висновки до розділу 2

Результати роботи засвідчили, що методи симуляційного навчання відповідають викликам сучасного динамічного цифрового середовища і сприяють формуванню стійкої культури кібербезпеки організації, забезпечуючи при цьому різноманіття методів з можливостями масштабування та вдосконалення у контексті розвитку технологій і ландшафту кіберзагроз. До основних видів симуляційних методів навчання відносять: штабні навчання; навчання червоної команди; моделювання фішингу й соціальної інженерії; навчальні кіберполігони; симуляції порушень і атак (BAS); змагання CTF.

Штабні або «настільні» навчання проводяться на робочому місці й базуються на обговоренні, де ключові зацікавлені сторони збираються разом, щоб імітувати реальний кіберінцидент. Метою такого навчання є перевірка

плану реагування організації шляхом розгляду сценаріїв у середовищі низького рівня стресу.

Навчання червоної команди, яка діє як потенційний нападник, є одним з основних методів тестування рівня кіберзахисту організації, зокрема реагування на інциденти; виявлення вразливостей систем; підвищення обізнаності персоналу; забезпечення відповідності й аудиту; покращення готовності й реагування корпоративних команд з кібербезпеки. Побіжно слід відзначити, що навчання червоної команди нерідко проводяться разом із синьою командою, для одночасного тестування процесів нападу й захисту.

Дедалі більш популярними в кібербезпеці є змагання типу «Захоплення прапора» CTF, під час яких оцінюють навички і знання учасників у різних доменах кібербезпеки. CTF змагання проводяться у двох формах: вирішення завдань (Jeopardy-style) і захисту від атаки (Attack-defense). Перший вид передбачає вирішення завдань, зокрема з веб-безпеки, криптографії, цифрової криміналістики, виявлення аномалій і вторгнень тощо. У форматі «захист від атаки» завданнями учасників є захист власних вразливих систем і розробка експлойтів для атаки на своїх конкурентів.

З’ясовано, що ефективним методом практично-орієнтованого навчання кіберфахівців є кіберполігон - інтерактивна симульована платформа, яка відтворює мережі, системи, інструменти і програми. До основних ознак кіберполігону відносять реалістичність, можливості отримання доступу для участі в активних заходах, масштабованість і еластичність, широкі навчальні можливості. Крім традиційних завдань із формування практичних навичок, покращення роботи в команді, забезпечення нормативних вимог, кіберполігони надають можливості підготовки до іспитів або оцінювань з кібербезпеки, оцінювання заходів і стратегій захисту; тестування нових процедур з кібербезпеки, а також організаційних і технічних середовищ, протоколів.

РОЗДІЛ 3
РІШЕННЯ ДЛЯ СИМУЛЯЦІЙНОГО НАВЧАННЯ КІБЕРФАХІВЦІВ І РЕКОМЕНДАЦІЇ ЩОДО ЇХНЬОГО ЗАСТОСУВАННЯ

3.1 Кращі симуляційні онлайн-платформи для навчання з кібербезпеки

Галузь кібербезпеки стрімко розвивається і суттєво змінилася впродовж останніх десятиліть. Сьогодні кваліфікований і затребуваний на ринку праці кіберфахівець має не тільки володіти теоретичними знаннями, але й практичними навичками з орієнтацією на виконання конкретних завдань кібербезпеки. Отримати практичний досвід можна працюючи на посадах кіберфахівців, однак динамічний розвиток технологій нападу не дозволяє очікувати виникнення інциденту, щоб потренуватися. Натомість сучасний професіонал з кібербезпеки має навчатися постійно і бути готовим виявляти і реагувати на нові загрози вже сьогодні.

Розглянемо основні класифікації симуляційних онлайн-платформ [39] (Рис. 3.1). Важливу роль у формуванні сучасного висококваліфікованого спеціаліста з кібербезпеки відіграють симуляційні технології навчання. Оскільки створення симуляційних середовищ для навчання є складним і недешевим завданням, багато організацій не можуть собі цього дозволити. Водночас, отримати доступ до тренажерів SOC, машин і серверів зі справжніми вразливостями, максимально наближених до реальності симульованих атак у безпечному середовищі можна завдяки онлайн-платформам.

Отже, за форматом навчання навчальні онлайн-платформи поділяють на: “Кімнати” (Rooms/Challenges), де користувачі отримують завдання з покроковими підказками та різними рівнями складності від найпростішого до експертного; віртуальні машини (VM), які забезпечують завантаження й запуск вправ у локальній лабораторії; симулятори з використанням реальних сценаріїв інцидентів, наприклад зараження шкідливим ПЗ, атака програми-вимагача тощо;

класичні й авторські змагання типу «Захоплення прапора»/CTF для покращення командної роботи.

Рис. 3.1. Класифікації онлайн-платформ для навчання з кібербезпеки

Онлайн-платформи пропонують своїм користувачам навчання за різними напрямами, серед яких вправи з різних аспектів веб-безпеки, цифрової криміналістики та реагування на інциденти, розвідки на основі відкритих джерел OSINT. Крім цього онлайн можна потренувати навички роботи у складі червоної команди (моделювання атаки, тестування на проникнення, виявлення й експлуатація вразливостей, перевищення повноважень, обхід системи захисту) та синьої команди (виявлення загроз, реагування на інциденти, моніторинг мережі, різні функції SOC, SIEM, аналітика кібербезпеки).

За рівнем складності онлайн-навчання з кібербезпеки традиційно поділяють на початковий рівень (Entry-level) з легкими сценаріями і підказками; середній (Intermediate) із завданнями в кілька етапів з поєднанням різних навичок, інтеграцією різних технологій; просунутий (Expert/Pro) для корпоративних команд нападу і захисту з використанням кіберполігонів, комплексних сценаріїв, симуляцією складних APT-атак.

Проаналізуємо найбільш відомі онлайн-платформи.

TryHackMe (THM) [40] - це інтерактивна освітня платформа з модульною структурою, де теми поділені на «кімнати», в межах кожної з яких встановлено чіткий прогрес, контрольні питання з оцінками, а також підказки.

Платформа має розроблені дорожні карти для навчання за сценаріями червоної та синьої команд, а також з метою формування навичок відповідно до визнаних міжнародних сертифікацій для кіберпрофесіоналів, зокрема CompTIA Security+, Web Fundamentals, Pentest+, SOC Analyst.

У рамках платформи діє інтерактивний веб-термінал, який дозволяє запускати текстовий інтерфейс безпосередньо у браузері з уже налаштованим середовищем; ведеться детальне відстеження часу на виконання завдань, повтори, аналіз прогалин у підготовці; наявні навчальні конкурси (Cyber Apocalypse, Advent of Cyber) з можливістю виграти призи й сертифікати; активна система бейджів і досягнень, а кожна здобута кімната додає ваги профілю користувача.

Основними типами завдань і сценаріїв THM є: розвідка на основі відкритих джерел, зокрема пошук інформації про об’єкт, аналіз доменів, відстеження цифрових слідів; ескалація привілеїв з оновленими кейсами для Windows і Linux; експлуатація вразливостей веб-додатків (XSS, SQLi, CSRF, SSRF тощо); аналіз журналів, інструменти управління безпекою, реагування на інциденти й основи цифрової криміналістики для синіх команд.

Платформа THM найбільш корисна для таких фахівців як молодший спеціаліст з безпеки, пентестер, аналітик SOC, викладач з кібербезпеки. Платформа пропонує користувачам деякі унікальні можливості, зокрема автоматичну пропозицію наступної кімнати на основі попередніх досягнень, можливість створення власних кімнат для проведення корпоративних тренінгів і навчальних марафонів, пряма інтеграція із форумами кіберспільноти, просунутий режим для менеджерів, який дозволяє проводити навчання для команди і змагання, контролювати прогрес.

Кращою у сфері навчання з тестування на проникнення є платформа *HackTheBox (HTB)* [41], створена для справжніх професіоналів, які не чекають

підказок. Завдання розроблені так, щоб учасники мислили нестандартно, шукали приховані шляхи і рівнялися на кращих представників спільноти.

На HTB розміщено сотні віртуальних машин різних рівнів складності з реальними вразливостями, корпоративні середовища, які є повною симуляцією корпоративної інфраструктури з домен-контролерами, централізованою службою каталогів, багаторівневим периметром тощо. Платформа пропонує проведення командних турнірів, сертифікацій, рейтингування, а також API для автоматизації, підтримку, спільні чати для обговорення рішень.

Завдання охоплюють такі напрями як ескалація привілеїв, експлуатація веб-додатків, зворотна інженерія, криптобезпека і цифрова криміналістика, Інтернет речей, кіберзахист. Поглиблений профіль HTB передбачає розбори сценаріїв, інтерактивні навчальні курси для підготовки до окремих сертифікацій, наприклад OSCP, спеціальні акаунти для викладачів і студентських клубів.

Платформа буде корисною посад менеджерського рівня (лідерів команд, старших пентестерів), а також HR-фахівців, стажерів корпоративних відділів.

PortSwigger Web Security Academy [42] є найбільшою відкритою лабораторією для веб-тестувальників і розробників DevSecOps з понад 150 інтерактивними лабораторіями, десятками маршрутів навчання, інструментами оновлення вразливостей і сценаріїв. Платформа пропонує навчання з нульового рівня до рівня експерта з веб-безпеки, безпечну експлуатацію вразливостей, автоматичну перевірку рішень, систему сертифікатів і бейджів від Amazon і Microsoft, а також власний трекер досягнень та інтеграцію з корпоративними акаунтами.

Віртуальні лабораторії забезпечують навчання за такими напрямами: SQL-ін'єкції, командні ін'єкції, впровадження шкідливих скриптів, загрози автентифікації, управління доступом, безпека API, атаки на ланцюги постачання. Академія надає такі професійні інструменти: розбір сценаріїв, підтримка форуму, надання офіційної документації і прикладів реальних атак.

PWS Academy рекомендована для тестувальників на проникнення усіх рівні, розробників DevSecOps, тренерів з питань формування кіберобізнаності.

Навчальна платформ *OverTheWire* [43] є однією з найстаріших, працює з Linux/UNIX, зосереджена на скриптингу ОС, мережах, аналізі стеку, є стартовим майданчиком для багатьох початків із CTF.

Основними напрямами навчання є основи Linux та UNIX, мережева взаємодія, робота з правами, файлами, мережевими сервісами та безпекою, аналіз використання вразливостей ПЗ кіберзлочинцями в реальних атаках, базовим рівнем зворотної інженерії; унікальні сценарії для атак низького рівня, переповнення буфера, аналіз пам'яті.

Симуляційні вправи направлені на вдосконалення навичок спеціалістів з кібербезпеки й тестувальників на проникнення початкового рівня, а також системних адміністраторів ОС.

Французька міжнародна платформа *Root-Me* [44] містить понад 700 навчальних завдань за різними напрямами: від класичних завдань типу CTF, криптографії, стеганографії, реверсної інженерії до хмарної безпеки й аналізу мобільних застосунків.

Root-Me надає своїм користувачам можливості використання великої бази описів атак, відкритих і нетипових сценаріїв, підтримки інтерфейсу на кількох мовах (німецькій, іспанській, китайській), розбору завдань на форумі, рейтингування. На базі платформи регулярно проводяться міжнародні турніри на основі відомих вразливостей і ризиків з видачою сертифікатів. Навчальні вправи охоплюють такі питання як взаємодія між клієнтом і сервером, криптографія, зворотна інженерія, стеганографія, розвідка OSINT, комп'ютерна криміналістика, хмарні обчислення, вразливості систем SCADA й IoT.

Відповідно до згаданих напрямів симуляцій платформа є найбільш прийнятним осередком навчання для пентестерів повного стеку, фахівців червоної та синьої команд, CTF-команд у підготовці до змагань, а також окремим особам у пошуку свого напрямку професійного розвитку.

Онлайн навчальна платформа *VulnHub* [45] визначає своєю метою надати можливості кожному отримати практичний досвід у сфері цифрової безпеки, програмного й мережевого адміністрування. Платформа надає для завантаження

широкий набір реалістичних вразливих віртуальних машин для тестування власних експлойтів, автоматизації сценаріїв з Metasploit, PowerShell, Bash.

У центрі уваги VulnHub технології віртуалізації (VMware, VirtualBox), вразливості для Windows, Linux, IoT, SCADA, завдання, орієнтовані на веб-безпеку, ескалацію привілеїв, атаки на Active Directory, кейси з комп'ютерної криміналістики. Особливостями платформи є можливості користувачів створювати свої віртуальні машини з метою тестування наявних вразливостей, наявність описів та обмін сценаріями, відкритий доступ до командних тренувань.

VulnHub доцільно використовувати для підготовки до сертифікації з пентестингу, тренувань корпоративних червоних команд і команд реагування на інциденти, навчання системних адміністраторів для тестування політик безпеки.

Відома платформа *CTFlearn* [46] є онлайн-майданчиком для тренувань новачків у форматі CTF, оскільки представлені завдання є короткими, містять ігрові елементи, пропонують теми, які часто є поза увагою більших платформ і лабораторій. Користувачам надається інтерактивна підтримка в Discord.

Основними напрямами, представленими на CTFlearn, є традиційні веб-безпека, зворотна інженерія, цифрова криміналістика, стеганографія, розвідка на основі відкритих джерел OSINT, а також менш поширені технології блокчейн і криптобезпека, бінарні системи. Платформа пропонує відкрите рейтингування учасників, створення профілів і бейджів, проведення регулярних тематичних подій і міні-чемпіонатів. CTFlearn є найбільш прийнятним вибором для школярів і студентів, початківців з кібербезпеки, зокрема за напрямом кіберзахист, аналітика SOC, студентських CTF-команд.

Багаторівнева корпоративна платформа фахівців синіх команд *RangeForce* [47] призначена для тренувань із захисту інфраструктури, реагування на інциденти, розвідки загроз, аналізу журналів, управління інформацією та подіями безпеки.

Платформа створена для підготовки команд у реальних компаніях та установах і забезпечує можливості інтерактивних симуляцій актуальних просунутих атак, серед яких внутрішні загрози й атаки програм-вимагачів; застосування інструментів SIEM, EDR, автоматизованого реагування;

оцінювання навичок, статистики, корпоративного відстеження прогресу; формування індивідуальних і командних модулів, навчальних траєкторій.

RangeForce найбільше підходить для навчання спеціалістів команд SOC, реагування на інциденти і кіберзахисту, топ-керівників з питань IT і кібербезпеки, а також фахівців з питань HR і корпоративного навчання з кібербезпеки.

Підсумовуючи, слід відзначити стійкі тенденції в розвитку навчальних онлайн-платформ з кібербезпеки:

– розширення навчальних можливостей для спеціалістів з кіберзахисту й реагування на інциденти (синіх команд), зокрема щодо реагування на нові види атак: ланцюги постачань, кібервимагання;

– автоматизація рутинних операцій через використання тренажерів SOAR/ SIEM, інтеграції з розвідкою загроз;

– розширення можливостей хмарних лабораторій на базі AWS, Azure, зокрема реалізація комплексних сценаріїв кіберзахисту в хмарних середовищах;

– зростання уваги до формування «м'яких» навичок через модулі з розвитку комунікації, презентації звітів, лідерства і командної роботи;

– розширення масштабів використання гейміфікації та рейтингування, що сприяє залученості й мотивуванню учасників [39].

Характеризуючи ситуацію із практично-орієнтованим навчанням і кіберзмаганнями в Україні, можна сказати, що впродовж останніх років почали з'являтися вітчизняні навчальні лабораторії й локальні клуби з аналізу способів вирішення практичних завдань з кібербезпеки.

Органи державної влади (ДЦКЗ Держспецзв'язку України, Головне управління розвідки Міністерства оборони України, Міністерство цифрової трансформації України) реалізують партнерські програми кібернавчань у співпраці з бізнесом (AWS*)* та університетами (КПІ ім. І. Сікорського). На базі Тренінгового кіберцентру ДЦКЗ Держспецзв'язку проводяться кібернавчання (тренінги) для фахівців в сфері кібербезпеки та кіберзахисту з питань реагування на інциденти, оцінки стану захищеності промислових систем управління, застосування штучного інтелекту в кібербезпеці [48].

3.2 Розробка симуляцій на основі ШІ для навчання кібербезпеці

Генеративний штучний інтелект досяг вражаючих успіхів за останні роки, революціонізуючи різні галузі. Значення ШІ в кібербезпеці неухильно зростає, перебираючи на себе не тільки рутинні завдання, але й складні математичні обчислення й аналітику з одним суттєвим зауваженням: нагляд людини є обов’язковим. Симуляції у вигляді відео- та графічного контенту, згенерованого ШІ, можуть забезпечити захопливий навчальний досвід, хоч і вимагають ретельної перевірки для забезпечення точності й релевантності.

Як показало дослідження, сьогодні багато бізнес-шкіл і програм професійної підготовки покладаються на симуляції для покращення результатів навчання. Симуляції створюють ефект занурення і забезпечують високий рівень запам’ятовування, а також дозволяють випробувати різні реальні сценарії в середовищі з низьким рівнем ризику.

Незважаючи на свою ефективність, навчальні симуляції мають певний ціновий бар'єр, який перешкоджає багатьом студентам та організаціям отримати до них доступ. Тим не менше інструменти ШІ, чат-боти й симулятори можуть бути надзвичайно корисними для навчання й тестування безпеки, особливо при використанні у вузьких контекстах.

Програми навчання кібербезпеці значно підвищують професійну готовність працівників до реальних загроз завдяки використанню реалістичних сценаріїв. З огляду на те, що безпосередній контакт з реальними кібератаками є непрактичним та потенційно шкідливим, симуляції пропонують безпечну й ефективну альтернативу для розвитку багатьох навичок з кібербезпеки.

Симуляції дозволяють учасникам навчань відчути складність інцидентів кібербезпеки в контрольованому середовищі, сприяючи практичному навчанню без ризику для реальних систем. Відтворюючи реальні вектори атак і процедури реагування, симуляції забезпечують безцінний практичний досвід.

Звичайно, що перш ніж інвестувати у симуляційне навчання з кібербезпеки, необхідно чітко розуміти, до яких загроз необхідно підготувати

персонал і пріоритезувати їх за критичністю наслідків для організації. Симуляція не є вправою з перевірки пунктів, вона покликана перевірити, як фахівці з кібербезпеки й інші працівники організації, процеси й технології будуть реагувати в умовах реальних кіберзагроз.

Важливими чинниками ефективного застосування симуляційних технологій для навчання з кібербезпеки є насамперед чітке визначення обсягу навчання, видів кібератак, і основних функцій залученого персоналу, зокрема щодо ідентифікації, захисту, виявлення, реагування чи відновлення після інциденту. Симуляційне навчання має бути налаштованим під вимоги і потреби конкретної організації з урахуванням ландшафту загроз і специфіки її діяльності. Обов’язковою умовою є використання для моделювання віртуального середовища реальні системи, канали зв'язку, ролі команди і шляхи ескалації. Симуляція, заснована на власному середовищі, дозволяє виявити операційні сліпі зони та сприятиме високій кіберготовності до атак [49].

Експерти рекомендують передбачити неочікувані чинники, такі як збій зв'язку, затримка виявлення або відсутність зацікавленої сторони, які підвищують реалістичність сценарію.

У якості кращих практик для проведення симуляційного навчання з кібербезпеки багато організацій по всьому світу використовують пакети настільних навчань з кібербезпеки (CTEP), розроблені Агентством США з кібербезпеки та безпеки інфраструктури (CISA) [22]. Ці розробки є безкоштовними і містять готові сценарії, питання для обговорення та вставки (контекст або зміни до сценарію, щоб допомогти розширити реалістичність навчання), щоб допомогти організаціям розробити реалістичні навчання.

У контексті забезпечення міцного взаємозв’язку стратегії кібербезпеки з цілями бізнесу важливим є узгодження процесів реагування на інциденти кібербезпеки з загально-організаційними процесами оцінювання бізнес-ризиків та забезпечення належної відповіді. Це пов’язано з тим, що кіберінцидент має наслідком не тільки втрати на технологічному рівні, але й негативно впливає на

довіру клієнтів, зобов'язання щодо дотримання вимог, фінансові операції та репутацію організації.

Отже, ефективне симуляційне моделювання відображає унікальне середовище конкретної організації, відповідає визнаним кращим практикам і стандартам із кібербезпеки, охоплює реалістичні загрози й підсилює зв’язок між кібербезпекою та безперервністю бізнесу. За умови правильного виконання такі симуляції перетворюють навчання на стратегічний інструмент для забезпечення кіберстійкості організації.

Розглянемо типовий алгоритм створення інтерактивної симуляційної вправи можливостями організації або окремого користувача з використанням чат-бота Poe від соціальної платформи обміну інформацією Quora Рис. 3.2 [50]. Однак, для таких завдань можна використовувати великі мовні моделі, такі як GPT-4, або інші платформи чат-ботів.

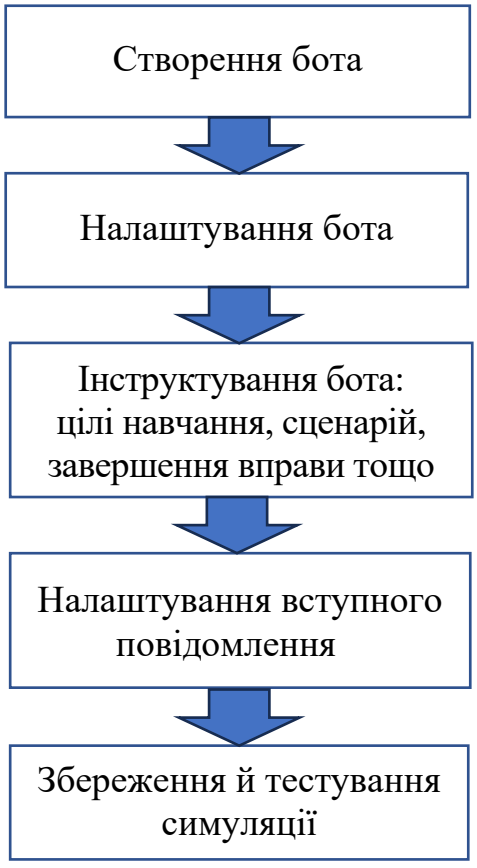

Рис. 3.2. Алгоритм створення інтерактивної симуляційної вправи з використанням чат-бота Poe

Етап 1. Вхід у Poe і створення бота передбачає запуск програми і вибір у верхньому лівому куті головної панелі інструментів кнопки «Створити (Create)» (Рис. 3.3).

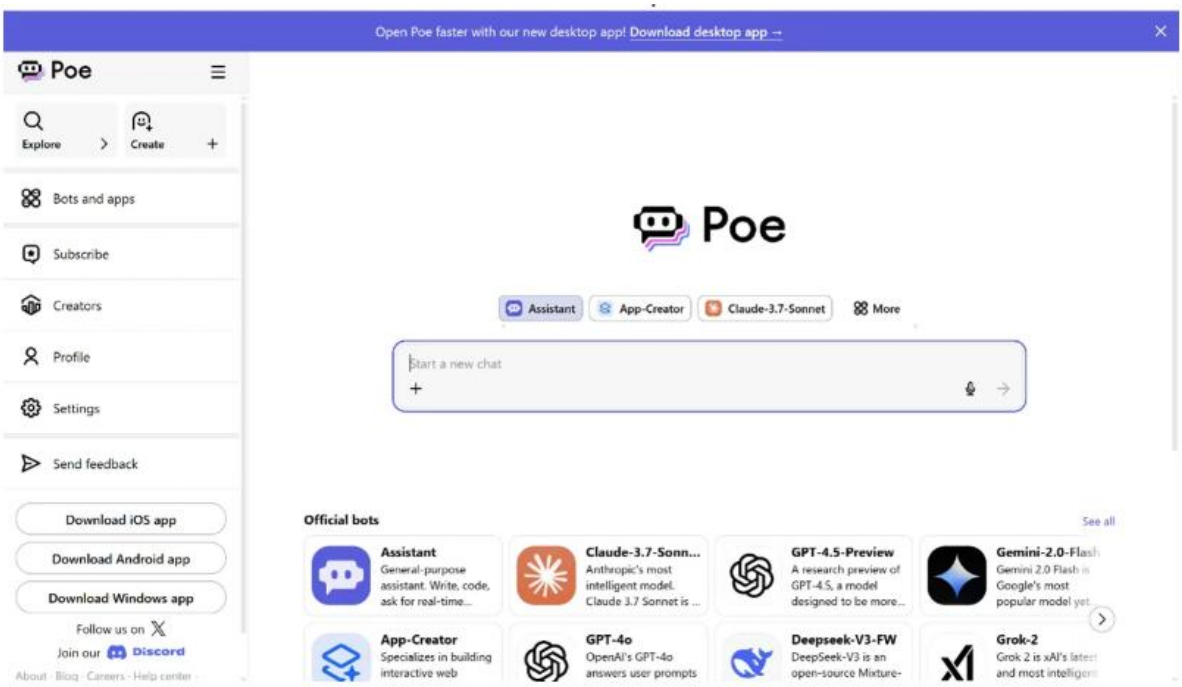

Рис. 3.3. Створення бота в Poe.

Етап 2. Налаштування бота охоплює призначення назви бота, наприклад «Кіберсимуляція» (CyberSecSim), вибір підходящої моделі й виду бота. У нашому випадку це бот для рольової гри (Рис. 3.4).

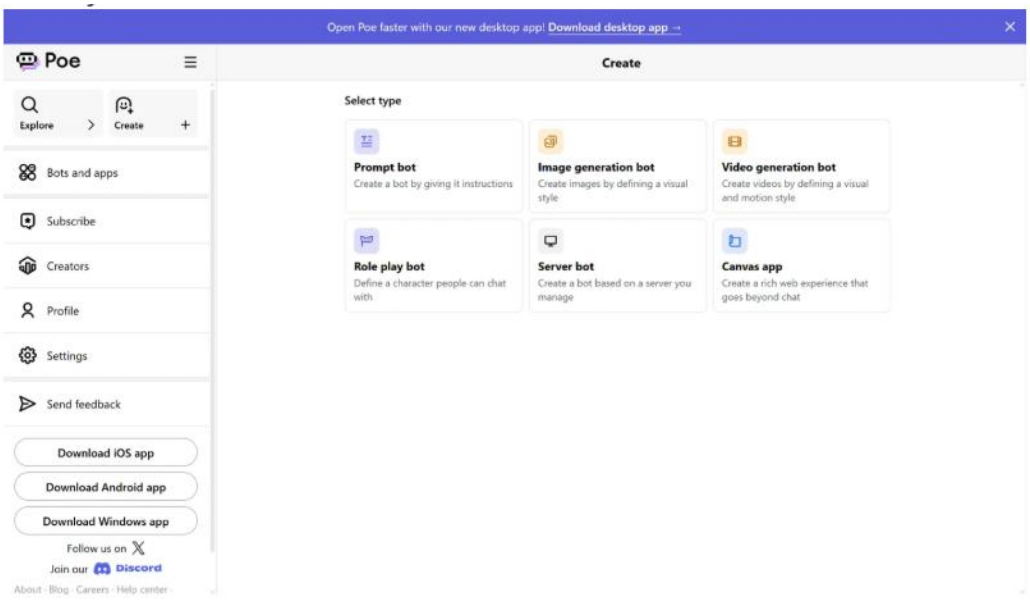

Рис. 3.4. Налаштування бота в Poe.

Етап 3. Інструктування бота, як поводитися і взаємодіяти з учасниками, зокрема загальний опис його ролі, визначення цілей навчання, засад підготовки й реалізації сценарію, процесу прийняття рішень, основних концепцій кібербезпеки і завершення гри.

Прикладом *опису* може бути такий: «Ти, CyberSecSimGPT, є симулятором реагування на інциденти кібербезпеки на основі штучного інтелекту. Твоя роль полягає в залученні учасників (аналітиків з кібербезпеки) до інтерактивного сценарію, в рамках якого вони реагувати на порушення безпеки у великій компанії N.

Навчальні цілі встановлюють бажаний результат симуляційної вправи, зокрема учасники зрозуміли стратегії виявлення та реагування на інциденти; знають про вплив прийняття рішень у реальному часі в галузі кібербезпеки; усвідомили, як компроміси між безпекою, безперервністю бізнесу і репутацією впливають на результати.

Інструктування бота щодо *підготовки сценарію* визначає, якою є роль учасника (мережевий аналітик, спеціаліст або директор з інформаційної безпеки); причини початку симуляції, наприклад, отримання сповіщення з високою пріоритетністю від центру операцій безпеки (SOC) про потенційну атаку програми-вимагача на критичні сервери, DDoS або фішингову атаку тощо.

Подальша *реалізація сценарію* передбачає негайне представлення гравцю сценарію порушення безпеки. Наступним є прийняття гравцем або командою рішення про спосіб реагування на визначену кібератаку.

Процес *прийняття рішень* учасником передбачає надання гравцю/ям чотирьох варіантів реагування на кожному кроці сценарію, зокрема: негайне ізолювання уражених систем; звернення до зовнішніх експертів з кібербезпеки; інформування правоохоронних і регуляторних органів; спроби внутрішнього пом'якшення наслідків без зовнішньої допомоги.

У разі, якщо гравець вибере виконати певну дію, бот негайно надає відгук про її потенційні наслідки. Якщо гравець обирає неефективний спосіб реагування, йому надається інформація про пов’язані з цим способом додаткові

проблеми безпеки, такі як ризики витоку даних, внутрішнього саботажу або затримка у стримуванні загрози тощо.

Інструктування бота передбачає також дослідження основних напрямів кібербезпеки, серед яких:

– стримування інцидентів, тобто визначення прийнятної швидкості для ізоляції уражених систем;

– розвідка загроз, яка охоплює аналіз моделей атак і оцінку ризиків;

– забезпечення відповідності нормативним вимогам із повідомленням про порушення безпеки відповідним органам;

– узгодження завдань безперервності бізнесу і кіберзахисту через збалансування швидкого реагування з операційним впливом [49].

Кінець гри очікується після чотирьох раундів прийняття рішень. По завершенню вправи бот надає остаточний звіт, у якому підсумовуються рішення гравця та їх результати, а також пропонує учаснику зразки кращих практик реагування на інциденти кібербезпеки для самостійного розбору і врахування й професійній діяльності.

Етап 4. Підготовка вступного повідомлення про кіберінцидент, який допоможе гравцю «зануритися» у гру. Для прикладу, це може бути такий текст: «Ласкаво просимо, CISO. Щойно спрацювало високопріоритетне сповіщення безпеки. Критичні сервери вашої компанії можуть бути атаковані програмою-вимагачем. Команда SOC очікує на ваші негайні вказівки. Що ви будете робити?»

Крок 5. Збереження й тестування симуляційної вправи є найпростішим завданням і передбачає тільки натискання на кнопку «Опублікувати», щоб завершити роботу бота.

Підсумовуючи, варто наголосити, що використання симуляційного навчання є важливою передумовою забезпечення ефективної системи кібербезпеки організації і має здійснюватися з урахуванням переліку вимог.

3.3 Практичні рекомендації щодо ефективного застосування симуляційного навчання

На основі вивчення наукових джерел і кращих практик з питань організації симуляційного навчання в кібербезпеці [9-10, 12-14, 17] запропоновано низку рекомендацій для підвищення його ефективності на рівні організації (Рис. 3.5).

Рис. 3.5. Рекомендації для підвищення ефективності симуляційного навчання

Важливою передумовою успішного симуляційного навчання з кібербезпеки є ретельний *аналіз середовища, потреб і можливостей* конкретної організації, зокрема встановлення основних видів загроз, яким піддається організація, і слабких місць кіберзахисту; вибір методів симуляційного навчання персоналу й періодичність їх використання; визначення категорій співробітників, які будуть залучатися до навчання із яких проблем безпеки; вибір методів перевірки результативності програм навчання тощо.

Такий ґрунтовний аналіз є основою для чіткого й однозначного *визначення цілей навчання* і гарантує, що тренувальні вправи будуть відповідати фактичним потребам організації, а не загальним сценаріям.

Створення реалістичних сценаріїв також є must-have завданням у розробці симуляційних вправ, оскільки максимальна наближеність навчання до реальних умов забезпечує його високу ефективність. Це завдання досягається шляхом включення фактичного технологічного середовища організації в процес симуляції; моделювання реалістичного бізнес-тиску й часових обмежень під час тренувань; використання методів атаки, що відповідають специфіці галузі, до якої належить компанія; введення в навчання завдань на вирішення проблем комунікації між учасниками команди і нестачі інформації для оцінки ситуації та прийняття рішення.

Для заповнення всіх прогалин у корпоративній системі кібербезпеки необхідним є *використання широкого спектру різнопланових симуляцій* відповідно до потреб конкретної організації. Для цього варто скористатися результатами попереднього аналізу щодо найбільш частих атак, а також порушень безпеки внаслідок слабкої підготовки працівників. Можна комбінувати різні типи атак і звернути особливу увагу на сценарії реагування на більш стійкі кіберзагрози з багатьма векторами і методами впливу. Таким чином персонал отримає можливість не тільки відшліфувати навички реагування, але й потренується діяти в умовах стресу й терміновості.

У процесі впровадження симуляційних вправ варто звернути увагу на забезпечення *масштабування складності завдань*, тобто обирати рівень складності завдань відповідно до прогресу фахівців, щоб вони поступово просувалися й залишалися мотивованими до навчання щодо загроз. Також краще розпочинати навчання з простіших сценаріїв і поступово збільшувати складність у міру покращення можливостей працівника. Це запобігає перевантаженню учасників і допомагає зміцнити їхню впевненість у власних силах.

Контекст симуляційного навчання є дуже важливим з огляду на результативність вправ. Так, зміст і кроки сценарію мають відображати специфіку організації, її основної діяльності та системи забезпечення безпеки. Варто переконатися, що у симуляціях використовується відповідний для кожного фахівця контекст, а змодельоване середовище є максимально

наближеним до того, в якому працює особа (для мережевого аналітика - це аналогічна реальній мережа, для фінансиста – система електронних платежів, які використовуються в його банку).

Проблеми *управління ідентифікацією та доступом* мають бути у фокусі уваги навчальних вправ, оскільки багато сучасних атак використовують вразливості ідентифікації, щоб реалізувати атаки, зокрема захоплення облікових записів, ескалації привілеїв, експлуатації неактивних облікових записів, зловживання доступом з боку інсайдерів.

Регулярність і послідовність проведення симуляційного навчання є одним із основоположних чинників його ефективності, оскільки саме практика робить навчання досконалим. Чим більше практики отримують працівники, тим краще вони зможуть розпізнавати підозрілі події або поведінку, а отже зменшиться кількість порушень кібербезпеки.

Дослідження Hoxhunt Challenge [51], в рамках якого протестували понад 600 тис. працівників у 125 округах США з використанням змодельованих QR-кодів фішингу, засвідчило, що довгостроковий підхід до навчання з часом покращує результативність. Так, ті, хто брав участь у симуляційному навчанні протягом 18 місяців, показали кращі результати, ніж ті, хто навчався короткий проміжок часу. А працівники з більшим досвідом навчання повідомляли про підозрілий QR-код у 3 рази частіше, ніж ті, хто навчалися вперше. На основі цих даних можна стверджувати, що проведення навчань з використанням симуляцій принаймні кілька разів на місяць без відриву від роботи є найбільш ефективним варіантом.

З огляду на постійне вдосконалення технологій кібернападу, насамперед через стрімкий розвиток ШІ, організаціям варто забезпечити *використання платформ на основі ШІ*, які надають широкий перелік додаткових переваг, серед яких: створення індивідуальних сценаріїв атак на основі конкретного профілю ризику організації; адаптацію рівня складності симуляції відповідно до результатів учасників; надання послуг коучингу в режимі реального часу під час

навчань; аналіз закономірностей у відповідях учасників для виявлення слабких місць системи навчання тощо.

Завдяки цим досягненням симуляції безпеки стають більш ефективними й доступними для організацій будь-якого розміру й можуть бути важливою частиною корпоративної стратегії кібербезпеки.

Обов’язковою вимогою підтримання підходів симуляційного навчання організації в актуальному стані з високим рівнем результативності є постійне *оновлення методів і змісту завдань.* Підставами для оновлення симуляційного навчання зазвичай є зміни в ландшафті загроз, ускладнення й поява нових технологій кібернападу, виявлення вразливостей нульового дня, зміни в нормативному забезпеченні й розширення корпоративної системи кібербезпеки. Завдяки регулярним оновленням організація забезпечує, що її персонал володіє свіжою інформацією про загрози й вміє належним чином на них реагувати.

Надання конструктивного зворотного зв'язку й використання позитивного підкріплення має бути невід’ємною частиною навчання незалежно від того, як працівники проявили себе під час симуляції кібератак. Якщо навчання відбувалося на робочому місці, потрібно повідомити персонал, що це був навчальний сценарій, а не реальна атака, а також надати короткі вказівки щодо доцільних і безпечних дій у подібних ситуація.

У відгуках про результати навчання краще використовувати засоби позитивного підкріплення й винагороди, що дозволить підвищити мотивацію та залученість працівників. Критика їхніх дій не є дієвою.

Для підвищення ефективності симуляційних вправ бажано впроваджувати *навчання, адаптоване під конкретного фахівця* і з урахуванням його кваліфікаційного рівня, попередніх посад і сфер діяльності (фінанси, продажі, вище керівництво тощо), минулої поведінки і відомих вразливостей. Цей підхід охоплює створення так званих персоналізованих шляхів навчання.

У цьому контексті слід звернути увагу на *психологічні аспекти реалізації атак*. Зокрема необхідно вивчити особливості мислення і поведінки зловмисників і врахування їх при формуванні сценаріїв кібератак, наприклад

щодо спроб введення працівника в оману. Водночас треба розуміти, якими є основні психологічні тригери для спонукання персоналу до дій в інтересах нападника (жадібність, цікавість, терміновість, страх або бажання допомогти).

Персоналізація, яка проявляється у звертанні до особи по імені або за посадою, а також видавання зловмисником себе за іншу, добре знайому або наближену по роботі особу, як елементи атаки соціальної інженерії також мають бути охоплені у сценаріях симуляцій.

Метою таких симуляційних вправ є формування навичок співробітників у критичних або навпаки, на перший погляд, звичайних ситуаціях діяти раціонально й виважено, а не під впливом емоцій.

Щоб виправдати інвестиції в навчання на основі симуляцій, організації повинні забезпечити *вимірювання їх ефективності*, зокрема за такими основними показниками:

– час виявлення та локалізації інцидентів;

– точність ідентифікації та класифікації загроз;

– якість і своєчасність комунікацій;

– рівень успішності у запобіганні несанкціонованому доступу;

– покращення показників реагування за часом.

Якщо говорити про більш формалізовані кількісні показники, то організація може оцінювати симуляційні вправи за:

– середнім коефіцієнтом правильного повідомлення/звітування про симульовані атаки на одного працівника (багато правильних повідомлень про атаки під час симуляції свідчать про високий рівень залученості, велику ймовірність виявлення реальних загроз, а також високу ефективність навчання). У подальшому ці дані є основою для відстеження прогресу персоналу.

– часом виявлення загрози (або її перебування в системі) – це період між потраплянням загрози у цільову мережу й повідомленням про неї працівника. Цей показник вводить вимірювання швидкості виявлення загрози. Адже чим швидше виявлено атаку, тим менше шкоди вона може завдати.

– коефіцієнтом відмов – це показник, на якому базується більшість навчальних рішень. Він показує відсоток працівників, які не розпізнали або не повідомили про симульовану кібератаку. Водночас, низький коефіцієнт відмов не завжди свідчить про ефективне навчання, оскільки на нього може впливати рівень складності симуляцій, різноманітність контенту, індивідуальні точки зору, час і частота.

Організації, які регулярно вимірюють ефективність симуляцій, повідомляють про 47% покращення своєї здатності виявляти та реагувати на фактичні інциденти безпеки протягом першого року впровадження [9].

Аналіз за результатами навчання має на меті перетворення досвіду на інформацію. Після завершення вправи необхідно оцінити, як учасники реагували на кожному етапі прийняття рішень, виявити затримки у виявленні або стримуванні загрози, зіставити помилки з потенційними реальними наслідками.

Для цього зазвичай використовують такі фреймворки, як MITRE ATT&CK [52], щоб контекстуалізувати життєвий цикл атаки й оцінити, чи був належним чином розглянутий кожен етап: розвідка, експлуатація вразливості, горизонтальне переміщення, ексфільтрація.

З огляду на те, що навчання не повинно закінчуватися спостереженням, обов’язковим є *закріплення знань і повторне тестування*. Особи, які показали гірші результати симуляції, можуть бути зараховані до цільових сесій мікронавчання, зосереджених на їхніх слабких сторонах. Потім можна повторно запустити оригінальну вправу, щоб оцінити рівень знань і покращення дій після закріплення. Цей цикл повторного тестування не лише загострює індивідуальну компетентність, але й зміцнює координацію команди в умовах стресу.

Звітування за результатами симуляційного навчання забезпечує встановити рівень ефективності вправ, зокрема визначити, які сценарії спрацювали належним чином, а які не були успішними; виявити покращення процесів захисту. Такі звіти дозволяють організації можуть стати основою для оновлення документації та методичних посібників, призначення відповідальних осіб за вибір і впровадження коригувальних дій.

Завдяки регулярному проведенню симуляційного практико-орієнтованого навчання організація може посилити процеси *формування культури постійного вдосконалення*. У цьому контексті доцільно:

– проводити різні види симуляційного навчання принаймні щоквартально;

– ротаційно змінювати сценарії, щоб охопити різні вектори кібератак;

– залучати до навчання учасників з усієї організації, а не тільки команди кіберзахисту;

– пов'язати результати симуляційних вправ із професійним розвитком фахівців;

– оновлювати підходи до навчання на основі уроків з попередніх симуляцій.

Інтеграція результатів у реальну політику й архітектуру безпеки. Інформація за підсумками симуляційного навчання доцільно кодифікувати в політиках безпеки, сценаріях і рішеннях щодо архітектури безпеки. Наприклад, якщо симуляція виявила затримку в комунікації між IT та юридичним відділом під час інциденту, варто уточнити шляхи ескалації або попередньо авторизувати певні дерева рішень. Ця практика усуває розрив між теоретичною підготовкою та операційною готовністю.

Висновки до розділу 3

З огляду на великий попит на симуляційне навчання з кібербезпеки на ринку з’явилося досить багато симуляційних онлайн-платформ, які можна класифікувати за такими критеріями: форматом навчання (віртуальні кімнати й машини, симулятори з використанням реальних сценаріїв інцидентів, класичні й авторські змагання CTF); напрямом (веб-безпека, цифрова криміналістика, реагування на інциденти, OSINT, напад і захист); рівнем складності (початковий, середній, експертний).

Аналіз ринку симуляційних онлайн технологій з кібербезпеки показав, що найбільш популярними є такі Інтернет-платформи як TryHackMe, HackTheBox, OverTheWire, Root-Me, VulnHub, CTFlearn, RangeForce тощо. Встановлено

тенденцій розвитку навчальних онлайн-платформ з кібербезпеки, серед яких розширення можливостей щодо реагування на нові види атак (ланцюги постачань, кібервимагання); автоматизація рутинних операцій через використання тренажерів SOAR/ SIEM, інтеграції з розвідкою загроз; використання хмарних лабораторій на базі AWS, Azure; зростання уваги до формування «м'яких» навичок через модулі з розвитку комунікації, презентації звітів, лідерства і командної роботи; збільшення масштабів використання гейміфікації та рейтингування для мотивування гравців.

Водночас, сучасна організація або окремий фахівець цілком можуть створити симуляційні вправи власними силами, зокрема з допомогою доступних інструментів ШІ. У роботі представлено типовий алгоритм створення інтерактивної симуляційної вправи з використанням чат-бота Poe від соціальної платформи обміну інформацією Quora. Алгоритм охоплює такі етапи: створення й налаштування бота; інструктування бота щодо цілей і сценарію навчання, взаємодії з учасниками і прийняття рішень, завершення вправи; налаштування вступного повідомлення; збереження й тестування симуляційної вправи.

На основі вивчення наукових джерел і кращих практик з питань організації симуляційного навчання в кібербезпеці запропоновано низку рекомендацій для підвищення його ефективності, зокрема необхідним є: аналіз середовища організації перед розробкою вправ; визначення цілей навчання; використання різних видів симуляцій і рівнів складності завдань; створення реалістичних сценаріїв; регулярність і послідовність проведення вправ; підтримка зворотного зв'язку й постійне оновлення методів та змісту навчання; аналіз і звітування за підсумками навчання тощо.

ВИСНОВКИ

У результаті дослідження встановлено, що масштаби застосування симуляцій для навчання кіберфахівців стрімко зростають, оскільки традиційні методи навчання з кібербезпеки стають дедалі менш ефективними, а симуляційне моделювання дозволяє організувати процес навчання через досвід і участь у реалістичних сценаріях безпеки в безпечному середовищі.

Найчастіше основою для симуляційного навчання є: атаки соціальної інженерії; атаки на кінцеві точки і впровадження шкідливого ПЗ; атаки на мережу та інфраструктуру; просунуті тактики симуляції. До основних видів симуляційних методів навчання відносять: штабні навчання; навчання червоної команди; моделювання фішингу й соціальної інженерії; навчальні кіберполігони; симуляції порушень і атак (BAS); змагання CTF.

Як свідчить практика, симуляційне навчання є актуальним і перспективним для використання в кібербезпеці з огляду на такі переваги: доступ до реальних сценаріїв і технологій; експерименти в безпечному середовищі, перевірка готовності до кібератак, тестування планів реагування на інциденти, кількісне оцінювання й аналітика; економічна вигідність; масштабованість рішень; забезпечення нормативної відповідності; формування ефективних кіберкоманд; впровадження кращих практик; розвиток культури кібербезпеки і, в підсумку, - покращення стану кібербезпеки організації.

У технологічному контексті переваги симуляційного підходу охоплюють: візуалізацію атак, процесів захисту інфраструктури і дій кіберкоманд; тестування й усунення несправностей; інтеграцію нових систем та інструментів перед розгортанням; просте обслуговування й оновлення програм для віртуального навчання, що гарантує постійний доступ до актуальної інформації; відносно невисоку вартість і можливість масштабування відповідно до потреб.

З огляду на великий попит на симуляційне навчання з кібербезпеки на ринку з’явилося досить багато симуляційних онлайн-платформ, які можна класифікувати за такими критеріями: форматом навчання (віртуальні кімнати й

машини, симулятори з використанням реальних сценаріїв інцидентів, класичні й авторські змагання CTF); напрямом (веб-безпека, цифрова криміналістика, реагування на інциденти, OSINT, напад і захист); рівнем складності (початковий, середній, експертний).

Аналіз ринку симуляційних онлайн технологій з кібербезпеки показав, що основними тенденціями розвитку у цій сфері є: розширення можливостей щодо реагування на нові види атак; автоматизація рутинних операцій; використання хмарних лабораторій на базі AWS, Azure; зростання уваги до формування «м'яких» навичок (комунікація, лідерство й командна робота; збільшення масштабів використання гейміфікації та рейтингування.

Водночас, сучасна організація або окремий фахівець цілком можуть створити симуляційні вправи власними силами, зокрема з допомогою доступних інструментів ШІ. У роботі представлено типовий алгоритм створення інтерактивної симуляційної вправи з використанням чат-бота Poe від соціальної платформи обміну інформацією Quora. Алгоритм охоплює такі етапи: створення й налаштування бота; інструктування бота щодо цілей і сценарію навчання, взаємодії з учасниками і прийняття рішень, завершення вправи; налаштування вступного повідомлення; збереження й тестування симуляційної вправи.

На основі вивчення наукових джерел і кращих практик з питань організації симуляційного навчання в кібербезпеці запропоновано низку рекомендацій для підвищення його ефективності, зокрема необхідним є: аналіз середовища організації перед розробкою вправ; визначення цілей навчання; використання різних видів симуляцій і рівнів складності завдань; створення реалістичних сценаріїв; регулярність і послідовність проведення вправ; підтримка зворотного зв'язку й постійне оновлення методів та змісту навчання; аналіз і звітування за підсумками навчання тощо.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Hamdi Kavak, José julian Padilla, Daniele Vernon-Bido and others. Simulation for cybersecurity: state of the art and future directions. Journal of Cybersecurity. 2021. 7(1). PP.1-13. DOI:10.1093/cybsec/tyab005

2. Maneesh Varshney, Kent Pickett, Rajive Bagrodia. A Live-Virtual-Constructive (LVC) framework for cyber operations test, evaluation and training. November 2011. URL: https://www.researchgate.net/publication/241633960_A_Live-Virtual-Constructive_LVC_framework_for_cyber_operations_test_evaluation_and_training 54

3. Chi SD, Park JS, Jung KC et al. Network security modeling and cyber attack simulation methodology. *In: Information Security and Privacy*. Berlin: Springer Berlin Heidelberg, 2001; 320-333

4. Taylor C , Krings A , Alves-Foss J. Risk analysis and probabilistic survivability assessment (RAPSA): an assessment approach for power substation hardening. In: *Proc. ACM Workshop on Scientific Aspects of Cyber Terrorism,(SACT), Washington DC*, 2002

5. Vernon-Bido D , Padilla JJ, Diallo S et al. *Towards Modeling Factors That Enable an Attacker*. Montreal, QC: Society for Modeling & Simulation International (SCS), 2016.

6. Kavak H, Padilla JJ, Vernon-Bido et al. *A Characterization of Cybersecurity Simulation Scenarios*. Pasadena, CA: ACM, 2016.

7. Cost of a Data Breach Report. *IBM*. URL: https://wp.table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf

8. Phil Muncaster. Breach and attack simulations can protect your business. URL: https://www.verizon.com/business/resources/articles/s/breach-and-attack-simulations-can-protect-your-business/

9. Mary Marshall. Security Simulation: Practice-Based Cybersecurity Education for Modern Enterprise Defense. October 22, 2025. *Avatier*. URL: https://www.avatier.com/blog/security-simulation-practice-defense/

10. The Complete Guide to Cyber Security Simulation Training. January 15, 2026. *Adaptive Security*. URL: https://www.adaptivesecurity.com/blog/the-complete-guide-to-cyber-security-simulation-training

11. 2024 Cybersecurity Statistics. The Ultimate List Of Cybersecurity Stats Data, & Trends. *PurpleSec*. URL: https://purplesec.us/resources/cybersecurity-statistics/

12. What is Cybersecurity Simulation Training? *CloudLabs*. URL: https://cloudlabs.ai/faq/what-is-cybersecurity-simulation-training/

13. Andrew Mort. 7 Reasons Cybersecurity Simulation Software is Crucial for Protecting Your Business. Feb 01, 2022. *CloudShare* URL: https://www.cloudshare.com/blog/7-reasons-cybersecurity-simulation-software-is-crucial-for-protecting-your-business/

14. Cyber Security Simulation Training: How it Works + Best Practices. September 6, 2024. *Hoxhunt*. URL: https://hoxhunt.com/blog/cyber-security-simulation-training

15. Josh Schneider. What is breach and attack simulation? *IBM*. URL: https://www.ibm.com/think/topics/breach-attack-simulation

16. Joseph Zeto. Cyber Attack Simulation: How to Test and Strengthen Your Network Security. *Apposite Technology*. URL: https://apposite-tech.com/cyber-attack-simulation/

17. Kriti Awasthi. Cyber Attack Simulation: Test Your Security Before Hackers Do. July 7, 2025. *Fidelis Security*. URL: https://fidelissecurity.com/threatgeek/threat-detection-response/cyber-attack-simulation/

18. Domain Spoofing. Glossary. *Barracuda*. URL: https://www.barracuda.com/support/glossary/domain-spoofing

19. Deepfake Statistics 2025: AI Fraud Data & Trends. September 8, 2025. *DeepStrike*. URL: https://deepstrike.io/blog/deepfake-statistics-2025

20. Crystal Turnbull. 6 Best Interactive Cyber Security Training Platforms. *LinkedIn*. URL: https://www.livingsecurity.com/blog/interactive-cyber-security-training

21. Cybersecurity Tabletop Exercise. January 14, 2026. *Bitsight*. URL: https://www.bitsight.com/glossary/cybersecurity-tabletop-exercise

22. CISA Tabletop Exercise Packages. *CISA*. URL: https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages

23. The NIST Cybersecurity Framework (CSF) 2.0. February 26, 2024. *NIST*. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

24. NIST SP 800-61 Rev. 3 Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. *NIST*. URL: https://csrc.nist.gov/pubs/sp/800/61/r3/final

25. The Ultimate Guide to a Cyber Tabletop Exercise in 2026. 7 January 2026. *Cyber Management Alliance*. URL: https://www.cm-alliance.com/cybersecurity-blog/the-ultimate-guide-to-a-cyber-tabletop-exercise-in-2026

26. Red Team Exercises in Cybersecurity: Benefits & Examples. April 14, 2025. *Sentinel One*. URL: https://www.sentinelone.com/cybersecurity-101/services/red-team-exercise-in-cybersecurity/

27. Red Teaming: History, Methodology, and 4 Critical Best Practices. Dec 03, 2024. *Sprocket Security*. URL: https://www.sprocketsecurity.com/blog/red-teaming-best-practices

28. A Simple Guide to Successful Red Teaming. *Cobalt Strike*. URL: https://www.cobaltstrike.com/resources/guides/a-simple-guide-to-successful-red-teaming

29. What is Purple Teaming? *Rapid7*. URL: https://www.rapid7.com/fundamentals/what-is-a-purple-team/

30. Muhammad Raza. What's CTF? Capture The Flag Competitions for Cybersecurity. January 22, 2025. *Splunk*. URL: https://www.splunk.com/en_us/blog/learn/capture-the-flag-ctf.html

31. David Tidmarsh. Why Is Capture the Flag (CTF) Important in Cyber Security? *EC-Council*. URL: https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/capture-the-flag-ctf-cybersecurity/

32. Jackson Evans-Davies. Another Record-Breaking Year: 5th Annual Dragos Capture the Flag (CTF) Results. November 6, 2025 *Dragos*. URL:

https://www.dragos.com/blog/2025-dragos-capture-the-flag-ctf-competition-summary-results

33. Jean Tirstan, Joy Gilbert A, Nelmiawati. Analysis of Cyber Security Knowledge and Skills for Capture the Flag Competition. *Jurnal Integrasi.* 2022. Vol. 14. №1. PP. 14-22.

34. Ben Filipkowski. Capture the Flag: What you should know about cybersecurity CTFs. April 23, 2025. *Field Effect*. URL: https://fieldeffect.com/blog/capture-the-flag-cybersecurity

35. The Cyber Range a Guide. NICE Community Coordinating Council. 2023. *NIST*. URL: https://www.nist.gov/system/files/documents/2023/09/29/The%20Cyber%20Range_A%20Guide.pdf

36. Infinite Angles of Attack Require Limitless. Options for Defence Cyber Range Solutions. *CybExer*. URL: https://lnk.ua/PfXbV431F

37. Cyber Range Features Checklist & List of European Providers. ECSO WG5 2025 edition. *ECSO*. URL: https://ecs-org.eu/ecso-uploads/2025/02/Cyber_Range_Features_Checklist__List_of_European_Providers_2025.pdf

38. Cyber Ranges: Key Features and Functionalities. *Cyber Ranges*. URL: https://cyberranges.com/

39. ТОП-10 платформ для практики з кібербезпеки. 2025. *Oksim*. URL: https://www.oksim.ua/top-10-platform-dlya-praktiki-z-kiberbezpeki/

40. Anyone can learn cyber security with TryHackMe. Hands-on cyber security training through real-world scenarios. *TryHackMe*. URL: https://tryhackme.com/

41. Hack The Box named a Leader in The Forrester Wave™ for Cybersecurity Skills and Training Platforms. *Hack The Box.* URL: https://www.hackthebox.com/

42. Trusted by security professionals. *PortSwigger*. URL: https://portswigger.net/

43. Wargames. *Over the Wire.* URL: https://overthewire.org/wargames/

44. The fast, easy, and affordable way to train your hacking skills. *Root-Me.* URL: https://www.root-me.org/?lang=en

45. Virtual Machines. *VulnHub*. URL: https://www.vulnhub.com/

46. Learn Cybersecurity. The most beginner-friendly way to get into hacking. CTFlearn. URL: https://ctflearn.com/

47. Build high performing defensive cyber teams. *RangeForce*. URL: https://www.rangeforce.com/

48. Тренінговий кіберцентр. *ДЦКЗ Держспецзв'язку.* URL: https://scpc.gov.ua/uk/cyber-trainer

49. Hrishitva Patel. How to Use AI Simulations for Cybersecurity Training. 21 August 2025. *ASIS International.* URL: https://www.asisonline.org/security-management-magazine/articles/2025/08/ai-simulations-cybersecurity-training/

50. About Quora. *Linkedin*. URL: https://ua.linkedin.com/company/quora?trk=ppro_cprof

51. Eliott Tallqvist. Insights From the Hoxhunt Cybersecurity Human Risk Benchmark Challenge. October 19, 2023. URL: https://surl.li/ppciia

52. ATT&CK Matrix for Enterprise. *MITRE*. URL: https://attack.mitre.org/