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: “МОДЕЛЬ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ НАВЧАННЯ СПІВРОБІТНИКІВ ІЗ ПРОТИДІЇ СОЦІОІНЖЕНЕРНИМ АТАКАМ”

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

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

_____ Ілля ПАЛАМАРЧУК
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ-61
Ілля ПАЛАМАРЧУК

Керівник:
Доктор філософії з кібербезпеки Михайло ЗАПОРОЖЧЕНКО

Рецензент:

_____ _____

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

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

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

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Студенту Паламарчуку Іллі Вікторовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи: “Модель оцінювання ефективності навчання співробітників із протидії соціоінженерним атакам”

керівник кваліфікаційної роботи Михайло ЗАПОРОЖЧЕНКО, доктор філософії
(Ім’я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від “30” жовтня 2025 р. № 467.

2. Строк подання кваліфікаційної роботи “11” грудня 2025 р.
3. Вихідні дані до кваліфікаційної роботи: *наукова література, стандарти з ІБ, аналітичні звіти, статистика інцидентів, корпоративні політики безпеки, кейси атак, типові вектори соціоінженерних впливів.*
4. Перелік питань, які потрібно розробити:
   1. Провести аналіз сучасних методів соціальної інженерії та існуючих підходів до оцінювання обізнаності персоналу з питань кібербезпеки.
   2. Розробити модель оцінювання ефективності навчання співробітників із протидії соціоінженерним атакам, що враховує поведінкові та когнітивні показники.
   3. Сформувати практичні рекомендації щодо впровадження розробленої моделі в систему управління інформаційною безпекою організації.
5. Перелік ілюстративного матеріалу: *презентація*
6. Дата видачі завдання “02” жовтня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	11.10.2025	
2.	Збір та аналіз літератури.	20.10.2025	
3.	Дослідження теоретичних та методичних засад оцінювання ефективності навчання персоналу з протидії соціоінженерним атакам	25.10.2025	
4.	Аналіз векторів соціоінженерних атак та існуючих метрик оцінювання стійкості користувачів.	08.11.2025	
5.	Розробка багатофакторної моделі оцінювання ефективності навчання співробітників із протидії соціоінженерним атакам.	16.11.2025	
6.	Формулювання висновків за результатами дослідження.	24.11.2025	
7.	Оформлення роботи.	05.12.2025	
8.	Оформлення презентації.	16.12.2025	
9.	Отримання рецензії на роботу.	17.12.2025	
10.	Захист в ЕК.	__.01.2026	

Здобувач вищої освіти _____ Ілля ПАЛАМАРЧУК
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Михайло ЗАПОРОЖЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

Направляється здобувач Паламарчук І.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека та захист інформації
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Модель оцінювання ефективності навчання співробітників із протидії соціоінженерним атакам"
Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач **ПАЛАМАРЧУК Ілля** у кваліфікаційній роботі проаналізував теоретичні аспекти оцінювання ефективності навчання персоналу, здійснив порівняльний аналіз сучасних метрик та інструментів тестування, а також розробив багатофакторну модель оцінювання поведінкової кіберстійкості співробітників в умовах соціоінженерних загроз.

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

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

Керівник кваліфікаційної роботи _____ Михайло ЗАПОРОЖЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Паламарчук І.В. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою
Управління кібербезпекою та захистом
інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

здобувача вищої освіти Паламарчука Іллі Вікторовича
на тему “ Модель оцінювання ефективності навчання співробітників із протидії соціоінженерним атакам ”

Актуальність За умов стрімкої цифровізації бізнес-процесів людський фактор залишається однією з найкритичніших вразливостей периметра безпеки. Сучасні методи соціальної інженерії ефективно обходять технічні бар'єри, експлуатуючи довіру та психологію співробітників. У цьому контексті критично важливим стає не просто проведення навчання, а й об'єктивне вимірювання його результативності. Дослідження та розробка комплексних моделей, що дозволяють оцінити реальну готовність персоналу протидіяти маніпуляціям, є актуальним науково-прикладним завданням для розвитку систем захисту інформації.

Позитивні сторони

1. У межах роботи здійснено всебічний аналіз сучасних векторів соціоінженерних загроз та існуючих підходів до оцінювання обізнаності персоналу. Проведено критичний огляд метрик ефективності, що дозволило виявити недоліки традиційних статичних методів тестування та обґрунтувати необхідність впровадження динамічних показників кіберстійкості.
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді таблиць та схем. Автор опрацював значну джерельну базу: понад 67 публікацій та електронних джерел, в тому числі англомовних.
3. За результатами дослідження запропоновано рекомендації щодо методики тестування стійкості до соціоінженерних впливів із використанням імітаційних сценаріїв.

Недоліки

1. В межах дослідження значну увагу було приділено розробці концептуальної моделі та архітектури оцінювання, проте для повного розкриття теми доцільно було б здійснити глибинне вивчення аспектів технічної інтеграції з конкретними SIEM-системами.

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 Паламарчук Ілля Вікторович заслуговує присвоєння кваліфікації “Магістр кібербезпеки за освітньо-професійною програмою “Управління інформаційною та кібернетичною безпекою”.

Рецензент:

_____ _____ _____
підпис *(Ім’я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 103 с., 9 рис., 9 табл., 67 джерел.

Метою роботи є підвищення рівня захищеності інформаційних ресурсів організації від соціоінженерних впливів шляхом розробки комплексної моделі оцінювання ефективності навчання співробітників, що дозволить забезпечити об'єктивний контроль набутих навичок та адаптивність системи підготовки кадрів.

Об'єктом дослідження є процес забезпечення інформаційної безпеки організації в умовах впливу соціоінженерних загроз.

Предмет дослідження – моделі, методи та метрики оцінювання ефективності заходів з підвищення обізнаності та навчання співробітників протидії соціоінженерним атакам.

Методи дослідження. Для вирішення поставлених завдань у роботі використано комплекс загальнонаукових та спеціальних методів: метод системного аналізу — для дослідження структури соціоінженерних загроз та існуючих підходів до навчання; методи класифікації та порівняльного аналізу — для систематизації недоліків існуючих методик оцінювання (моделі Кіркпатріка, Філліпса); метод математичного моделювання — для побудови Багатофакторної моделі поведінкової кіберстійкості (MBCR) та розрахунку інтегрального індексу (CRI); логіко-аналітичні методи — для розробки рекомендацій щодо інтеграції моделі в систему управління інформаційною безпекою.

Короткий зміст роботи. У кваліфікаційній роботі проведено аналіз сучасного ландшафту загроз соціальної інженерії та визначено критичну роль людського фактору в системі захисту. Здійснено порівняльний аналіз існуючих інструментів оцінювання обізнаності персоналу, виявлено їх обмеженість у контексті реальних поведінкових реакцій. Основним результатом роботи є розробка Багатофакторної моделі поведінкової кіберстійкості (MBCR), яка, на відміну від традиційних підходів, інтегрує когнітивні, поведінкові, психологічні та контекстуальні параметри.

Запропоновано архітектуру впровадження моделі з використанням компонентно-сервісного підходу та її інтеграцію з системами моніторингу подій безпеки (SIEM) і реагування (SOAR). Розроблено практичні рекомендації щодо використання моделі для реалізації ризик-орієнтованого управління доступом та мінімізації інцидентів, пов'язаних із людським фактором.

Галузь застосування. Отримані результати можуть бути використані при плануванні та реалізації стратегії кадрової безпеки в державних установах, банківському секторі та на підприємствах критичної інфраструктури для переходу від формального навчання до управління кіберстійкістю в режимі реального часу.

КЛЮЧОВІ СЛОВА: СОЦІАЛЬНА ІНЖЕНЕРІЯ, ІНФОРМАЦІЙНА БЕЗПЕКА, ЕФЕКТИВНІСТЬ НАВЧАННЯ, МОДЕЛЬ КІБЕРСТІЙКОСТІ, ЛЮДСЬКИЙ ФАКТОР, КІБЕРГІГІЄНА, SIEM-СИСТЕМА.

ABSTRACT

The textual part of the qualification work for obtaining a Master's degree comprises 103 pages, 9 figures, 9 tables, and 67 references.

The purpose of the work is to increase the level of protection of an organization's information resources against social engineering influences by developing a comprehensive model for evaluating the effectiveness of employee training, which enables objective assessment of acquired skills and ensures adaptability of the personnel training system.

Object of research is the process of ensuring information security of an organization under the influence of social engineering threats.

Subject of research includes models, methods, and metrics for evaluating the effectiveness of awareness-raising and training activities aimed at countering social engineering attacks.

Research methods Methods of system analysis, graph theory, theory of complex networks, theory of sets and theories of information security and information adversarial are used to solve problems and processes of spreading informational influences. The foundations of social psychology were used to model the objects and subjects of information conflict, their characteristics and behavioral strategies.

Brief content of research. As a result, the work analyzed the modern landscape of social engineering threats and determined the critical role of the human factor in the protection system; a comparative analysis of existing tools for assessing personnel awareness was carried out, revealing their limitations in the context of real behavioral reactions. The main result of the work is the development of the Multifactor Behavioral Cyber Resilience Model (MBCR), which, unlike traditional approaches, integrates cognitive, behavioral, psychological, and contextual parameters. An architecture for implementing the model using a component-service approach and its integration with security information and event management (SIEM) and response (SOAR) systems is proposed. Practical recommendations for using the model to implement risk-based access control and minimize incidents related to the human factor are developed.

Field of research. The obtained results can be used in the planning and implementation of the personnel security strategy in government institutions, the banking sector, and critical infrastructure enterprises for the transition from formal training to real-time cyber resilience management.

KEYWORDS: SOCIAL ENGINEERING, INFORMATION SECURITY, TRAINING EFFECTIVENESS, CYBER RESILIENCE MODEL, HUMAN FACTOR, CYBER HYGIENE, SIEM SYSTEM.

ЗМІСТ

ВСТУП

Актуальність теми. Сучасний етап розвитку інформаційного суспільства характеризується тотальною цифровізацією всіх сфер життєдіяльності. Інтернет став невід'ємним елементом функціонування економіки та державного управління, проте стрімкий технологічний прогрес неминуче супроводжується еволюцією кіберзагроз. В умовах, коли технічні засоби захисту інформації досягли високого рівня надійності, вектор атак змістився у бік найслабшої ланки будь-якої системи — людини. Дефіцит медіаграмотності та низька культура кібергігієни серед персоналу створюють критичні вразливості, що неможливо усунути виключно програмно-апаратними методами.

Соціальна інженерія як метод маніпуляції з метою отримання несанкціонованого доступу до інформації сьогодні є домінуючим інструментом кіберзлочинців. Успішні атаки призводять до значних фінансових втрат, витоку конфіденційних даних та руйнування репутації організацій. Поточна ситуація ускладнюється тим, що заходи з навчання персоналу часто мають формальний характер і не забезпечують реальної готовності співробітників протидіяти загрозам.

Таким чином, розробка моделі оцінювання ефективності навчання співробітників для протидії соціоінженерним атакам є актуальним науково-прикладним завданням.

Мета роботи полягає у підвищенні рівня захищеності інформаційних ресурсів організації шляхом розробки моделі оцінювання ефективності навчання, що дозволить забезпечити об'єктивний контроль навичок персоналу та адаптивність системи підготовки кадрів.

Об'єкт дослідження – процес забезпечення інформаційної безпеки організації в умовах впливу соціоінженерних загроз.

Предмет дослідження – моделі, методи та метрики оцінювання ефективності заходів з підвищення обізнаності та навчання співробітників протидії соціоінженерним атакам.

Для досягнення поставленої мети в роботі необхідно вирішити такі *завдання*:

1. Провести аналіз сучасних методів соціальної інженерії та існуючих підходів до оцінювання обізнаності персоналу з питань кібербезпеки.
2. Розробити модель оцінювання ефективності навчання співробітників із протидії соціоінженерним атакам, що враховує поведінкові та когнітивні показники.
3. Сформувати практичні рекомендації щодо впровадження розробленої моделі в систему управління інформаційною безпекою організації.

Методи дослідження. Для вирішення поставлених завдань використано методи системного аналізу, класифікації та порівняння, а також методи моделювання процесів управління інформаційною безпекою.

Наукова новизна отриманих результатів полягає в тому, що в межах роботи запропоновано багатофакторну модель поведінкової кіберстійкості (MBCR), яка інтегрує когнітивні, поведінкові та психологічні параметри, що дозволяє здійснювати оцінювання готовності персоналу в режимі реального часу та адаптувати навчальні сценарії до поточних загроз.

Практичне значення одержаних результатів. Застосування розробленої моделі дозволить здійснити обґрунтований вибір інструментів навчання, об’єктивно оцінити готовність персоналу до інцидентів та оптимізувати ресурси на забезпечення кадрової безпеки.

Апробація результатів. Основні положення та результати кваліфікаційної роботи доповідались та обговорювались на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 27 лютого 2025 року.

РОЗДІЛ 1
СУЧАСНИЙ СТАН ТА ОСОБЛИВОСТІ СОЦІОІНЖЕНЕРНИХ АТАК ЯК ЗАГРОЗИ ІНФОРМАЦІЙНИМ РЕСУРСАМ

Перед початком дослідження теми кваліфікаційної роботи та розробки моделі оцінювання ефективності навчання необхідно провести ґрунтовний аналіз предметної області. Це передбачає ознайомлення з основними визначеннями у галузі соціальної інженерії, вивчення трансформації загроз під впливом новітніх технологій, розгляд типових сценаріїв атак, а також аналіз сучасних методів протидії кіберзагрозам, що базуються на людському факторі. Розуміння ландшафту загроз є критичним фундаментом для побудови будь-якої системи захисту, оскільки неможливо ефективно навчати персонал протидіяти загрозам, природа яких залишається невивченою.

1.1. Поняття та сутність соціальної інженерії в контексті забезпечення інформаційної безпеки організації

В епоху цифрової трансформації інформація стала ключовим активом будь-якої організації, а її захист — пріоритетним завданням менеджменту. Традиційно системи захисту будувалися навколо технічного периметра: брандмауерів, систем виявлення вторгнень та антивірусного програмного забезпечення. Проте зловмисники, адаптуючись до посилення технічного захисту, змістили фокус своїх атак на найслабшу ланку системи — людину.

Сучасний стан інформаційної безпеки характеризується радикальним переходом від технічно орієнтованих експлуатацій програмного забезпечення до витонченого маніпулювання людським фактором. Соціальна інженерія, яку часто називають «мистецтвом обману», у 2024 та 2025 роках досягла безпрецедентного рівня складності, ставши домінуючим вектором початкового доступу до корпоративних та державних мереж. Зловмисники дедалі частіше

віддають перевагу експлуатації довіри, страху та рутинних процесів, а не пошуку вразливостей у програмному коді.

Аналіз глобальної активності у першій половині 2025 року вказує на історичний максимум фішингових інцидентів, що продовжує тенденцію, започатковану наприкінці 2023 року. У 2025 році соціальна інженерія перестала бути окремим типом атаки, перетворившись на «приховану прогалину», яка стоїть за кожним значним зломом. Соціальна інженерія – це стратегія комунікації, яка використовує психологічні прийоми для досягнення бажаного впливу на аудиторію. Її суть полягає в створенні та трансляції повідомлень, що резонують з існуючими потребами та страхами цільової аудиторії, з метою спонукання її до певних дій [1]. Даний метод поєднує в собі як глибокі знання у сфері інформаційних технологій, так і неабиякі навички та знання з соціології та психології. Суть соціальної інженерії полягає у використанні когнітивних викривлень, емоцій (страху, цікавості, співчуття, жадібності) та соціальних норм для маніпуляції жертвою з метою примусити її виконати дії, що суперечать інтересам безпеки, або розголосити конфіденційну інформацію.

Аналіз сучасного стану кібербезпеки свідчить про те, що сучасний стан соціоінженерних атак характеризується їх домінуванням у ландшафті кіберзагроз, інтеграцією з передовими технологіями ШІ та переходом від масових розсилок до високоточних персоналізованих впливів. Це свідчить про еволюцію підходу зловмисників: від стратегії «килимового бомбардування» (масові спам-розсилки з низькою конверсією) до стратегії «снайперського вогню» (таргетовані атаки на конкретних співробітників).

З точки зору методології інформаційної безпеки, соціальна інженерія являє собою специфічний клас загроз, що базується на людській взаємодії. Механізм атаки ґрунтується на застосуванні психологічної маніпуляції, метою якої є спонукання користувачів до здійснення критичних помилок у сфері безпеки або ненавмисного розголошення конфіденційних даних [2].

Фундаментальна відмінність цього вектору від традиційного хакінгу полягає в об'єкті впливу: замість експлуатації технічних вразливостей програмного забезпечення, атакуючий експлуатує когнітивні механізми та емоційні стани людини (довіру, страх, цікавість). Основна мета зловмисника — маніпулювати жертвою таким чином, щоб вона виконала бажану дію, наприклад, розкрила запитувану інформацію або надала доступ до активів, фактично порушуючи встановлені політики безпеки організації [3]. Реалізація атаки часто відбувається поетапно: від попереднього збору інформації про ціль до встановлення довірливого контакту, який слугує стимулом для подальших дій, що компрометують систему захисту [2].

Соціальний інженер – фахівець широкого профілю, який зазвичай володіє нестандартним способом мислення, гнучким розумом, використовує обман, психологічний вплив, переконання, хороші манери в спілкуванні, позитивні та негативні якості людини для того, щоб змусити людину робити справи, які вони не робили б зазвичай для незнайомої людини [4].

Соціальний інженер у контексті інформаційної безпеки розглядається як специфічний суб'єкт загрози [4]. Це поняття можна деталізувати через сукупність наступних характеристик, що також зображені на рис. 1.1:

- є активним порушником периметра інформаційної безпеки, який діє всупереч встановленим політикам захисту, маючи на меті несанкціоноване подолання системи розмежування доступу не через технічні вразливості, а через людський фактор;
- володіє розвиненими компетенціями у сфері соціальної інженерії, застосовуючи техніки містифікації (видавання себе за іншу особу), переконання та шахрайства як основний інструментарій для реалізації вектора атаки;
- здатний здійснювати цілеспрямований психологічний вплив, експлуатуючи когнітивні викривлення та емоційні стани жертви (довіру, страх, цікавість) для маніпулятивного спонукання її до виконання дій, що порушують регламенти безпеки (наприклад, розголошення паролів або запуск шкідливого ПЗ);

- застосовує комплексні методи розвідки (Reconnaissance) для збору інформації, використовуючи як відкриті джерела (OSINT), так і методи прямої комунікації, щоб акумулювати дані, необхідні для підвищення вірогідності успішної атаки;
- володіє аналітичними здібностями для ефективного синтезу отриманих даних, що дозволяє інтегрувати розрізнені фрагменти інформації у цілісний та переконливий сценарій атаки (претекст), адаптований під конкретну жертву або організацію;
- поєднує психологічні навички з глибокими технічними знаннями у сфері інформаційних технологій, архітектури комп'ютерних мереж та процедур автентифікації, що дозволяє формулювати технічно грамотні запити та уникати викриття під час спілкування з кваліфікованим персоналом.

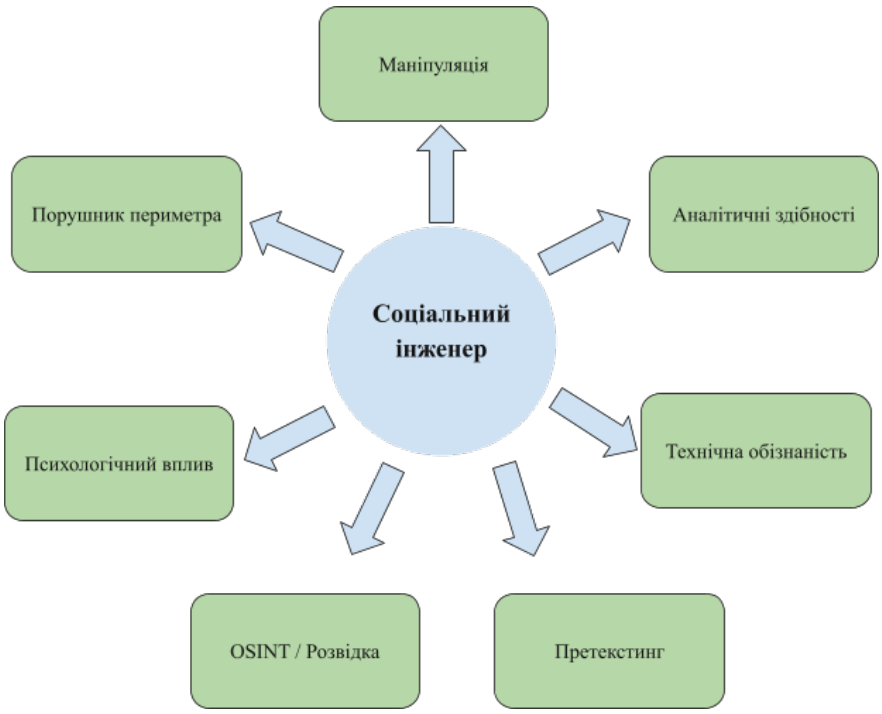

Рис. 1.1. Концептуальна схема характеристик соціального інженера як суб'єкта загрози

Соціальні інженери є креативними, і можна очікувати, що їхні тактики будуть еволюціонувати, щоб скористатися новими технологіями та ситуаціями [5].

Соціальна інженерія — це «мистецтво і наука змушувати людей виконувати ваші бажання» [6]. Її можна визначити як практику отримання інформації технічними та нетехнічними засобами [7]. Отже, атаки соціальної інженерії базуються на переконанні людей, що соціальний інженер є надійним другом або колегою.

Ключовим теоретичним підґрунтям сучасних атак залишаються принципи впливу, описані Робертом Чалдіні, але адаптовані до можливостей штучного інтелекту та миттєвих комунікацій. Принцип терміновості (Urgency) та страху (Fear) використовується для зменшення впливу критичного мислення на рішення особи. Повідомлення про підозрілу активність на рахунку або загрозу блокування облікового запису протягом однієї години стимулюють паніку, за якої користувач не помічає ознак підробки.

Принцип авторитету реалізується через імітацію запитів від вищого керівництва (CEO) або IT-адміністраторів. Оскільки людська психіка історично схильна до покори авторитетним фігурам, запит від «генерального директора» на терміновий переказ коштів часто виконується без жодних сумнівів. Узагальнення ключових психологічних принципів, що використовуються в соціоінженерних атаках, та механізмів їх експлуатації наведено в таблиці 1.1.

Таблиця 1.1

Психологічні принципи соціальної інженерії та механізми їх експлуатації

Психологічний принцип	**Механізм експлуатації**	**Приклад реалізації у 2025 році**
Дефіцит (Scarcity)	Створення відчуття обмеженості часу або ресурсу	Таймери зворотного відліку на сторінках оновлення ПЗ
Взаємність (Reciprocity)	Пропозиція дрібної послуги або «подарунка»	Безкоштовні PDF-інструкції, що містять шкідливі скрипти
Соціальний доказ (Social Proof)	Створення ілюзії, що «всі вже це зробили»	Фальшиві відгуки на фішингових сайтах або згадка колег у листі
Прихильність (Liking)	Встановлення рапорту через компліменти або спільні інтереси	Кампанії в LinkedIn, що починаються з пропозицій про співпрацю

Важливо розуміти, що успішна реалізація соціоінженерної атаки — це не кінцева мета зловмисника, а лише інструмент або вектор доставки для досягнення конкретних деструктивних результатів. Специфіка цих загроз полягає в їхній асиметричності: мінімальні ресурси, витрачені на підготовку фішингового листа чи телефонного дзвінка, можуть призвести до катастрофічних наслідків, які неможливо нівелювати навіть найдорожчими апаратними засобами захисту.

Якщо розглядати організацію як складну соціотехнічну систему, то соціальна інженерія діє як «універсальний ключ», що дозволяє обійти ешелоновану оборону периметра. Наслідки таких атак виходять далеко за межі суто технічних інцидентів, трансформуючись у фінансові, репутаційні та правові ризики.

Однією з найбільш поширених та очевидних загроз є витік конфіденційної інформації. Цей сценарій передбачає несанкціоноване розголошення відомостей, що становлять комерційну таємницю, персональних даних клієнтів або співробітників, а також облікових даних для доступу до внутрішніх систем. Втрата конфіденційності в даному випадку відбувається добровільно з боку жертви, яка введена в оману, що робить цей процес непомітним для систем моніторингу трафіку до моменту фактичного оприлюднення даних. Дотичною, але більш витонченою загрозою є обхід засобів захисту від витоку інформації. Технічні системи DLP ефективно блокують спроби передачі файлів з певними сигнатурами через електронну пошту або на зовнішні носії. Проте соціальна інженерія дозволяє «обійти» ці алгоритми через використання альтернативних каналів комунікації, які не піддаються машинному аналізу. Це може бути продиктування пароля телефоном, фотографування екрана монітора з секретним документом або передача інформації під час особистої зустрічі.

Серйозною загрозою, особливо для наукоємних та виробничих компаній, є порушення авторських прав та крадіжка інтелектуальної власності. Ця діяльність часто кваліфікується як промислове шпигунство. Зловмисники

можуть використовувати методи претекстингу для отримання доступу до вихідного коду програмного забезпечення, креслень, патентної документації або стратегічних планів розвитку компанії. Втрата ексклюзивних прав на інтелектуальний продукт може призвести до втрати конкурентних переваг на ринку ще до офіційного релізу продукту. Безпосередньо з цим пов'язане шахрайство з інформаційними активами. Легітимні облікові записи з високими правами доступу є цінним товаром на чорному ринку кіберзлочинності. Соціальні інженери часто атакують адміністраторів систем або топ-менеджмент з метою перехоплення їхніх сесій. Отримані таким чином цифрові ідентичності можуть бути використані для подальшого продажу так званим брокерам початкового доступу.

Прямі фінансове шахрайство завдає найбільш відчутних та швидких втрат. Сценарії, відомі як компрометація ділової електронної пошти, можуть включати підробку рахунків-фактур, де реквізити легітимного постачальника замінюються на рахунки зловмисників. Інший поширений варіант — вимога від імені керівника здійснити термінову транзакцію на значну суму. Оскільки платіж ініціює авторизований співробітник, банківські системи антифроду часто не розпізнають таку операцію як підозрілу. Крім прямих фінансових втрат, існує загроза нецільового використання інформаційних ресурсів організації. Зловмисники можуть використовувати обчислювальні потужності скомпрометованих через фішинг комп'ютерів для власних цілей, наприклад, для майнінгу криптовалют, організації розподілених атак DDoS або як проксі-серверів для приховування іншої злочинної діяльності. Це призводить до зносу обладнання, сповільнення бізнес-процесів та збільшення операційних витрат.

Катастрофічним наслідком є пошкодження або блокування IT-інфраструктури. Соціальна інженерія є основним вектором доставки програм-вимагачів. Відкриття одного шкідливого вкладення неуважним співробітником може призвести до шифрування всіх серверів компанії, зупинки виробництва та блокування операційної діяльності на тривалий час, що завдає колосальних

збитків. Нарешті, слід відзначити ризик модифікації або знищення конфіденційної інформації. Окрім крадіжки, існує загроза порушення цілісності даних. Зловмисник, отримавши доступ через довірливого користувача, може непомітно внести зміни в бази даних, наприклад, змінити суми заборгованості, або підробити лог-файли для приховування слідів присутності. Найбільш критичним є цілеспрямоване знищення резервних копій, що робить відновлення системи неможливим і підтверджує, що людський фактор є ключовим ризиком для цілісності та доступності інформаційних систем.

Фундаментальну основу більшості сучасних кіберзагроз становить Фішинг, який визначається як метод отримання конфіденційних даних користувача шляхом маніпулятивного обману через електронні листи чи повідомлення . Ця методологія базується на імітації офіційних запитів від легітимних організацій і нагадує риболовлю, де зловмисник розсилає масові "приманки" в надії, що частина отримувачів розкриє свої дані . Основними каналами поширення є електронна пошта та соціальні мережі, а технічна реалізація часто включає підроблені веб-сторінки та шкідливі вкладення [8].

В умовах мобільної комунікації поширеним є смішинг (Smishing) — різновид фішингу, де інструментом атаки виступають SMS-повідомлення. Унікальність методу полягає у високому рівні довіри користувачів до повідомлень на особистих пристроях. Через обмеженість формату SMS зловмисники використовують короткі фрази та скорочені посилання, закликаючи до негайних дій під загрозою фінансових санкцій або блокування послуг.

Більш складною технікою є Претекстинг (Pretexting), що передбачає створення вигаданого сценарію (претексту) для завоювання довіри жертви. На відміну від масових розсилок, тут зловмисник імітує конкретну роль (аудитора, IT-спеціаліста) та використовує дані попередньої розвідки. Мета полягає у створенні атмосфери, в якій передача конфіденційної інформації виглядає логічною та необхідною дією [9].

Для атак на конкретні цілі застосовується Спір-фішинг (Spear Phishing) — високоточна операція, де повідомлення персоналізується під професійні інтереси та обов'язки жертви. Окремим підвидом є "полювання на китів" (Whaling), спрямоване на топ-менеджмент, та компрометація ділової пошти (BEC), що часто завдає значних фінансових збитків. Ефективність таких атак базується на ретельному вивченні профілю жертви [10].

На експлуатації людської цікавості або жадібності ґрунтується Бейтінг (Baiting). Метод передбачає використання фізичних (заражені USB-накопичувачі) або цифрових "приманок", на які жертва має натрапити самостійно. Підключення знайденого носія або завантаження "безкоштовного" контенту призводить до автоматичного встановлення шкідливого програмного забезпечення [11].

Принцип взаємності використовує метод Квід про кво (Quid Pro Quo), де атакуючий пропонує послугу в обмін на інформацію. Найпоширеніший сценарій — імітація технічної підтримки, яка пропонує вирішити неіснуючу проблему в обмін на паролі або віддалений доступ. Жертва, відчуваючи вдячність за допомогу, часто ігнорує правила безпеки [12].

Загрозу фізичному периметру безпеки становить Тейлгейтинг (Tailgating), що дозволяє обійти системи контролю доступу шляхом слідування за авторизованим співробітником. Зловмисники використовують соціальні норми ввічливості, імітуючи зайнятість рук або впевнену поведінку, щоб змусити працівників притримати двері. Це створює ризики як для витоку даних, так і для фізичної безпеки об'єкта.

Інтеграція технологій генеративного штучного інтелекту (GenAI) у сферу кіберзлочинності ознаменувала перехід від ручного створення контенту атак до автоматизованих, високоточних кампаній. Фундаментальна зміна полягає у тому, що LLM, такі як GPT-4, Claude та Gemini, змінюють ландшафт кіберзагроз, особливо в області соціальної інженерії. Ці моделі дають можливість зловмисникам автоматизувати, персоналізувати та масштабувати атаки фішингу,

видавання себе за іншу особу та компрометації ділової електронної пошти (BEC) із безпрецедентним реалізмом [13].

Найбільш помітний вплив технології спостерігається у текстовому векторі атак. Традиційні методи виявлення фішингу, які базувалися на пошуку лінгвістичних аномалій, втрачають свою ефективність. Інструменти генеративного ШІ можуть створювати технічно бездоганну прозу практично всіма основними світовими мовами, приховуючи деякі з найбільш очевидних ознак соціальної інженерії та обманюючи більше жертв [14]. Це також усуває мовні бар'єри для зловмисників, дозволяючи реалізовувати сценарії багатомовного фішингу, де раніше обмеженням було вільне володіння мовою, а тепер доступна адаптація перекладу та тону в реальному часі.

Масштабування цих загроз підтверджується статистичними даними, що свідчать про масове прийняття нових інструментів кіберзлочинцями. Згідно з останніми дослідженнями, понад 82,6% усіх фішингових електронних листів, проаналізованих у період із вересня 2024 року по лютий 2025 року, використовували ШІ в тій чи іншій формі [15]. Така насиченість цифрового простору синтетичним контентом створює значне навантаження на персонал організацій, якому стає все важче відрізнити легітимну комунікацію від шкідливої. Наукові дослідження сприйняття таких атак показують пряму залежність між якістю генерації та успішністю маніпуляції. Кореляція між двома змінними вказує на помірний позитивний зв’язок, оскільки коефіцієнт кореляції Пірсона становить 0,468, що досягає статистичної значущості 0,01. Це означає, що чим вищий рівень реалістичності вмісту, створеного ШІ, то більшою мірою люди відчуватимуть, що атака соціальної інженерії на основі ШІ є більш екстремальною та значущою [16].

Окрім текстових загроз, критичним викликом стає еволюція мультимедійних атак. Клонування голосу на основі ШІ тепер може імітувати людську мову з надзвичайною точністю, вводячи потужну дозу реалізму у фішингові схеми. Яскравим прикладом матеріалізації цієї загрози є інциденти,

де шахраї викрали понад 200 мільйонів гонконгських доларів у компанії, використовуючи клонування голосу та діпфейки. Показовим є те, що навіть професійні команди з тестування безпеки, такі як Mandiant Red Team, включила ці TTP (Tactics, Techniques, and Procedures) під час тестування захисних механізмів.

Найвищим рівнем складності сучасних атак є так звана кросмодальна оркестрація, яка синхронізує діпфейк-відео, клонований аудіозапис, синтетичні документи, що посвідчують особу, та генерацію природної мови [13]. Це дозволяє створювати цілісні синтетичні особистості, верифікація яких традиційними методами стає майже неможливою.

Перспектива розвитку загроз пов'язана з переходом від пасивного використання інструментів до автономних систем. Агентський ШІ (Agentic AI) являє собою фундаментальний стрибок уперед. Ці системи можуть мислити, приймати рішення, навчатися на помилках і працювати разом для вирішення складних проблем, подібно до команди людських експертів. На відміну від попереднього ШІ, який чекає на команди, агентський ШІ може ставити власні цілі, розробляти плани для їх досягнення та адаптуватися, коли обставини змінюються. Це означає появу загроз, здатних динамічно змінювати вектори атаки в залежності від реакції жертви без участі оператора-людини.

Враховуючи вищезазначене, парадигма захисту також потребує докорінних змін. Ефективний захист в еру генеративного ШІ вимагає переходу до архітектури "Нульової довіри" (Zero Trust), яка розглядає кожну взаємодію як потенційно ворожу, покладаючись на поведінкову телеметрію для виявлення тонких аномалій у моделях поведінки користувачів.

На даркнет-форумах сформувався стійкий ринок шкідливих моделей штучного інтелекту. Такі інструменти, як WormGPT, FraudGPT та SpamGPT, спеціально навчені для написання шкідливого коду та створення ідеальних фішингових повідомлень. Вони не мають етичних обмежень, властивих публічним моделям, таким як ChatGPT, і дозволяють зловмисникам генерувати

тисячі унікальних варіантів приманок, що робить контентні фільтри безпеки неефективними. Порівняння моделей ШІ, що використовується зловмисниками надане у таблиці 1.2.

Таблиця 1.2

Порівняння зловмисних моделей ШІ

Інструмент Dark AI	**Спеціалізація**	**Вплив на безпеку**
FraudGPT	Створення фішингових сторінок та експлуатація вразливостей	Знижує бар'єр входу для нових кіберзлочинців
WormGPT	Написання шкідливого коду та BEC-листів	Дозволяє створювати листи без граматичних помилок
SpamGPT	Автоматизація та A/B тестування спам-кампаній	Забезпечує доставку приманок у масштабах, що долають ліміти виявлення
Xanthorox AI	Автоматизація соціоінженерних циклів	Прискорює розробку індивідуальних сценаріїв атак

Крім того, з'являються експериментальні зразки шкідливого ПЗ, які використовують можливості LLM безпосередньо під час виконання для динамічної зміни своєї поведінки з метою уникнення виявлення антивірусними системами.

Технології діпфейків трансформували вішинг у надзвичайно небезпечну загрозу. Кількість інцидентів з використанням глибоких підробок у першому кварталі 2025 року зросла на 19% порівняно з усім 2024 роком [17]. Збитки від таких атак тільки у другому кварталі 2025 року склали близько 350 мільйонів доларів США [18].

Найбільш небезпечним розвитком є «живі діпфейки» (Live Deepfakes). Під час реальних відеодзвінків зловмисники імітують вигляд та голос керівників компаній або партнерів, що дозволяє їм здійснювати «висококонтактні» маніпуляції. Це створює умови для успішного проведення масштабних фінансових шахрайств, оскільки жертва впевнена, що бачить і чує живу людину,

яку вона знає. У 2024 році бізнеси втрачали в середньому $500,000 на кожному успішному інциденті з використанням діпфейків [19].

Аналіз трендів на 2026–2030 роки вказує на те, що ми перебуваємо на порозі появи повністю автономних систем соціальної інженерії.

Якщо у 2024–2025 роках AI використовувався як інструмент підтримки (копірайтинг, клонування голосу), то у 2026 році очікується поява автономних «кіберзлочинних агентів». Ці системи зможуть самостійно вести складні багатоступеневі розмови з багатьма цілями одночасно, адаптуючи тактику в реальному часі на основі реакцій жертви[20]. Такі агенти зможуть виконувати повний цикл атаки: від OSINT-розвідки до фінального викрадення даних, мінімізуючи участь людини та роблячи атаки неймовірно дешевими та масштабними.

З розвитком квантових обчислень зростає ризик атак типу «збирай зараз, дешифруй пізніше» (harvest now, decrypt later). Зловмисники вже зараз можуть накопичувати зашифровані дані, сподіваючись зламати їх у майбутньому. Це вимагає від організацій поступового переходу на квантово-стійке шифрування, особливо для критично важливих інформаційних ресурсів.

1.2. Роль людського фактору в системі управління інформаційною безпекою підприємства

У сучасному цифровому середовищі забезпечення інформаційної безпеки виходить далеко за межі суто технічних рішень. Еволюція кіберзагроз демонструє, що навіть найбільш досконалі архітектури захисту, побудовані на базі штучного інтелекту та криптографії, можуть бути скомпрометовані через одну помилкову дію користувача. Незалежно від складності програмно-апаратних комплексів захисту, центральним елементом будь-якої інформаційної системи залишається людина. Саме вона приймає рішення, надає доступи, обробляє дані та реагує на інциденти. Саме тому аналіз ролі людського фактору

є критично важливим етапом у побудові ефективної СУІБ. Ігнорування цього аспекту призводить до ситуації, коли інвестиції в технічні засоби не приносять бажаного результату через низьку культуру кібербезпеки персоналу.

Розуміння природи людської помилки починається з визначення самого поняття. Згідно з офіційним визначенням, закріпленим у нормативно-правовій базі України, Людський фактор — індивідуальні характеристики персоналу (психофізіологічний стан, кваліфікація та інші), які впливають на забезпечення ядерної та радіаційної безпеки (позитивно чи негативно) [21]. Хоча це визначення походить зі сфери фізичної безпеки, воно влучно описує дуалістичну природу впливу людини на будь-яку систему безпеки: співробітник може бути як найсильнішою ланкою (завдяки кваліфікації та пильності), так і найслабшою (через психофізіологічний стан, втому або стрес). У контексті інформаційних систем це означає, що емоційний стан або рівень концентрації адміністратора чи оператора може стати вирішальним фактором під час кібератаки.

Для глибокого аналізу проблеми необхідно звернутися до теоретичних основ. У науковій літературі поняття людського фактору розглядається у двох основних підходах: широкому та вузькому. Широкий підхід охоплює людські ресурси в цілому та всі види діяльності, до яких вони залучені в межах підприємства. Такий погляд дозволяє оцінити вплив організаційної культури та управлінських процесів на безпеку.

Представниками широкого підходу є Козмінський та Ємельняк, які зазначають, що людський фактор — це досить широка група понять, що зустрічаються в теорії та практиці менеджменту. До них відносяться конкретні особи та групи людей, які заповнюють організаційні структури та виконують обов'язки і завдання, що випливають з їхніх ролей в організаціях, а також досягають своїх особистих цілей і прагнень [22]. Цей підхід підкреслює, що кожен співробітник діє не ізольовано, а в рамках певної структури, переслідуючи власні цілі, які іноді можуть суперечити політикам безпеки. Аналогічної думки дотримується Лент, який стверджує, що людський фактор визначає всіх осіб, які

беруть участь у проєкті, та людей з оточення проєкту, на яких він впливає. Людський фактор визначає всіх учасників проекту та людей, які знаходяться в оточенні проекту і на яких він впливає, з усіма їхніми відносинами та взаємодіями [23].

У складних людино-машинних системах людина розглядається не просто як користувач, а як активний елемент управління, чия ефективність залежить від когнітивного навантаження, психофізіологічного стану та навколишнього середовища. Ускладнення виробничих процесів та впровадження штучного інтелекту призводять до того, що вимоги до професійної підготовки та психологічної стійкості працівників зростають експоненціально.

Людський фактор у теорії управління ризиками розглядається через два фундаментальні компоненти: ставлення до ризику та сприйняття ризику. Ставлення до ризику визначає індивідуальну та колективну схильність персоналу до прийняття рішень у ситуаціях невизначеності. Сприйняття ризику, у свою чергу, є здатністю суб'єкта адекватно усвідомлювати потенційні загрози. Деформація сприйняття часто стає причиною того, що співробітники ігнорують складні парольні політики або протоколи двофакторної автентифікації, вважаючи їх надлишковими перешкодами для продуктивності.

Класифікація проявів людського фактора традиційно поділяється на дві категорії: ненавмисні помилки та свідомі порушення. Помилка — це дія або рішення, що є відхиленням від правильного алгоритму через втому, стрес, недостатню пильність або дефіцит знань. Порушення ж мають на увазі усвідомлене ігнорування встановлених правил. При цьому порушення не завжди мають зловмисний характер; часто вони є результатом спроби оптимізувати робочі процеси в обхід "незручних" засобів контролю. Психологічна установка оператора, його емоційна напруженість та рівень підготовки формують базис надійності всієї СУІБ підприємства.

Однак, коли мова йде про моделювання загроз та оцінку ризиків, загальних визначень недостатньо. Для сфери інформаційної безпеки більш прикладним є

вузький підхід, який визначає людський фактор як набір характеристик і поведінки, що впливають на функціонування системи. Ванг підкреслює, що людські фактори — це ролі та ефекти людської діяльності в системі, які вносять додаткові сильні сторони, слабкі сторони та невизначеність [24]. Саме ця «невизначеність» є ключовим викликом для фахівців з кібербезпеки, оскільки поведінку людини важче прогнозувати та алгоритмізувати, ніж роботу програмного коду.

Людина, будучи головним компонентом як інформаційної, так і IT-системи, своїми діями безпосередньо формує рівень безпеки керованих ресурсів. У багатьох дослідженнях саме персонал визначається як основна причина загроз, що підтверджує відому аксіому: система безпеки настільки сильна, наскільки сильною є її найслабша ланка. Ця теза набуває особливої актуальності в епоху гібридних загроз, коли межа між зовнішнім та внутрішнім периметром безпеки розмивається.

Зловмисники та розробники шкідливого програмного забезпечення активно використовують людські слабкості для інфільтрації в корпоративні мережі. Вони розуміють, що обійти міжмережевий екран складно, але змусити співробітника натиснути на посилання — значно простіше. Часто це відбувається через експлуатацію цікавості або недбалості користувачів, наприклад, через відкриття фішингових листів. Помилка користувача в цьому випадку полягає в завантаженні програмного забезпечення з неперевірених джерел. Така дія часто є автоматичною реакцією на грамотно побудований сценарій соціальної інженерії.

До основних помилок персоналу(зображені на рис. 1.2), які не є наслідком прямого саботажу, але суттєво впливають на інформаційну безпеку, відносять цілий спектр поведінкових патернів:

- перш за все, це надмірна довіра до контенту в глобальній мережі. Користувачі часто не перевіряють джерела інформації, вважаючи, що наявність антивірусу гарантує повну безпеку;

- по-друге, це використання заходів безпеки низького рівня, таких як слабкі паролі. Небажання запам'ятовувати складні комбінації призводить до використання примітивних паролів (наприклад, "123456"), що робить систему вразливою до брутфорс-атак;
- по-третє, це підключення мобільних пристроїв до незахищених мереж. У прагненні залишатися на зв'язку співробітники часто ігнорують ризики перехоплення трафіку в публічних Wi-Fi мережах;
- нарешті, критичною проблемою є приховування помилок, пов'язаних із забезпеченням інформаційної безпеки. Страх покарання змушує працівників мовчати про інциденти, що дає зловмисникам додатковий час для закріплення в системі.

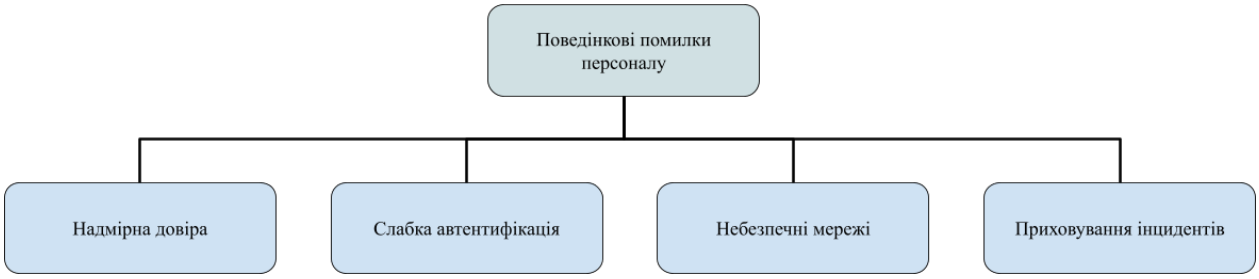

Рис. 1.2. Поведінкові помилки персоналу

Масштаб проблеми ілюструє той факт, що майже половина інцидентів може бути пов'язана з випадковим порушенням політики безпеки. Особливу небезпеку становить латентність таких порушень. У багатьох випадках (до 40%) співробітники намагаються приховати інцидент, що лише збільшує потенційні збитки для бізнесу [25]. Це створює "сліпі зони" для служби безпеки, яка дізнається про атаку вже на етапі витоку даних або шифрування серверів.

Аналіз ландшафту загроз інформаційній безпеці дозволяє стверджувати, що інсайдерські ризики в СУІБ не є гомогенним явищем, а поділяються на кілька категорій залежно від інтенції суб'єкта та механізму виникнення інциденту. Парадокс сучасного сприйняття кібербезпеки полягає в тому, що хоча медійна увага часто прикута до зловмисних шпигунів та спланованих диверсій,

статистично найбільш небезпечними для організацій є недбалі та випадкові інсайдери, чиї дії не мають на меті завдати шкоди, проте призводять до критичних наслідків.

Категорія зловмисних інсайдерів (Malicious Insiders) охоплює співробітників, які свідомо використовують свій легітимний доступ до корпоративних ресурсів для реалізації деструктивних дій, таких як крадіжка інтелектуальної власності, продаж конфіденційних баз даних конкурентам або прямий саботаж функціонування інформаційних систем. Дослідження мотиваційної складової показують, що домінуючим фактором у таких випадках є фінансова вигода, яка фігурує у розслідуваних інцидентах, тоді як іншими поширеними мотивами виступають помста за несправедливе (на суб'єктивну думку працівника) ставлення з боку керівництва або ідеологічні міркування. З технічної точки зору, особливу загрозу в цьому сегменті становлять користувачі з розширеними привілеями — системні адміністратори та розробники програмного забезпечення. Їхня висока кваліфікація та рівень доступу дозволяють їм створювати "приховані входи" (backdoors) у систему або навмисно відключати механізми логування подій для ефективного приховування своїх слідів та ускладнення форензік-розслідування [26].

Діаметрально протилежною за намірами, але не менш руйнівною за наслідками, є категорія ненавмисних інсайдерів (Unintentional Insider Threats). До цієї групи належать авторизовані користувачі, які створюють вразливості в периметрі безпеки через власну необережність, некомпетентність або ігнорування політик безпеки. Типовим проявом такої недбалості є помилкова відправка конфіденційних документів або внутрішньої документації на неправильну адресу електронної пошти, що часто трапляється через функції автозаповнення в поштових клієнтах. Іншим системним проявом людського фактору є недотримання цифрової гігієни, зокрема використання слабких або повторюваних паролів для різних сервісів. Це явище створює передумови для

атак типу credential stuffing, коли скомпрометовані дані з одного ресурсу автоматично використовуються для доступу до корпоративних систем [27].

Крім того, ненавмисна загроза посилюється через поведінку співробітників у публічному інформаційному просторі. Публічне розкриття особистої або службової інформації в соціальних мережах дозволяє зловмисникам формувати детальні цифрові профілі жертв, що значно полегшує підготовку та реалізацію таргетованих атак соціальної інженерії [28]. Новітнім викликом для СУІБ стала проблема так званого Shadow AI — несанкціонованого використання інструментів генеративного штучного інтелекту (GenAI) для вирішення робочих завдань. Завантаження корпоративних даних у публічні чат-боти для аналізу або обробки фактично призводить до їх витоку в бази навчання моделей, роблячи конфіденційну інформацію потенційно доступною для третіх осіб [29].

Трансформація загроз у 2025 році призвела до появи та закріплення нового терміну — індукований інсайдер (coerced insider). Ця категорія описує ситуації, коли лояльного та добропорядного співробітника примушують до співпраці зі зловмисниками проти його волі. Інструментами тиску виступають шантаж, погрози фізичної розправи або репутаційного знищення, причому для фабрикації компромату або створення переконливих сценаріїв тиску все частіше використовуються технології діпфейків [30].

Усунення впливу людського фактору є надзвичайно складним завданням, оскільки неможливо очевидними шляхами “покращити” захист людської психіки так само як програмне забезпечення. Більшість сучасних хакерів керуються принципом, озвученим Кевіном Мітніком: «Я зламував людей, а не паролі». Ця фраза підкреслює, що технічний захист є вторинним по відношенню до психологічної стійкості персоналу.

Тому стратегія захисту повинна базуватися не лише на технічних засобах, а й на систематичному навчанні та розумінні мотивації дій співробітників. Простого ознайомлення з інструкціями недостатньо — необхідно формувати

культуру кібербезпеки. Необхідно переконатися, що персонал усвідомлює можливі ризики та тактики вилучення інформації потенційними конкурентами. [31]. Тільки перетворивши кожного співробітника на активний елемент системи захисту ("людський фаєрвол"), організація може розраховувати на ефективну протидію сучасним соціоінженерним загрозам. Інсайдерські загрози в системі управління інформаційною безпекою не є однорідним явищем і можуть бути класифіковані за інтенцією суб'єкта та механізмом виникнення інциденту. Узагальнену класифікацію основних типів інсайдерських загроз наведено на рисунку 1.3.

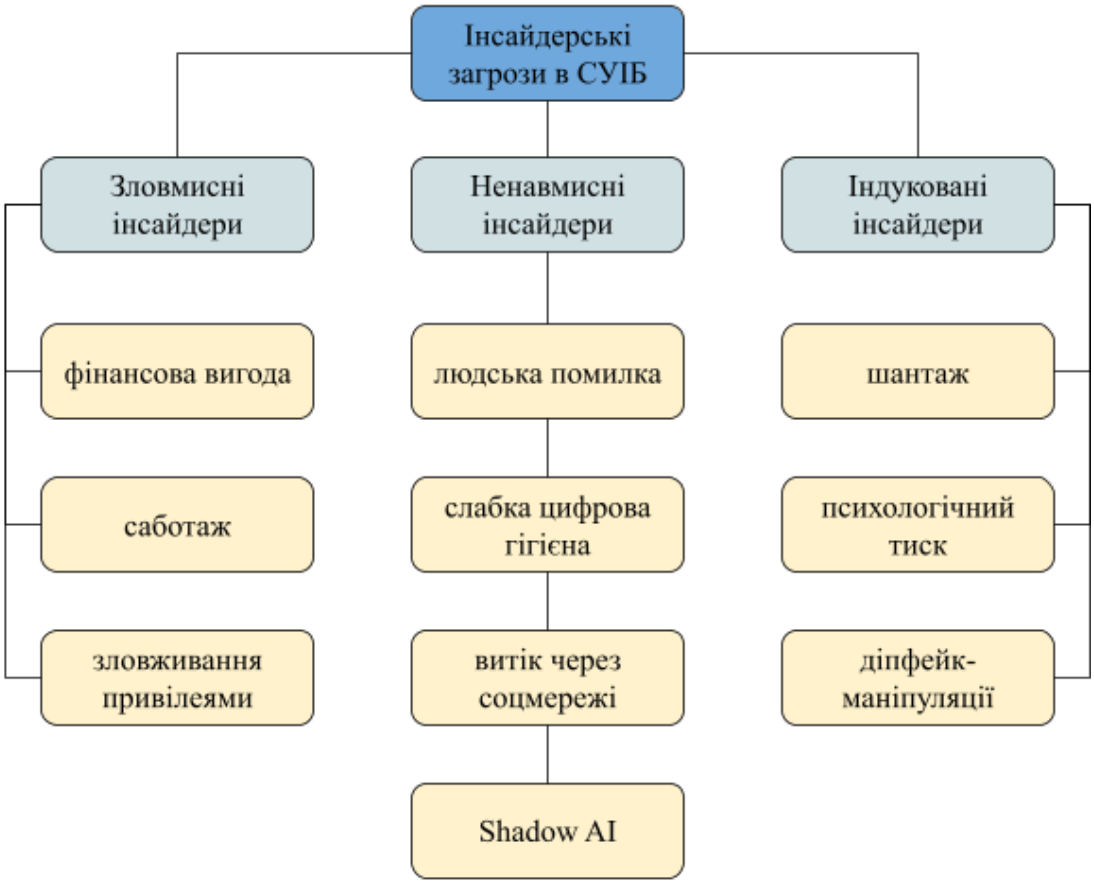

Рис. 1.3. Типи інсайдерських загроз

Еволюція підходів до забезпечення інформаційної безпеки демонструє необхідність перегляду парадигми роботи з персоналом. Традиційні методи управління людським фактором, що обмежувалися щорічними лекціями та

формальними інструктажами, на сьогоднішній день визнані неефективними, оскільки вони не формують стійких навичок. Сучасна СУІБ вимагає переходу до концепції динамічного управління людськими ризиками (Human Risk Management — HRM), що базується на зміні поведінкових патернів, а не лише на пасивному інформуванні співробітників [32].

Методологічним фундаментом для успішної трансформації культури безпеки виступає модель BMAP (Behavior, Motivation, Ability, Prompt). Згідно з цією концепцією, цільова дія (безпечна поведінка) відбувається лише тоді, коли три ключові компоненти — мотивація, здатність та підказка — збігаються в часі [33].

Перший компонент, мотивація (Motivation), передбачає відмову від політики залякування на користь створення позитивних стимулів. Для цього широко застосовуються механізми гейміфікації, такі як нарахування балів, присвоєння значків та формування лідербордів. Психологічна мета полягає в тому, щоб працівники відчували себе "героями безпеки", які захищають організацію, а не потенційними злочинцями чи джерелом проблем [34].

Другий компонент, здатність (Ability), фокусується на усуненні бар'єрів для виконання правил безпеки. Це досягається шляхом максимального спрощення безпечних дій. Технічна реалізація цього принципу включає впровадження корпоративних менеджерів паролів та рішень єдиного входу (SSO), що робить дотримання суворої парольної політики легким та необтяжливим для користувача .

Третій компонент, підказка (Prompt), забезпечує своєчасні тригери для активації необхідної поведінки. Найбільшу ефективність тут демонструє підхід мікронавчання (just-in-time training), яке активується контекстуально — безпосередньо після того, як користувач зробив помилку, наприклад, клікнув на посилання у симульованій фішинговій атаці [35]. Такий підхід гарантує, що навчання відбувається саме в той момент, коли увага користувача максимально сфокусована на проблемі.

1.3. Нормативно-правові та стандартизовані вимоги до підвищення обізнаності співробітників

Процес розбудови стійкої національної системи кібербезпеки в Україні вступає у фазу глибокої інституційної трансформації. У центрі цієї трансформації знаходиться людський капітал, який, з одного боку, залишається найвразливішою ланкою в ланцюгу захисту інформації, а з іншого — виступає головним активним бар'єром проти складних кіберзагроз. Аналіз сучасного стану нормативно-правового регулювання свідчить про перехід від декларативних рекомендацій до жорсткої регламентації процесів підвищення обізнаності та навчання персоналу.

Фундамент державної політики у сфері кібербезпеки закладено Законом України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII. Цей акт не лише визначив правові та організаційні основи захисту національних інтересів у кіберпросторі, а й заклав механізм координації діяльності державних органів. Проте тривалий час вимоги до навчання персоналу мали розпорошений характер. Ситуація докорінно змінилася з ухваленням Закону № 4336-IX від 27 березня 2025 року, який запровадив обов'язкове та систематичне навчання з кібергігієни.

Законодавець чітко розмежував сфери відповідальності. Кабінет Міністрів України через Національний координаційний центр кібербезпеки (НКЦК) та спеціалізовані органи, такі як Держспецзв'язку, формує єдині стандарти підготовки кадрів. Основною метою нових регуляцій є перехід до моделі «кіберстійкість через обізнаність», де кожен державний службовець та працівник об'єкта критичної інфраструктури розглядається як суб'єкт забезпечення кібербезпеки [36].

Закон України «Про захист персональних даних» № 2297-VI встановлює суворі вимоги до персоналу, який має доступ до конфіденційної інформації. Згідно зі статтею 24, володільці та розпорядники баз персональних даних зобов'язані забезпечити їх захист від незаконної обробки та випадкових втрат.

Це передбачає не лише технічні заходи, а й організаційну роботу, центральним елементом якої є навчання співробітників.

Важливим аспектом є правовий статус працівників. Використання персональних даних має здійснюватися лише відповідно до їхніх професійних, службових чи трудових обов'язків [37]. У кожній організації, незалежно від форми власності, має бути визначено відповідальну особу або підрозділ, що організовує роботу із захисту даних. Це створює ієрархічну систему контролю, де відповідальна особа забезпечує інформування персоналу про принципи обробки, такі як обмеження мети, мінімізація даних та обмеження зберігання.

Працівники, допущені до обробки даних, зобов'язані надати письмове зобов'язання про нерозголошення. Це зобов'язання має безстроковий характер і діє після припинення трудових відносин. В освітніх та медичних закладах, де обробляються особливо чутливі дані (стан здоров'я, успішність), вимоги до обізнаності деталізуються у внутрішніх положеннях, які розробляються на базі Закону № 2297-VI.

Побудова ефективної системи захисту інформації вимагає, щоб навчання персоналу базувалося не лише на технічних інструкціях, а й на глибокому розумінні фундаментальних принципів, закладених у чинному законодавстві. Першочерговим аспектом, який має бути інтегрований у навчальні програми, є забезпечення прозорості та законності обробки даних. Це означає, що кожен працівник, допущений до роботи з конфіденційною інформацією, повинен чітко усвідомлювати правові підстави для збору даних, а також володіти алгоритмами належного інформування суб'єкта даних про його права та механізми їх реалізації [38].

Критично важливим елементом формування культури приватності є імперативне дотримання принципу обмеження мети. У процесі професійної підготовки необхідно сформувати у співробітників чітке розуміння того, що інформація, акумульована для досягнення однієї конкретної цілі (наприклад, для забезпечення трудових правовідносин), за жодних обставин не може бути використана для інших потреб, зокрема маркетингових досліджень чи

комерційних розсилок, без отримання додаткової верифікованої згоди від суб’єкта даних. Порушення цього принципу часто стає причиною юридичних конфліктів та репутаційних втрат організації.

Окрім цього, навчальні заходи повинні бути спрямовані на розвиток практичних навичок щодо дотримання принципів мінімізації та точності даних. Персонал зобов'язаний вміти оперувати виключно тим обсягом інформації, який є критично необхідним для виконання поточних завдань, уникаючи надмірного накопичення даних. Водночас, важливим компонентом є розуміння обов’язку щодо своєчасної актуалізації інформації або її безповоротного знищення у випадках, коли виявляється її неточність або втрата релевантності [38].

З огляду на те, що об’єкти критичної інфраструктури (ОКІ) є пріоритетними цілями для кібератак, державне регулювання їхньої безпеки вирізняється найвищим ступенем деталізації та імперативності. Фундаментом національної системи вимог у цій сфері виступає Постанова Кабінету Міністрів України від 19 червня 2019 року № 518, яка затвердила «Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури». Цей документ визначає навчання та підвищення обізнаності персоналу не як рекомендаційний, а як базовий і обов’язковий організаційний захід. Згідно з пунктами 8 та 9 зазначених Вимог, оператори ОКІ зобов’язані забезпечувати регулярність навчального процесу, який має будуватися на принципі диференціації. Це означає відмову від уніфікованих курсів на користь адаптивних програм, що враховують функціональні обов’язки та рівень доступу працівника до інформаційних систем. На практиці це вимагає розробки принципово відмінних навчальних треків для різних ролей, наприклад, системних адміністраторів та офіс-менеджерів, хоча базовий рівень кібергігієни залишається обов'язковим для всього персоналу.

Найбільш показовим прикладом імплементації цих вимог є енергетичний сектор, де положення деталізовані Наказом Міністерства енергетики № 417 від 15.12.2022. Документ впроваджує категорію заходів PR.AT (Awareness and

Training), яка структурує вимоги за п’ятьма ієрархічними рівнями, охоплюючи всі ланки управління підприємством(зображено на рис. 1.4) [39].

Базовий рівень, PR.AT-1 (Загальна обізнаність), стосується абсолютно всіх працівників об'єкта та вимагає наявності затвердженого плану дій і постійного моніторингу успішності проходження курсів. Спеціалізований рівень PR.AT-2 (Привілейовані користувачі) фокусується на адміністраторах із правами розширеного доступу, які через критичність своїх ролей повинні проходити поглиблене технічне навчання. Комплексний підхід до безпеки виходить за межі штатного персоналу, що відображено у вимозі PR.AT-3 (Обізнаність партнерів). Цей рівень зобов'язує поширювати стандарти обізнаності на контрагентів та підрядників, які мають доступ до інформаційних систем оператора, мінімізуючи ризики атак через ланцюг постачання.

Окремий акцент робиться на управлінській ланці: рівень PR.AT-4 (Керівництво) вимагає, щоб топ-менеджмент чітко усвідомлював свою роль у стратегічному плануванні та забезпеченні ресурсами для кіберзахисту. Замикає цю структуру рівень PR.AT-5 (Персонал з безпеки), який передбачає безперервне підвищення кваліфікації фахівців профільних підрозділів та чітке розуміння ними своїх повноважень у разі виникнення інцидентів.

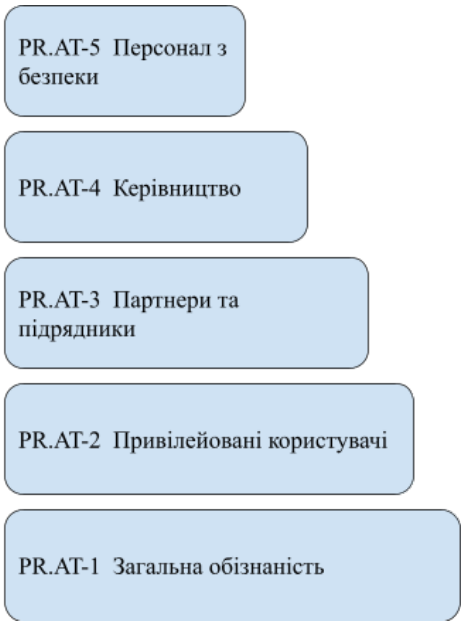

Рис. 1.4. Ієрархія рівнів заходів PR.AT для об’єктів критичної інфраструктури

Варто також зазначити, що регулювання торкається не лише змісту, а й форми проведення навчальних заходів. Для забезпечення ефективності навчання у дистанційному форматі та верифікації присутності встановлюються чіткі технічні вимоги до робочого місця учасника: обов’язкова наявність увімкненої камери, мікрофону та забезпечення швидкості інтернет-з'єднання не менше 20 Мбіт/с, що гарантує повноцінну інтерактивну взаємодію під час тренінгів [40].

Банківський сектор традиційно виступає об’єктом посиленої уваги з боку регулятора через критичну важливість фінансових даних та високі ризики шахрайства. Національний банк України вибудовує систему кіберзахисту на принципах пропорційності та адекватності заходам реальним загрозам. Фундаментальним нормативним актом у цій сфері є Постанова Правління НБУ № 95 від 28.09.2017, яка встановлює імперативний обов’язок банківських установ розробляти та впроваджувати комплексну Політику інформаційної безпеки. У цьому документі організація практичних заходів щодо безперервного навчання та підвищення обізнаності персоналу визначається як один із стратегічних пунктів забезпечення операційної стійкості фінансової установи [41].

Згідно з регуляторними вимогами, навчання працівників банку має охоплювати специфічні вектори атак, що показано на рис. 1.5:

- захист від зловмисного коду (malware);
- безпека при використанні електронної пошти (боротьба з фішингом);
- контроль доступу до банківських інформаційних систем;
- криптографічний захист інформації.

Рис. 1.5. Вектори атак, що повинне охоплювати навчання працівників банків

Важливою особливістю банківського регулювання є перехід від формального проведення інструктажів до вимоги постійного моніторингу ефективності функціонування СУІБ. Цей процес включає аналітичну оцінку того, наскільки навчання персоналу реально знижує кількість інцидентів та мінімізує вразливості, пов'язані з людським фактором. Для технічної реалізації цього завдання банки часто використовують спеціалізовані LMS-платформи, що надає можливість для індивідуалізації навчальних траєкторій кожного співробітника залежно від його доступу до активів. Такий підхід дозволяє фінансовим установам виконувати вимоги національного стандарту ДСТУ ISO/IEC 27001, який є методичною основою для побудови СУІБ у банківському секторі України [42].

Уніфікованим методологічним базисом для побудови системи обізнаності в Україні виступає національний стандарт ДСТУ ISO/IEC 27001:2023, який є ідентичним міжнародному стандарту ISO/IEC 27001:2022. Цей документ визначає не лише технічні параметри захисту, а й організаційні вимоги до людського капіталу. Ключовим елементом стандарту є розділ 7.3 «Обізнаність» (Awareness), виконання якого є обов’язковим для успішної сертифікації системи управління. Цей розділ імперативно вимагає, щоб усі особи, які працюють під контролем організації (включаючи штатний персонал, підрядників та волонтерів), знали про:

- політику інформаційної безпеки організації;
- свій внесок у результативність СУІБ;
- наслідки порушення вимог СУІБ.

Практична імплементація цих вимог вимагає створення чітких механізмів реалізації та доказової бази. Для забезпечення розуміння політик безпеки недостатньо формального ознайомлення; процес має включати регулярні інформаційні розсилки, тематичні семінари та процедури онбордингу для нових співробітників. Доказом відповідності у цьому випадку виступають особисті

підписи про ознайомлення або, що більш актуально для цифрового середовища, цифрові записи (логи) в системах дистанційного навчання (LMS).

Усвідомлення персоналом своєї ролі в СУІБ досягається шляхом впровадження рольових сценаріїв та практичних вправ, специфічних для конкретних посад. Валідація результативності цього напрямку здійснюється через аналіз звітів про проведені імітаційні атаки, зокрема фішинг-тести, які демонструють реальну здатність персоналу протидіяти загрозам. Щодо інформування про наслідки порушень, навчальні матеріали мають містити не лише абстрактні попередження, а й деталізовані кейси відповідальності, включаючи опис конкретних дисциплінарних та юридичних санкцій.

Окрему увагу стандарт приділяє компетентності фахівців. Згідно з Додатком А (контроль 6.3), організація повинна забезпечити не просто «навчання», а «освіту та тренінг», що передбачає регулярне оновлення знань відповідно до змін у ландшафті загроз. Для ключових фахівців це передбачає проходження спеціалізованих тренінгів (наприклад, обсягом 24 академічні години). Організації зобов'язані зберігати документовану інформацію як доказ компетентності працівників, якою можуть слугувати сертифікати, дипломи або протоколи результатів складання кваліфікаційних іспитів [43, 44].

Адміністрація Державної служби спеціального зв’язку та захисту інформації України (Держспецзв’язку) виступає ключовим суб’єктом, що визначає стратегічний вектор навчання та підвищення обізнаності персоналу в державному секторі. Важливим кроком до уніфікації освітніх стандартів стало прийняття Наказу № 661 від 21.10.2025, яким було затверджено «Методичні рекомендації щодо проведення інструктажів і тренінгів з кібергігієни». Цей документ спрямований на докорінну зміну підходів до організації навчання: перехід від ситуативних заходів до побудови системного, контрольованого та методично обґрунтованого процесу підвищення кваліфікації державних службовців.

Інституційна спроможність регулятора була суттєво посилена на законодавчому рівні. Закон № 4336-IX значно розширив повноваження Держспецзв’язку, надавши право здійснювати перевірку фактичного дотримання норм щодо навчання персоналу в рамках загального аудиту стану кіберзахисту державних органів. Такий механізм державного нагляду створює імперативні стимули для керівників установ відмовлятися від практики формальних звітів на користь забезпечення реальної підготовки кадрів. Змістовна частина базового курсу з кібергігієни, відповідно до рекомендацій, має фокусуватися на критично важливих навичках: використанні багатофакторної автентифікації (MFA), забезпеченні захисту облікових записів від компрометації та здатності розпізнавати маніпулятивний контент у цифровому середовищі.

Окремий акцент у регуляторній рамці зроблено на інтеграції людського капіталу в систему управління ризиками. Затверджена Держспецзв’язку Методика оцінювання ризиків кібербезпеки передбачає, що людський фактор (рівень обізнаності, схильність до помилок) має обов'язково враховуватися як вагомий параметр при визначенні ймовірності виникнення інциденту. Крім того, для підтримання високого рівня готовності, актуальна інформація про стан кібербезпеки та нові загрози повинна регулярно циркулювати та передаватися по всьому об’єкту кіберзахисту, що є необхідною умовою для забезпечення злагодженого та своєчасного реагування на інциденти.

Забезпечення якості навчання персоналу вимагає високого рівня кваліфікації самих викладачів та тренерів. Для осіб, чия професійна діяльність безпосередньо пов’язана з навчанням інших у цій сфері, розроблено та затверджено професійний стандарт «Провідний інструктор-методист з інформаційної безпеки та кібербезпеки». Цей документ формалізує вимоги до профілю компетенцій фахівця, який повинен виступати не лише носієм технічних знань, а й педагогом та ментором. Згідно зі стандартом, такий фахівець повинен володіти розвиненими загальними компетентностями, зокрема здатністю діяти соціально відповідально, враховуючи етичні аспекти професії,

та ефективно застосовувати теоретичні знання у складних практичних ситуаціях для вирішення нестандартних завдань.

Окремою ланкою в системі освіти є курси підвищення кваліфікації та спеціалізована підготовка з менеджменту інформаційної безпеки. Типові програми такого спрямування, як правило, розраховані на 24 академічні години інтенсивного навчання. Їх змістовне наповнення включає детальне вивчення вимог міжнародного стандарту ДСТУ ISO/IEC 27001, опанування сучасних методів ідентифікації та оцінювання ризиків, а також, що критично важливо для роботи з персоналом, — розгляд психологічних аспектів безпеки. Зокрема, програми інтегрують вивчення класичних теорій мотивації (наприклад, піраміди потреб Маслоу або двофакторної теорії Херсберга), що дозволяє менеджерам з безпеки знаходити ефективні важелі для кращого залучення персоналу до процесів захисту інформації та формування стійкої культури кібербезпеки.

Фундаментальна підготовка кадрів здійснюється в системі вищої освіти України. Навчання бакалаврів за спеціальністю 125 «Кібербезпека» регламентується державними стандартами, які передбачають отримання здобувачами 240 кредитів ECTS протягом майже 4 років навчання. Освітня програма будується на поєднанні обов’язкових та вибіркових компонентів, що дозволяє формувати гнучкі індивідуальні траєкторії навчання. Обов'язкові блоки включають такі фундаментальні дисципліни, як криптографія, архітектура комп'ютерних систем та мережева безпека, що забезпечує глибоку теоретичну та практичну базу для майбутніх фахівців, необхідну для розуміння природи кіберзагроз та методів протидії їм [45].

Аналіз нормативних вимог та стандартів дозволяє сформувати цілісну картину того, як має виглядати сучасна система підвищення обізнаності в Україні. Перехід від «безпеки як продукту» до «безпеки як процесу» вимагає від організацій зміщення фокусу на безперервне навчання.

Головними напрямками розвитку систем обізнаності є:

1. Систематизація навчання. Відхід від одноразових інструктажів до постійних циклів підготовки та перевірки знань.

2. Використання ризик-орієнтованого підходу. Програма навчання повинна адаптуватися під актуальні загрози, виявлені під час оцінки ризиків організації.

3. Автоматизація та моніторинг. Застосування LMS та інструментів імітації атак дозволяє отримати об’єктивні дані про рівень підготовки персоналу та вчасно коригувати навчальні плани.

4. Синхронізація з державними стандартами. Використання методичних рекомендацій Держспецзв’язку та вимог ISO 27001 гарантує не лише захищеність, а й відповідність регуляторним нормам, що критично для успішного проходження аудитів.

Впровадження Закону № 4336-IX та оновлених стандартів ДСТУ ISO/IEC 27001 у 2025 році створює в Україні нове регуляторне середовище, де інформаційна обізнаність стає невід’ємною частиною професійної придатності. Співробітники більше не є пасивними користувачами систем; вони стають активними учасниками процесу захисту, що є єдиним ефективним способом протидії сучасним гібридним кіберзагрозам. Подальший розвиток галузі залежатиме від здатності організацій інтегрувати ці вимоги у свою корпоративну культуру, роблячи кібергігієну природною складовою щоденної професійної діяльності.

Висновки до розділу 1

У першому розділі проведено комплексний аналіз сучасного стану соціоінженерних атак та визначено роль людського фактору в системі управління інформаційною безпекою (СУІБ) організації.

Досліджено поняття та сутність соціальної інженерії, яка в умовах 2024–2025 років еволюціонувала від масових розсилок до високоточних персоналізованих впливів. Встановлено, що соціальна інженерія є специфічним класом загроз,

спрямованим на експлуатацію когнітивних механізмів людини. Деталізовано характеристики соціального інженера як суб'єкта загрози та систематизовано ключові психологічні принципи, на яких базуються атаки: дефіцит, авторитет, взаємність та соціальний доказ. Проаналізовано спектр деструктивних наслідків — від прямих фінансових втрат до компрометації критичної IT-інфраструктури.

Особливу увагу приділено трансформації ландшафту загроз під впливом генеративного штучного інтелекту. Визначено, що використання технологій GenAI (LLM, дипфейки, автономні агенти) дозволяє зловмисникам автоматизувати створення бездоганного фішингового контенту та імітувати біометричні характеристики особи (голос, відео), що нівелює ефективність традиційних методів захисту.

З'ясовано роль людського фактору як центрального елемента інформаційних систем. Класифіковано інсайдерські загрози на зловмисні, ненавмисні та індуковані, де остання категорія набула особливої гостроти через можливість шантажу за допомогою дипфейків. Доведено, що традиційний підхід до навчання персоналу є недостатнім, що зумовлює необхідність переходу до концепції управління людськими ризиками (HRM) та формування стійкої культури кібербезпеки за моделлю BMAP.

Здійснено огляд нормативно-правової бази, зокрема Законів України «Про основні засади забезпечення кібербезпеки України» та «Про захист персональних даних», а також нових вимог 2025 року щодо обов'язкового навчання з кібергігієни. Проаналізовано галузеві стандарти для об'єктів критичної інфраструктури (рівні PR.AT) та банківського сектору, а також методологічний базис ДСТУ ISO/IEC 27001:2023.

Таким чином, результати першого розділу підтверджують, що в умовах стрімкого технологічного розвитку персонал залишається критичною вразливістю, а ефективна протидія загрозам вимагає впровадження системних, ризик-орієнтованих програм підготовки, що базуються на актуальних нормативних вимогах та психологічних аспектах поведінки користувачів.

РОЗДІЛ 2
АНАЛІЗ ІСНУЮЧИХ ПІДХОДІВ ТА ЗАСОБІВ ОЦІНЮВАННЯ ОБІЗНАНОСТІ ПЕРСОНАЛУ

2.1. Огляд сучасних платформ та інструментів для навчання і тестування персоналу

В умовах Четвертої промислової революції та стрімкого розвитку інформаційного суспільства питання кібербезпеки набувають критичного значення. Складні екосистеми, що включають Інтернет речей (IoT), хмарні технології та взаємопов’язані мережі, створюють поверхню атаки, яка постійно розширюється. У цьому контексті людина часто розглядається як «найслабша ланка» в системі захисту, що робить професійне навчання необхідністю не лише для технічного персоналу, але й для широкого кола користувачів. Ринок навчання та підвищення обізнаності з питань кібербезпеки демонструє значне зростання, що підтверджується прогнозами провідних аналітичних агентств, таких як Gartner [46].

На сьогоднішній день існує широкий спектр інструментальних засобів для навчання — від традиційних академічних курсів до спеціалізованих платформ, що використовують віртуальні лабораторії та кіберполігони (cyber-ranges). Аналіз існуючих рішень дозволяє класифікувати їх за рівнем інтерактивності, адаптивності та використаними педагогічними методиками.

Перший рівень інструментів представлений платформами масових відкритих онлайн-курсів, такими як Coursera, Udacity та edX. Вони пропонують вступні та базові курси з кібербезпеки, проте часто обмежуються теоретичним викладом матеріалу та не забезпечують достатньої практичної взаємодії з реальними системами.

Більш просунутий рівень навчання пропонують спеціалізовані платформи, орієнтовані на професійний розвиток у сфері інформаційної безпеки. До них

належать рішення від SANS, CyberInternAcademy, StationX, Cybrary та AwareGO. Зазначені платформи підтримують більш поглиблене та цілеспрямоване навчання, спрямоване на розвиток конкретних навичок. Однак, їхнім суттєвим недоліком є обмежена можливість надання практичного досвіду роботи в умовах реальних інцидентів або на повнофункціональних кіберполігонах. У більшості випадків ці рішення орієнтовані на індивідуальних користувачів і не завжди враховують специфіку корпоративних систем або рівень початкової підготовки конкретного співробітника.

Найбільш ефективним інструментом для підготовки персоналу до протидії соціоінженерним та технічним атакам є сучасні платформи кіберполігонів. Такі рішення, як BeOne, ISACA CyberSecurity Nexus (CSX), Kaspersky Security Awareness та CyberBit, пропонують розширені функціональні можливості. Вони дозволяють моделювати реалістичні сценарії атак, надаючи користувачам можливість відпрацьовувати навички захисту в безпечному середовищі.

Проте, навіть провідні комерційні платформи часто мають обмежену гнучкість у плані адаптації навчального процесу. Більшість навчальних програм розробляється технічними фахівцями, які не завжди враховують педагогічні принципи навчання дорослих, такі як таксономія Блума або цикл навчання Колба. Це створює розрив між технічним змістом курсу та здатністю співробітника ефективно засвоїти матеріал і застосувати його на практиці.

Перспективним напрямком розвитку інструментів навчання є поєднання серйозних ігор (serious gaming), емуляції, симуляції та безперервного оцінювання безпеки. Прикладом такого комплексного підходу є платформа THREAT-ARREST. Особливістю даної системи є використання методології моделювання CTTP (Cyber Threat and Training Preparation), яка визначає навчальні цілі, траєкторію навчання користувача, а також керує створенням віртуальних лабораторій на вимогу[47].

Сучасні інструменти навчання повинні підтримувати використання засобів тестування безпеки, моніторингу та оцінювання на різних рівнях реалізації системи(рис. 2.1):

1. Мережевий рівень - інструменти виявлення вторгнень (IDS), брандмауери, honeypots.
2. Інфраструктурний рівень - монітори безпеки, інструменти пасивного та активного тестування на проникнення (наприклад, перевірка конфігурації, SSL/TLS).
3. Прикладний рівень - аналіз коду, тестування автентифікації, перевірка валідації даних та стійкості до ін'єкцій.

Рис. 2.1. Рівні реалізації системи сучасного інструменту навчання

Важливим елементом ефективної платформи є попередній аналіз системи організації. Наприклад, інструмент Assurance Tool дозволяє оцінити поточний рівень безпеки та виявити найбільш значущі проблеми, які повинні лягти в

основу навчального процесу. Це дозволяє створювати гібридні навчальні програми, адаптовані до потреб конкретної організації та типів стажерів.

Використання гейміфікації (серйозних ігор) у навчальних платформах позитивно впливає на процес засвоєння знань. Дослідження показують, що ігрові методики дозволяють користувачам ознайомитися зі складними темами, такими як соціальна інженерія, у більш невимушеній атмосфері. Наприклад, гра PROTECT використовує карткову механіку для навчання методам захисту від фішингу та інших соціоінженерних атак. Інші підходи, такі як HATCH, також демонструють ефективність у навчанні протидії маніпуляціям.

Сучасні платформи комбінують емуляцію (відтворення реальних систем) та симуляцію (моделювання поведінки окремих компонентів). Це дозволяє створювати реалістичні сценарії, де співробітники можуть взаємодіяти з цифровими двійниками своїх робочих систем, не ризикуючи порушити роботу реальної інфраструктури.

Ринок платформ для навчання персоналу (Security Awareness & Training) характеризується високим рівнем конкуренції та технологічної спеціалізації. У сегменті корпоративних рішень для управління ризиками людського фактору домінуючі позиції займають комплексні системи, що поєднують теоретичну підготовку з практичними симуляціями атак.

Серед лідерів ринку особливе місце посідає платформа KnowBe4, яка станом на 2025 рік утримує значну частку ринку завдяки інтегрованому підходу до навчання та симуляції соціальної інженерії. Методологічною основою платформи виступає перевірена методика чотирьох кроків, що включає базову оцінку вразливості персоналу (baseline testing), надання структурованого навчального матеріалу, безперервне тестування через імітаційні атаки та детальний аналіз результатів. Функціонал платформи дозволяє використовувати групи «Smart Groups» для автоматизації призначення курсів залежно від поведінки користувача. Крім того, її контентна бібліотека визнана найбільшою в

індустрії, пропонуючи матеріали на більш ніж 34 мовах, що є критичним фактором для глобальних корпорацій з розподіленими офісами.

Іншим значущим гравцем є компанія Proofpoint, яка реалізує стратегію екосистемного захисту. Їхнє рішення (зокрема модуль ZenGuide) глибоко інтегроване з технічними засобами захисту електронної пошти та шлюзами безпеки. Така архітектура дозволяє створювати персоналізовані навчальні шляхи на основі реальних атак, які блокуються на периметрі організації, забезпечуючи високу контекстуальну релевантність навчання та фокусуючись на зміні поведінки.

Платформа Hoxhunt, у свою чергу, робить ставку на поведінкову науку, гейміфікацію та адаптивне навчання. Особливістю системи є те, що складність фішингових симуляцій автоматично коригується в реальному часі відповідно до індивідуального рівня знань та історії попередніх помилок користувача, що дозволяє реалізовувати ефективні мікротренінги без перевантаження персоналу.

Окрім зазначених лідерів, на ринку представлені спеціалізовані рішення, що використовують унікальні методики впливу. Наприклад, Infosec IQ фокусується на рольовому навчанні з можливістю глибокої персоналізації під корпоративну культуру. Платформи NINJIO та SoSafe використовують методи психологічного сторітелінгу та поведінкової психології для підвищення залученості. Окремий сегмент формують рішення нового покоління, такі як Adaptive Security, що інтегрують технології штучного інтелекту для симуляції діпфейк-атак та OSINT-аналізу, готуючи персонал до протидії новітнім векторам загроз.

Детальний порівняльний аналіз функціональних можливостей провідних платформ наведено в таблиці 2.1.

Таблиця 2.1

Порівняння провідних платформ для навчання персоналу

Назва платформи	Основна спеціалізація	Ключовий функціонал
KnowBe4	Масове навчання та фішинг	Smart Groups, ШІ-рекомендації, дипфейк-тренінги
Proofpoint	Екосистемний захист пошти	Інтеграція з безпекою шлюзів, поведінкові зміни
Infosec IQ	Рольове навчання	Понад 2000 ресурсів, персоналізація під культуру
Hoxhunt	Людський ризик-менеджмент	Гейміфіковані мікро-тренінги, ШІ-персоналізація
NINJIO	Психологічний сторітелінг	Анімовані епізоди, алгоритм оцінки ризику
SoSafe	Поведінкова психологія	Навчання в момент ризику, предиктивна аналітика
Adaptive Security	ШІ-захист нового покоління	Симуляція дипфейків, OSINT-аналіз, ШІ-контент

Окрім комплексних корпоративних платформ, на ринку присутній сегмент вузькоспеціалізованих рішень, які фокусуються на поглибленому опрацюванні конкретних векторів загроз. Такий підхід дозволяє організаціям закривати специфічні прогалини у безпеці, не переплачуючи за зайвий функціонал. Яскравим прикладом є платформа Cofense PhishMe, яка орієнтована на розвиток навичок ідентифікації фішингу через концепцію «колективного інтелекту» користувачів. Методологія платформи передбачає, що кожне повідомлення співробітника про підозрілий лист аналізується та використовується для посилення загального периметру захисту організації, перетворюючи персонал на активних сенсорів безпеки.

Для організацій з високим рівнем зрілості процесів кібербезпеки (CMMI Level 4-5) доцільним є використання ресурсів рівня SANS Security Awareness. Курси цієї платформи розробляються провідними світовими експертами-практиками, що гарантує актуальність матеріалів щодо найновіших тактик зловмисників (TTPs), хоча вартість впровадження може бути бар’єром для малого бізнесу. Натомість, для сегменту малого та середнього бізнесу існують

доступніші, але ефективні рішення, такі як PhishingBox або ESET Cybersecurity Awareness Training. Вони надають базовий, але достатній інструментарій для тестування та навчання персоналу за помірну ціну, забезпечуючи виконання нормативних вимог.

Однак для технічного персоналу, системних адміністраторів та фахівців з інформаційної безпеки стандартного навчання з обізнаності (Awareness) критично недостатньо. Ця категорія співробітників потребує спеціалізованих середовищ — технічних тренажерів та віртуальних лабораторій (Hands-on Labs), де можливо безпечно відпрацьовувати практичні навички захисту, форензіки та реагування на інциденти без ризику для продуктивної інфраструктури.

У сегменті технічної підготовки домінують рішення, що надають доступ до браузерних віртуальних машин та симуляцій реальних мережевих інфраструктур. Найбільш відомими платформами, які активно використовуються корпоративним сектором для апскіллінгу (upskilling) технічних команд, є Hack The Box та TryHackMe. Ці ресурси дозволяють моделювати сценарії проникнення та захисту різного рівня складності. Детальний порівняльний аналіз провідних технічних платформ за методологією та бізнес-функціями наведено у таблиці 2.2.

Таблиця 2.2

Порівняння провідних платформ для навчання персоналу

Платформа	**Методологія**	**Цільова аудиторія**	**Бізнес-функції**
TryHackMe	Керовані сценарії, покрокові лаби	Початківці та середній рівень	Дашборд менеджменту, відстеження ROI
Hack The Box	Challenge-based, відкриті світи	Досвідчені профі, Red Teams	Приватні CTF, Talent Sourcing
RangeForce	Симуляція Blue Team у реальних інструментах	SOC-аналітики, Incident Responders	Робота в Splunk, CrowdStrike, Gap-аналіз
Immersive Labs	CTI-driven практичне навчання	Розробники, інженери безпеки	Skills Analytics, відповідність MITRE
Cybrary	Відео-курси + віртуальні лаби	Широкий спектр IT-фахівців	Підготовка до сертифікацій (CISSP, CEH)

Вершиною еволюції навчальних систем є платформи типу RangeForce, які створюють повномасштабні «кіберполігони» (Cyber Ranges). Їхня унікальність полягає в тому, що команди захисту (Blue Teams) повинні відбивати атаки в реальному часі, використовуючи ті самі інструменти, що й у своєму робочому середовищі, наприклад, SIEM-системи Splunk або міжмережеві екрани Fortinet. Такий підхід дозволяє виявити не лише прогалини в технічних знаннях окремих співробітників, а й системні проблеми в комунікації та координації дій команди під час кризових ситуацій. Важливим елементом мотивації на таких платформах виступає гейміфікація через змагання типу Capture The Flag , які пропонують Hack The Box та TryHackMe. Це стимулює здорову конкуренцію та значно підвищує залученість фахівців до процесу безперервного навчання.

Аналіз ефективності впровадження автоматизованих систем навчання персоналу (Security Awareness Training) дозволяє стверджувати, що попри наявні виклики та ресурсні витрати, стратегічні переваги використання спеціалізованих інструментів суттєво переважають потенційні ризики. Це твердження стає особливо актуальним в умовах експоненційного зростання складності кіберзагроз та необхідності швидкої адаптації захисних механізмів організації.

Фундаментальною перевагою сучасних рішень є забезпечення масштабованості та стандартизації освітніх процесів. Використання хмарних архітектур дозволяє імплементувати єдиний, уніфікований стандарт знань для всіх співробітників компанії, незалежно від їхньої локації чи часового поясу. Такий підхід є критично важливим для великих транснаціональних підприємств, де традиційні методи ручного навчання тисяч людей є організаційно неможливими та економічно недоцільними. Крім того, високий рівень автоматизації адміністративних функцій радикально оптимізує управлінські ресурси: сучасні платформи дозволяють одному менеджеру з інформаційної безпеки ефективно координувати навчання для всієї організаційної структури, отримуючи деталізовані консолідовані звіти та аналітику в реальному часі одним кліком.

Критичним фактором для бізнесу є забезпечення відповідності регуляторним вимогам та комплаєнсу. Для низки стратегічних галузей, таких як фінансовий сектор, охорона здоров'я та державне управління, регулярне навчання персоналу трансформувалося з рекомендації в обов'язкову нормативну вимогу міжнародних стандартів, зокрема GDPR, HIPAA, PCI DSS та ISO 27001 [48]. Впровадження спеціалізованих платформ дозволяє автоматизувати процес документування прогресу навчання та результатів тестувань кожного співробітника. Це забезпечує організацію надійною доказовою базою (audit trail) для зовнішніх аудиторів та регуляторів, що значно спрощує та пришвидшує процедури проходження сертифікації та атестації систем захисту [49].

Ще однією ключовою перевагою є висока адаптивність до нових векторів загроз. Динаміка оновлення контенту на провідних платформах значно перевищує можливості внутрішніх відділів навчання, що дозволяє організаціям миттєво реагувати на появу нових типів атак. Показовим прикладом є ситуація 2024 року, коли було зафіксовано різке зростання кількості атак із використанням QR-кодів (так званий Quishing). Провідні вендори навчальних платформ продемонстрували здатність протягом лічених тижнів інтегрувати відповідні навчальні модулі та симуляційні сценарії у свої каталоги, забезпечивши клієнтів актуальними інструментами протидії новій загрозі.

Критичним аспектом сучасних інструментів є їх здатність до динамічної адаптації. Традиційні програми часто є статичними, тоді як передові рішення використовують моделі, що дозволяють змінювати складність завдань у реальному часі залежно від успішності користувача. Для цього використовуються педагогічні фреймворки, такі як таксономія Блума.

Таксономія Блума класифікує навчальні цілі за рівнями складності: від запам'ятовування та розуміння до аналізу, оцінювання та створення. Це дозволяє платформі автоматично підвищувати рівень складності сценаріїв. Наприклад, початківець може проходити сценарії на рівні «Запам'ятовування» (основи

криптографії), тоді як досвідчений користувач працюватиме на рівні «Оцінювання» (аналіз фішингових листів у емульованому середовищі).

Для моделювання загроз у навчальних сценаріях широко використовується методологія STRIDE [50]. Вона дозволяє систематизувати загрози за категоріями: Spoofing (спуфінг), Tampering (втручання), Repudiation (відмова від авторства), Information disclosure (розкриття інформації), Denial of Service (відмова в обслуговуванні) та Elevation of privilege (підвищення привілеїв). Інтеграція цієї моделі в навчальні платформи забезпечує покриття всіх ключових аспектів безпеки та дозволяє формувати чіткі метрики оцінювання ефективності навчання.

Ефективність платформи визначається не лише фактом проходження курсів, а й здатністю вимірювати реальні зміни в поведінці персоналу. Сучасні системи підтримують безперервний моніторинг та оцінювання після завершення навчання. Це включає перевірку журналів реальних систем (logs) для виявлення того, чи застосовують співробітники отримані знання (наприклад, чи стали вони частіше оновлювати паролі). Такий підхід базується на циклі навчання Колба, який передбачає проходження етапів конкретного досвіду, рефлексивного спостереження, абстрактної концептуалізації та активного експериментування.

Оцінювання в таких системах часто є багаторівневим і включає:

1. Кількісне (автоматизоване) оцінювання: бали за виконання вправ у віртуальних лабораторіях, правильні відповіді в іграх, час реакції на інцидент.
2. Якісне (ручне) оцінювання: аналіз дій тренером, результати опитувань та інтерв’ю.

Загальний бал ефективності навчання може розраховуватися за складними алгоритмами, що враховують вагу кожного компонента (гра, симуляція, тест) та рівень складності сценарію. Це дозволяє отримати об’єктивну картину готовності персоналу до протидії загрозам, зокрема соціоінженерного характеру.

Підсумовуючи огляд, слід зазначити, що майбутнє інструментів навчання лежить у площині повної інтеграції технічних засобів симуляції з передовими

педагогічними методиками та моделями адаптивного навчання. Використання таких платформ дозволяє перейти від формального проходження інструктажів до реального розвитку компетенцій, необхідних для захисту інформаційних активів в умовах постійно змінюваного ландшафту загроз.

2.2. Аналіз метрик та алгоритмів оцінювання ефективності навчання, що використовуються на практиці

В умовах зростання обсягів освітніх даних та необхідності переходу до проактивних стратегій управління кібербезпекою, критичного значення набуває вибір інструментарію для об’єктивного вимірювання результативності навчальних заходів. Традиційні методи оцінювання, що базуються на описовій статистиці або суб’єктивних опитуваннях, часто виявляються недостатніми для виявлення складних нелінійних залежностей між поведінкою співробітника під час навчання та його реальною стійкістю до соціоінженерних атак.

Сучасна парадигма оцінювання зміщується в бік використання предиктивної аналітики та методів ML. Як зазначають дослідники, еволюція підходів у цій сфері характеризується переходом від класичних статистичних моделей до складних ансамблевих методів та архітектур глибокого навчання, здатних обробляти багатовимірні та різнорідні дані.

В умовах цифрової трансформації освітніх процесів та необхідності підготовки персоналу до протидії складним соціоінженерним загрозам, підходи до оцінювання ефективності навчання зазнають суттєвих змін. Сучасна методологія виходить за межі простого тестування знань, інтегруючи широкий спектр педагогічних методологій (класичних рівневих моделей) та математичних алгоритмів, що базуються на аналізі даних (EDM) та психометриці [51]. Такий синтез дозволяє не лише констатувати факт завершення навчання, а й прогнозувати реальну поведінку співробітників у критичних ситуаціях.

Традиційним фундаментом для вимірювання результативності корпоративного навчання залишаються ієрархічні рамкові моделі. Вони забезпечують системний погляд на освітній процес, розглядаючи його як поетапну трансформацію інформації у бізнес-результат.

Найбільш авторитетною та поширеною у світовій практиці є Модель Дональда Кіркпатріка. Вона вважається стандартом де-факто в індустрії навчання та розвитку (L&D) і структурує оцінювання за чотирма послідовними рівнями. Перший рівень — реакція — вимірює суб'єктивну задоволеність учасників; другий — навчання — оцінює обсяг засвоєних знань; третій — поведінка — визначає, наскільки набуті навички застосовуються на робочому місці; четвертий — результати — аналізує кінцевий вплив на показники організації.

Попри те що модель була розроблена Дональдом Кіркпатріком ще у 1954 році в рамках його докторської дисертації, вона залишається базовим фреймворком для інструкційних дизайнерів та фахівців з кібербезпеки. Методологія передбачає, що ефективна оцінка освітньої програми можлива лише за умови послідовного проходження всіх чотирьох етапів, що зображені на рис. 2.2. Сучасні дослідники також пропонують модифікований підхід до використання цієї моделі: починати планування з четвертого рівня (результатів) і рухатися у зворотному напрямку до першого, що дозволяє краще узгодити навчання зі стратегічними цілями організації**.** Детальна характеристика рівнів моделі дозволяє зрозуміти механіку оцінювання на кожному етапі:

Рівень 1: Реакція (Reaction). На цьому етапі оцінюється ступінь залученості учасників та релевантність курсу їхнім очікуванням. Метою є отримання зворотного зв'язку щодо якості навчального матеріалу та організації процесу. Для вимірювання зазвичай використовуються опитування після завершення курсу (часто із застосуванням шкали Лайкерта), які дозволяють виявити сильні та слабкі сторони програми очима користувачів. У контексті електронного навчання (LMS) індикаторами

реакції також можуть слугувати показники завершення курсу (completion rates): низькі показники часто свідчать про низьку задоволеність контентом.

Рівень 2: Навчання (Learning). Другий рівень фокусується на вимірюванні успішності набуття нових знань, навичок або поведінкових патернів. Ключовим завданням є визначення того, чи зрозуміли співробітники матеріал і чи здатні вони його застосувати. Ефективними методами оцінювання тут виступають практичні завдання, постренінгові тести та інтерв'ю. Для підвищення об'єктивності рекомендується проводити попереднє тестування (pre-course quiz) для порівняння результатів з фінальним оцінюванням, що дозволяє кількісно виміряти приріст знань (delta).

Рівень 3: Поведінка та вплив (Behavior/Impact). Цей рівень вимірює, чи призвело навчання до реальної зміни поведінки співробітника на робочому місці. Це критично важливо, оскільки згідно з «кривою забування», нові знання можуть бути втрачені протягом 24 годин, якщо не будуть застосовані на практиці. Оцінювання поведінки дозволяє зрозуміти, наскільки успішно теоретичні знання трансформуються у практичні компетенції. Найбільш ефективним інструментом на цьому етапі вважається метод «360 градусів» (зворотний зв'язок від керівників, колег та підлеглих), а також моніторинг робочих метрик.

Рівень 4: Результати (Results). Вищий рівень оцінювання спрямований на ідентифікацію довгострокового впливу навчання на бізнес-показники. У контексті кібербезпеки це може бути зниження кількості інцидентів, спричинених людським фактором, або підвищення рівня відповідності стандартам безпеки. Вимірювання здійснюється через аналіз ключових показників ефективності (KPI), результатів опитувань співробітників та коефіцієнтів утримання персоналу. Це найбільш складний для вимірювання етап, проте саме він демонструє реальну цінність програми для бізнесу.

Аналіз застосування моделі Кіркпатріка дозволяє виділити як її переваги, так і суттєві обмеження. До сильних сторін відносять гнучкість, адаптивність до різних форматів навчання (онлайн, змішане, очне) та наявність чіткої структури.

Однак, модель піддається критиці за лінійність та значні часові витрати на реалізацію всіх чотирьох рівнів, що може бути проблематичним у динамічному корпоративному середовищі. Крім того, модель констатує факт ефективності або неефективності навчання, але не завжди надає діагностичні дані про причини невдач, що ускладнює процес внесення коректив у навчальну програму.

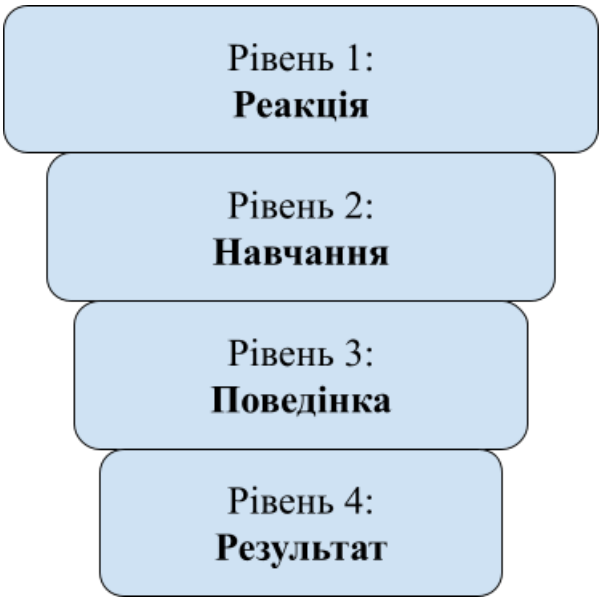

Рис. 2.2. 4 рівні моделі Кірпатріка

Логічним розвитком цього підходу стала Модель Джека Філліпса (ROI Methodology). Вона нівелює головний недолік моделі Кіркпатріка — відсутність фінансового виміру. Філліпс додав п’ятий рівень оцінювання (рис. 2.3), який фокусується на розрахунку коефіцієнта повернення інвестицій (Return on Investment). Це дозволяє транслювати якісні показники навчання у мову фінансів, порівнюючи вартість програми з грошовим еквівалентом отриманих вигод. У більш широкому організаційному контексті ця концепція визначається як методологія та процес для команд L&D та HR, що дозволяє пов'язати витрати на навчальні програми з їхніми фактичними результатами, що підкреслює її роль не лише як інструменту вимірювання, але і як процесу прийняття управлінських рішень. Структура моделі Філліпса розширює класичну ієрархію Кіркпатріка, додаючи глибини аналізу на кожному етапі та фіналізуючи процес економічним обґрунтуванням:

1. Рівень 1: Реакція (Reaction). На початковому етапі здійснюється збір даних щодо первинного сприйняття учасниками навчального контенту. Хоча цей рівень концептуально схожий з моделлю Кіркпатріка, у методології Філліпса акцент робиться на стратегічній відповідності: позитивні дані на цьому рівні розглядаються як індикатор узгодженості L&D стратегії (Learning and Development) з очікуваннями персоналу. Оцінювання проводиться за допомогою коротких опитувань, що дозволяє виявити потенційні бар'єри у сприйнятті матеріалу ще до початку його практичного застосування.

2. Рівень 2: Навчання (Learning). Цей етап передбачає об'єктивне вимірювання приросту знань, навичок або зміни установок. Для верифікації результатів використовуються стандартизовані інструменти: тести множинного вибору (MCQ), квізи та практичні симуляції, що проводяться до та після навчання (pre- and post-training assessment). Метою є підтвердження того, що навчальна інтервенція дійсно призвела до когнітивних змін у учасників.

3. Рівень 3: Застосування та впровадження (Application & Implementation). Ключова відмінність моделі Філліпса на цьому рівні полягає у фокусуванні не лише на факті застосування знань, а й на аналізі причин успіху або невдачі («WHY analysis»). Якщо модель Кіркпатріка лише констатує відсутність результату, то методологія Філліпса збирає якісний зворотний зв'язок для ідентифікації причинно-наслідкових зв'язків. Це дозволяє розрізнити ситуації, коли проблема полягає у неефективному навчанні, від випадків, коли бар'єром виступають зовнішні фактори (наприклад, некоректні вхідні дані або відсутність управлінської підтримки). Такий підхід перетворює оцінювання на інструмент діагностики бізнес-процесів.

4. Рівень 4: Вплив (Impact). На цьому рівні аналіз виходить за межі навчальної аудиторії та фокусується на багатовимірному впливі на бізнес-показники. Критично важливим елементом методології є техніка ізоляції ефекту навчання (isolation of training effects). Модель дозволяє відокремити вплив навчальної програми від інших факторів (наприклад, зовнішніх трендів,

маркетингових активностей або самоосвіти через відкриті джерела), що забезпечує чистоту даних для подальшого фінансового аналізу.

5. Рівень 5: Повернення інвестицій (ROI). Фінальний рівень, який є унікальним для даної методології, передбачає проведення аналізу «витрати-вигоди» (Cost-Benefit Analysis). Зібрані дані про вплив (Level 4) трансформуються у грошовий еквівалент, до якого додаються нематеріальні вигоди (intangible benefits). Отриманий результат зіставляється з повними витратами на проведення навчання. Це забезпечує менеджмент організації «твердими доказами» (hard evidence) ефективності інвестицій у людський капітал та дозволяє обґрунтувати бюджети на навчання перед стейкхолдерами.

Рис. 2.3. Рівні моделі Джека Філліпса

Для глибшого розуміння причинно-наслідкових зв'язків застосовується Метод успішного випадку Брінкергоффа (Success Case Method — SCM). На відміну від масових опитувань, цей підхід фокусується на якісному аналізі полярних груп — найбільш та найменш успішних прикладів застосування навчання.

Серед інших системних підходів варто виділити Модель Андерсона (Value of Learning), яка зміщує фокус з оцінки окремих тренінгів на узгодження цілей навчання зі стратегічними пріоритетами всієї організації. Також важливою є група моделей CIPP (Context, Input, Process, Product) та CIRO(Context, Input, Reaction, Outcome), які пропонують цілісний погляд на архітектуру навчання. Вони аналізують не лише результат, а й контекст, вхідні ресурси та сам процес реалізації програми. Модель CIRO розроблена для оцінювання управлінського навчання, робить акцент на контексті — аналізі потреб та цілей перед початком розробки програми. Вона ієрархічна: неможливо оцінити результат (Outcome), не проаналізувавши попередньо реакцію та вхідні ресурси [52]. Порівняння вище наведених моделей наведено у таблиці 2.3.

Таблиця 2.3

Порівняльна характеристика моделей оцінювання ефективності навчання

Модель	**Ключові рівні оцінювання**	**Основний фокус**	**Переваги для кібербезпеки**
Кіркпатрік	Чотирирівнева структура: Реакція, Навчання, Поведінка, Результати	Оцінка загальної ефективності та результативності навчального курсу	Висока простота впровадження та зрозуміла логічна структура процесу оцінювання
Філліпс	Розширення базової моделі додатковим рівнем 5: ROI (Return on Investment)	Вимірювання економічної вигоди та рентабельності інвестицій	Можливість надати фінансове обґрунтування бюджетів на навчання перед керівництвом
Кауфман	П'ять рівнів оцінки: Вхід, Процес, Мікро, Макро, Мега	Соціальний ефект та системний вплив на оточення	Глибокий аналіз якості навчальних матеріалів та оцінка зовнішніх ефектів
CIRO	Комплексний підхід: Контекст, Вхід, Реакція, Вихід	Спеціалізація на навчанні менеджменту та управлінських кадрів	Ефективний аналіз дефіциту ресурсів та потреб організації ще на етапі планування
Anderson	Оцінка стратегічного вирівнювання (Strategic alignment) з пріоритетами компанії	Досягнення цілей організації як головний критерій успіху	Забезпечення прямого та доказового зв’язку результатів навчання з бізнес-стратегією

Якщо педагогічні моделі надають загальну рамку оцінювання, то для глибокого аналізу та відстеження прогресу студентів у цифрових середовищах (наприклад, під час симуляцій фішингових атак) застосовують спеціалізовані математичні алгоритми. Вони дозволяють моделювати приховані процеси засвоєння знань.

Одним із найпоширеніших алгоритмів є Bayesian Knowledge Tracing (BKT). Цей метод базується на ймовірнісному підході та використовує приховані Марковські моделі (Hidden Markov Models — HMM). Алгоритм розглядає знання студента як прихований стан (освоїв/не освоїв), який неможливо спостерігати прямо, але можна оцінити на основі послідовності правильних чи неправильних відповідей.

Іншим фундаментальним підходом є Теорія відповіді на завдання (Item Response Theory — IRT). Це класична психометрична модель, що оцінює ефективність навчання через математичний взаємозв'язок між складністю тестового завдання та рівнем здібностей студента. Сучасні модифікації моделі (3PL, 4PL) дозволяють враховувати такі параметри, як ймовірність вгадування та випадкова помилка, що значно підвищує точність вимірювання.

З розвитком нейромережевих технологій набув поширення метод Deep Knowledge Tracing (DKT). Він застосовує рекурентні нейронні мережі (RNN) та мережі довгої короткострокової пам'яті (LSTM), що дозволяє моделювати складні нелінійні динаміки навчання. На відміну від BKT, цей метод здатний враховувати довгострокові залежності у великих масивах логів взаємодії та прогнозувати майбутні результати з вищою точністю.

Також варто згадати Performance Factor Analysis (PFA) — альтернативу BKT, що використовує логістичну регресію. Цей метод моделює здатність до навчання як динамічний параметр, який залежить від історії успішних та неуспішних спроб студента, дозволяючи адаптувати складність завдань у реальному часі.

Окрім моделювання знань, сучасні системи оцінювання використовують методи аналізу неструктурованих даних та поведінкових патернів.

Аналіз соціальних мереж (Social Network Analysis — SNA) дозволяє оцінити роль комунікації у навчанні. Цей метод вимірює інтегрованість студента в інформаційний обмін через метрики центральності, що часто корелює з успішністю навчання та лідерськими якостями в групі. Аналіз соціальних мереж не розглядає учнів ізольовано, а як вузли в графі, де зв'язки або ребра представляють взаємодії, такі як публікації на форумах, обмін контентом…

Застосування методів обробки природної мови (NLP) дозволяє автоматизувати оцінювання за Таксономією Блума. Сучасні алгоритми глибокого навчання, такі як BERT або RoBERTa, здатні автоматично класифікувати запитання та відповіді студентів за когнітивними рівнями (від простого запам’ятовування до створення нових концепцій). Це забезпечує об'єктивну оцінку глибини розуміння матеріалу без участі викладача. Експериментальні дані підтверджують ефективність цього підходу. Модель LSTM+BERT досягла максимальної точності класифікації 88,7% для класифікації екзаменаційних питань на основі переглянутих рівнів таксономії Блума».

Важливим джерелом даних є аналіз клікстрім-даних (Clickstream Analysis). Аналіз клікстрім-даних — це процес аналізу поведінки користувачів на веб-сайтах, у мобільних додатках та на інших цифрових платформах. Цей аналіз передбачає збір даних про взаємодію користувачів, таких як кліки, перегляди сторінок та інші дії, а також використання цих даних для отримання інформації про моделі поведінки користувачів [53]. Використання логів активності в системах управління навчанням (LMS) дозволяє виявляти приховані патерни залученості. Дослідження показують, що такі метрики, як час перегляду контенту, частота відвідування домашньої сторінки та динаміка проходження квізів, мають високу прогностичну цінність щодо фінального результату навчання.

Традиційні підходи до вимірювання ефективності навчання часто піддаються критиці через їхню статичність та нездатність відобразити реальну поведінку персоналу в динамічних умовах загроз. У сфері кібербезпеки розрив між теоретичними знаннями та практичними діями є критичним фактором ризику. Емпіричні дослідження підтверджують, що навіть співробітники, які нещодавно пройшли інструктаж, можуть ігнорувати загрози під впливом стресу, часового тиску або внаслідок когнітивних упереджень [54]. Це зумовлює необхідність трансформації систем оцінювання та впровадження нових рішень, орієнтованих на вимірювання практичної стійкості.

Одним із ключових індикаторів у сучасній практиці є показник схильності до фішингу (Phish-prone Percentage — PPP), що визначається як відсоток співробітників, які виконують небезпечні дії під час контрольованої симуляції атаки [55]. Глобальна статистика свідчить, що базовий рівень PPP до початку системного навчання становить приблизно 33,1%, що вказує на вразливість кожного третього працівника організації [56]. Проте, аналіз результатів показує, що покладання виключно на низький відсоток кліків не завжди гарантує успіх, оскільки це може свідчити про недостатню складність симуляцій або їх нерелевантність робочому контексту [57, 58].

Експертне середовище наголошує на необхідності інтеграції комплексних метрик поведінки. Зокрема, критично важливим є відстеження дій (Action Tracking), що дозволяє аналізувати поведінку користувача вже після переходу за посиланням — введення облікових даних, завантаження вкладень або ігнорування попереджень браузера. Не менш вагомим є коефіцієнт звітування (Reporting Rate): високий рівень цього показника (понад 60%) вважається маркером зрілої культури безпеки, де персонал діє як активний сенсор захисту [59]. Також критичним параметром є час звітування (Reporting Dwell Time) — часовий проміжок від отримання листа до повідомлення про нього, мінімізація якого дозволяє SOC-командам швидше нейтралізувати загрозу для всієї мережі.

Ефективність навчання вимірюється через операційні показники ефективності (KPI), які відображають професійну готовність до реагування на інциденти. Ці метрики дозволяють організаціям встановити кореляцію між проведенням технічних тренінгів (наприклад, на кіберполігонах) та підвищенням стійкості інфраструктури [60].Систематизація ключових метрик для технічних фахівців наведена в таблиці 2.4.

Таблиця 2.4

Операційні метрики оцінювання ефективності навчання технічного персоналу

Метрика	Опис	Ціль навчання
MTTD	Mean Time to Detect (Середній час виявлення)	Скорочення часу перебування зловмисника в мережі (Dwell Time)
MTTR	Mean Time to Respond (Середній час реагування)	Підвищення швидкості та якості процесу інцидент-менеджменту
MTTC	Mean Time to Contain (Середній час локалізації)	Мінімізація можливостей для латерального (горизонтального) переміщення атаки
Patch Latency	Час між виходом патча та його впровадженням	Зменшення вікна вразливості критичних систем

2.3. Порівняння та виявлення недоліків існуючих моделей оцінювання в умовах сучасних кіберзагроз

Історично склалося так, що більшість організацій імплементували процеси навчання з кібербезпеки, керуючись насамперед вимогами комплаєнсу (відповідності стандартам). Традиційні рішення, що базуються на періодичних лекціях, перегляді відеоматеріалів та підсумковому тестуванні, досі займають значну частку ринку.

Безумовною перевагою таких підходів є їхня організаційна зрозумілість. Легкість у розумінні для стейкхолдерів завдяки багаторічній практиці використання дозволяє швидко інтегрувати такі метрики у звіти для керівництва. Крім того, з економічної точки зору, ці методи характеризуються низькою вартістю впровадження, оскільки часто обмежуються використанням опитувань

та простих тестів множинного вибору, що не вимагають розгортання складної інфраструктури. З позиції регуляторних вимог, такі системи забезпечують чітку структуру для комплаєнс-аудитів, надаючи формальні докази компетентності персоналу, такі як наявність сертифікатів про завершення курсів або журнали відвідування інструктажів [61].

Однак, в умовах реального кіберпротиборства, недоліки традиційних моделей стають критичними вразливостями організації. Головною проблемою є низька валідність результатів оцінювання: успішне складання теоретичного тесту не гарантує безпечної поведінки співробітника в стресовій ситуації реальної атаки. Знання правил парольної політики не означає, що користувач не введе свій пароль на фішинговому сайті під тиском «термінового запиту від керівника».

Іншим суттєвим недоліком є статичність метрик. Традиційні моделі оцінювання фіксують зріз знань у конкретний момент часу, і ці метрики не відображають динаміку змін загроз у реальному часі. Зловмисники оновлюють тактики щотижня, тоді як перевірка знань може відбуватися раз на рік. Крім того, спостерігається відсутність контексту: результати тестів часто існують у вакуумі HR-звітів і відірвані від операційних показників SOC, таких як кількість реальних інцидентів або швидкість реагування на них. Це призводить до ситуації, коли організація має «на папері» навчений персонал, але на практиці залишається незахищеною.

Відповіддю на обмеження теоретичних тестів стало впровадження практико-орієнтованих інструментів — платформ імітації фішингу та кіберполігонів (Cyber Ranges). Цей клас рішень переносить фокус з перевірки пам'яті на перевірку навичок.

Ключовою перевагою симуляційних підходів є висока реалістичність, що сприяє формуванню «м'язової пам'яті» у захисників. Регулярне зіткнення з імітованими загрозами виробляє у співробітників автоматизм у розпізнаванні підозрілих ознак повідомлень. Для технічних команд кіберполігони надають

можливість оцінювати командну роботу, а не лише індивідуальні навички, що є критичним для злагодженого реагування на інциденти. Також важливим є те, що результати симуляцій мають пряму кореляцію з часовими метриками виявлення та реагування (MTTD/MTTR), дозволяючи виміряти реальний вплив навчання на безпеку периметра.

Проте і цей підхід не позбавлений системних недоліків. Впровадження повнофункціональних кіберполігонів або просунутих симуляційних платформ характеризується високою вартістю розгортання та підтримки актуальності сценаріїв [61]. Сценарії швидко застарівають, і їх адаптація вимагає значних ресурсів. Крім того, існує психологічний ризик «втоми від безпеки» (security fatigue) у співробітників через занадто часті перевірки. Надмірна інтенсивність симуляцій може призвести до того, що користувачі почнуть ігнорувати будь-які підозрілі повідомлення або сприймати їх як перешкоду роботі, а не як реальну загрозу.

Інтеграція технологій ШІ та ML у системи оцінювання відкрила нові можливості для персоналізації освітнього процесу. Системи класу «Smart Learning» обіцяють вирішити проблему статичності традиційних тестів.

Серед переваг таких рішень слід виділити гіпер-персоналізацію, що підвищує залученість та ефективність засвоєння матеріалу шляхом адаптації контенту під профіль ризику конкретного користувача . ШІ володіє здатністю обробляти величезні масиви даних з логів активності користувачів для виявлення прихованих ризиків та поведінкових аномалій, які неможливо помітити при ручному аналізі. Також критичною перевагою є автоматизація зворотного зв'язку в реальному часі (Just-in-time training), що дозволяє навчати співробітника безпосередньо в момент виникнення ризикованої ситуації [62].

Разом з тим, застосування ШІ породжує нові категорії ризиків та недоліків. Насамперед, це питання прозорості та інтерпретованості рішень («Black Box problem»): часто важко пояснити, чому модель прийняла саме таке рішення щодо присвоєння високого рівня ризику конкретному користувачу [63]. Це може викликати недовіру з боку персоналу та конфлікти.

Другою проблемою є упередженість алгоритмів (Algorithmic Bias). Якщо дані для навчання ШІ були зміщені (наприклад, базувалися на статистиці лише одного регіону або галузі), результати оцінювання будуть несправедливими по відношенню до певних груп співробітників. Нарешті, самі системи оцінювання стають об'єктом атак. Вразливість до атак на моделі ML, зокрема отруєння даних (Data poisoning), створює загрозу, коли зловмисники можуть маніпулювати системою навчання, щоб приховати свої дії або знизити поріг чутливості до атак [64].

Фундаментальною проблемою при проведенні агресивних симуляцій є явище емоційного втручання, відоме в нейропсихології як «Amygdala Hijack» (захоплення мигдалеподібного тіла). Дослідження показують, що різкий негативний зворотний зв'язок одразу після помилки (наприклад, червоний екран з повідомленням «Ви попалися на фішинг!») може викликати гостру стресову реакцію «бий або біжи», яка фізіологічно блокує когнітивні функції та здатність до навчання. У такому стані, замість конструктивного засвоєння уроку, співробітник відчуває сором, страх або гнів. Це не лише нівелює навчальний ефект, але й погіршує подальшу залученість співробітника у програму безпеки, формуючи захисні психологічні бар'єри. З огляду на це, найбільш ефективним визнається підхід «Teachable Moment».

Іншим суттєвим фактором, що спотворює результати оцінювання, є Ефект Готорна (Hawthorne effect). Його суть полягає в тому, що коли співробітники знають, що за ними спостерігають або що проводиться запланований тест, вони свідомо чи підсвідомо змінюють свою поведінку, діючи значно обережніше, ніж у звичайному житті. Це явище здатне критично спотворити валідність метрик симуляцій фішингу. Наприклад, поширеним сценарієм є ситуація, коли один пильний співробітник, ідентифікувавши навчальну атаку, попереджає колег у робочому месенджері («обережно, зараз йде розсилка від HR»). В результаті показник Reporting Rate штучно зростає, створюючи ілюзію високої захищеності, яка не відображає реального рівня індивідуальної обізнаності всієї групи за відсутності підказок.

Окремою загрозою для довгострокової ефективності навчання є феномен «втоми від безпеки» (Security Fatigue). У стані втоми співробітники починають ігнорувати навіть легітимні попередження систем безпеки, оскільки вони сприймаються мозком як «черговий тест» або прикра завада виконанню основних робочих обов'язків. Крайнім проявом цього стану є «вивчена безпорадність»: якщо тести сприймаються як занадто складні, маніпулятивні або нечесні, користувач припиняє робити будь-які спроби їх пройти, пасивно приймаючи роль «порушника». Результати узагальнення наведено у таблиці 2.5.

Таблиця 2.5

Матриця порівняльного аналізу підходів до оцінювання ефективності навчання

Критерій порівняння	**Традиційні методи (Тестування)**	**Симуляційні методи (Phishing/Ranges)**	**AI-рішення (Адаптивні)**	**Необхідний цільовий стан (Нова модель)**
Об'єкт оцінювання	Декларативні знання (що знає?)	Процедурні навички (що робить?)	Патерни поведінки (як діє?)	Комплексна стійкість (Knowledge + Behavior + Psychology)
Часова характеристика	Ретроспективна (пост-фактум)	Періодична (за розкладом)	Предиктивна (майбутнє)	Безперервна (Real-time monitoring)
Врахування контексту	Низьке (універсальні питання)	Середнє (шаблонні сценарії)	Високе (аналіз даних)	Контекстуально-залежне від бізнес-ролі та поточних загроз
Психологічний вплив	Нейтральний / Нудний	Високий стрес / Гейміфікація	Прихований вплив	Етично збалансований (мінімізація "Amygdala Hijack")
Основний недолік	Низька валідність у реальних умовах	Втома від безпеки та Ефект Готорна	"Black box" та упередженість	—

Підсумовуючи викладене, можна констатувати, що жоден із існуючих підходів у чистому вигляді не здатен забезпечити повноцінну верифікацію готовності персоналу до протидії сучасним соціоінженерним загрозам. Традиційні методи є занадто повільними та теоретичними; симуляційні підходи, хоч і більш ефективні, страждають від спотворень, викликаних психологічними факторами (ефект Готорна, стрес); а новітні AI-інструменти стикаються з проблемами прозорості та етики.

Висновки до розділу 2

У другому розділі проведено детальний аналіз сучасного інструментарію та методологічних підходів до навчання персоналу, а також систем оцінювання результативності освітніх заходів у сфері кібербезпеки.

Досліджено ландшафт сучасних платформ навчання, який класифіковано за рівнем інтерактивності: від загальноосвітніх онлайн-курсів (Coursera, edX) до спеціалізованих корпоративних систем (KnowBe4, Proofpoint, Hoxhunt) та високотехнологічних кіберполігонів (RangeForce, Hack The Box). Встановлено, що найбільш ефективними є рішення, які інтегрують педагогічні методики (таксономія Блума, цикл Колба) з технічними засобами симуляції та гейміфікації. Окремо виділено роль серйозних ігор та симуляцій у формуванні «м’язової пам’яті» користувачів при розпізнаванні соціоінженерних атак.

Проаналізовано методології та алгоритми оцінювання ефективності навчання. Розглянуто ієрархічні рамкові моделі (Д. Кіркпатріка та Дж. Філліпса), що дозволяють оцінювати процес від первинної реакції до розрахунку повернення інвестицій (ROI). Систематизовано математичні алгоритми моделювання знань, зокрема ймовірнісні методи (BKT), психометричні моделі (IRT) та новітні підходи на основі глибокого навчання (DKT), які забезпечують високу точність прогнозування успішності навчання.

Визначено специфічні метрики кібербезпеки, де акцент зміщується з формального проходження тестів на поведінкові показники: відсоток схильності до фішингу (PPP), коефіцієнт та час звітування про інциденти (Reporting Rate/Dwell Time). Для технічного персоналу ключовими ідентифіковано операційні метрики швидкості виявлення та локалізації загроз (MTTD, MTTR, MTTC).

Здійснено порівняльний аналіз підходів та виявлено їхні критичні недоліки в умовах сучасних загроз. Традиційні методи мають низьку валідність, оскільки теоретичні знання не гарантують безпечної поведінки у стресових ситуаціях. Симуляційні підходи та кіберполігони, попри реалістичність, провокують феномен «втоми від безпеки» (Security Fatigue) та спотворюються «ефектом Готорна» (зміна поведінки під наглядом). AI-рішення стикаються з проблемою «чорної скриньки» (непрозорість прийняття рішень) та потенційною упередженістю алгоритмів.

Узагальнення результатів розділу підтверджує наявність суттєвого розриву між існуючими статичними методами оцінювання та динамічною природою кіберзагроз. Це обґрунтовує необхідність розробки нової багатофакторної моделі (MBCR), яка б етично збалансовано поєднувала когнітивні, поведінкові та психологічні метрики в режимі реального часу, мінімізуючи негативний вплив стресових реакцій (Amygdala Hijack) на процес навчання.

РОЗДІЛ 3
РОЗРОБЛЕННЯ МОДЕЛІ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ НАВЧАННЯ СПІВРОБІТНИКІВ

Актуальність розробки моделі оцінювання ефективності навчання обумовлена необхідністю мінімізації ризиків, пов'язаних із людським фактором, який залишається критичною вразливістю в периметрі кіберзахисту сучасних організацій. В умовах еволюції методів соціальної інженерії традиційні підходи до перевірки теоретичних знань часто не відображають реальної готовності співробітників протидіяти маніпулятивним впливам. Це створює нагальну потребу у формуванні формалізованого підходу, який дозволив би перейти від суб'єктивних оцінок до об'єктивного вимірювання поведінкової стійкості персоналу в умовах, наближених до реальних атак.

Запропонована у цьому розділі модель спрямована на інтеграцію кількісних метрик вразливості та якісних показників культури безпеки в єдину аналітичну систему. Створення такого інструментарію є необхідною умовою для трансформації освітніх процесів з формальної вимоги комплаєнсу в стратегічний елемент СУІБ. Це дозволяє не лише фіксувати поточний рівень захищеності, а й прогнозувати ефективність інвестицій у розвиток персоналу, забезпечуючи адаптивність системи захисту до динамічних змін у ландшафті загроз.

3.1. Визначення параметрів та інструментів для оцінки стійкості персоналу до соціоінженерних атак

Сучасна парадигма інформаційної безпеки зазнає фундаментальних трансформацій, зміщуючи стратегічний фокус від виключно технологічного захисту периметра до концепції комплексного управління людським фактором. Цей зсув зумовлений об'єктивною реальністю кіберзагроз: згідно з аналітичними даними, більшість успішних інцидентів безпеки включають елемент маніпуляції

персоналом, що робить людину критичним вектором атаки. Соціальна інженерія, як метод експлуатації когнітивних вразливостей, еволюціонувала з набору ізольованих технік у складну багатовекторну загрозу. Сучасні атаки синергетично поєднують методи психологічного тиску, глибокі знання соціальної динаміки та, все частіше, передові технології генеративного штучного інтелекту, що дозволяє автоматизувати створення висококонтекстних сценаріїв впливу.

Проста фіксація ретроспективних кількісних показників, таких як відсоток переходів за фішинговими посиланнями (click rate), вже не є достатнім індикатором реальної захищеності організації. Побудова ефективної моделі оцінювання потребує глибокого розуміння психологічних параметрів, що впливають на прийняття рішень у стресових умовах, а також застосування теоретичних моделей поведінки для прогнозування реакцій користувачів. Окрім технічних та психологічних аспектів, критично важливим стає врахування етичних обмежень, що неминуче виникають у процесі безперервного моніторингу та проведення реалістичних імітаційних симуляцій. Даний підрозділ присвячено систематизації параметрів та інструментарію, необхідних для об'єктивної оцінки готовності співробітників протидіяти сучасному спектру соціоінженерних загроз.

Для побудови цілісної та об'єктивної моделі оцінювання ефективності навчання необхідно спиратися на верифіковані методологічні підходи, серед яких провідне місце в сучасній науковій думці посідають концепції Дональда Кіркпатріка та Джека Філіпса. Класична чотирирівнева модель Кіркпатріка, яка де-факто є світовим стандартом у сфері корпоративного навчання та розвитку (L&D), пропонує чітку ієрархічну структуру вимірювання успіху. Вона передбачає послідовний рух від оцінки суб'єктивної реакції учасників до вимірювання конкретних бізнес-результатів організації. Проте в специфічному контексті кібербезпеки класична модель Кіркпатріка часто піддається критиці за обмежену здатність пояснити глибинні причини успіху або невдачі освітньої програми. Відповіддю на ці виклики стала сучасна інтерпретація методології — «New World Kirkpatrick Model». Цей підхід фокусується на поєднанні традиційних метрик із аналізом реальних дій людей

у робочому середовищі, забезпечуючи глибший та більш доказовий зв'язок між отриманими знаннями та підвищенням організаційної стійкості.

Еволюційним розвитком цього підходу є модель Джека Філіпса, яка розширює базову структуру, додаючи п'ятий рівень — оцінку рентабельності інвестицій (ROI) та врахування впливу нематеріальних активів (Intangibles), таких як репутація компанії чи довіра клієнтів. Впровадження цього рівня є критично важливим для сфери кібербезпеки, оскільки витрати на комплексне навчання персоналу часто вимірюються сотнями тисяч доларів, і вищий менеджмент вимагає чітких, фінансово обґрунтованих доказів того, що ці інвестиції запобігають реальним збиткам від потенційних атак. Унікальною особливістю методології Філіпса є пропозиція деталізованого 10-крокового процесу, який включає процедуру ізоляції ефектів навчання від інших факторів впливу. Це дозволяє математично відокремити результат тренінгів від наслідків впровадження нових технічних засобів захисту або сезонних коливань активності зловмисників, забезпечуючи чистоту експерименту. Порівняльний аналіз рівнів оцінювання за обома методологіями наведено в таблиці 3.1.

Таблиця 3.1

Порівняльна структура рівнів оцінювання за Кіркпатріком та Філіпсом

Рівень	**Назва рівня**	**Об’єкт та методи оцінювання**	**Ключові цілі в контексті безпеки**
1	Реакція та заплановані дії	Опитування, форми зворотного зв’язку після тренінгу	Визначення актуальності контенту та залученості персоналу
2	Навчання	Тести, вікторини, практичні демонстрації навичок	Оцінка приросту знань щодо розпізнавання фішингу та індикаторів атак
3	Застосування та поведінка	Симульовані атаки, спостереження, аудити безпеки	Вимірювання реальних змін у поведінці (наприклад, звітування про загрози)
4	Вплив на бізнес	Аналіз інцидентів, швидкість виявлення загроз (MTTD)	Зниження загального профілю ризику та операційних збитків
5	ROI (тільки Філіпс)	Фінансове зіставлення вигод від запобігання інцидентам із витратами	Обґрунтування бюджету на безпеку перед акціонерами та правлінням

Імплементація цих моделей дозволяє трансформувати навчання з формального процесу «перевірки галочки» на стратегічний інструмент управління корпоративними ризиками. Особливу цінність у моделі Філіпса становить механізм збору та аналізу якісного зворотного зв'язку. Це допомагає організаціям зрозуміти не лише констатацію факту провалу навчання, а й виявити, де саме стався збій та чому це відбулося. На основі таких даних стає можливим проведення точкових коригувальних дій, таких як адаптація складності навчального контенту або зміна формату подачі матеріалу для конкретних функціональних підрозділів, що підвищує загальну ефективність системи захисту.

Комплексна оцінка стійкості організації до соціоінженерних атак вимагає переходу від одновимірних показників до системи специфічних параметрів, які відображають діалектичну єдність вразливості та активної здатності персоналу протидіяти загрозам. Традиційно в індустрії кібербезпеки основним індикатором успішності вважався показник кліків (Phishing Click Rate). Проте сучасні наукові дослідження та практика вказують на суттєву обмеженість цієї метрики як єдиного критерію істини. Низький показник переходів за посиланнями не є гарантією безпеки, якщо він супроводжується пасивною поведінкою співробітників, які просто ігнорують підозрілі листи без інформування служби безпеки. Така «мовчазна відмова» залишає зловмиснику часовий простір для модифікації вектора атаки та пошуку іншої, менш пильної жертви всередині периметра організації.

Справжня кіберстійкість вимірюється через призму концепції «людського сенсора» (Human Sensor). Цей підхід постулює, що кожен співробітник є активним елементом системи моніторингу. У цьому контексті найбільш значущим параметром стає показник звітування (Reporting Rate) — відсоток співробітників, які не лише ідентифікували загрозу, а й здійснили активну дію, повідомивши про неї у відділ безпеки через офіційні канали (наприклад, кнопку

PhishButton). Систематизація ключових кількісних параметрів, необхідних для побудови моделі оцінювання, наведена в таблиці 3.2.

Таблиця 3.2

Ключові кількісні параметри оцінки стійкості персоналу

Параметр	**Визначення та формула**	**Значення для аналізу**
Phishing Click Rate	$\frac{\text{Кількість тих, хто клікнув}}{\text{Загальна кількість цілей}} \cdot 100\%$	Прямий показник вразливості "людського фактора" та ефективності фільтрів
Reporting Rate	$\frac{\text{Кількість звітованих атак}}{\text{Загальна кількість цілей}} \cdot 100\%$	Показник активної оборони та рівня залученості персоналу в процеси безпеки
Credential Submission Rate	$\frac{\text{Кількість введених паролів}}{\text{Загальна кількість цілей}} \cdot 100\%$	Найбільш критична метрика ризику компрометації облікових записів
Resilience Ratio	$\frac{\text{Кількість звітів}}{\text{Кількість кліків}}$	Співвідношення між тими, хто захищає організацію, та тими, хто наражає її на ризик
Mean Time to Report (MTTR)	Середній час від отримання атаки до моменту звітування	Параметр швидкості реакції, що безпосередньо впливає на час експозиції загрози

Окрім абсолютних кількісних показників, модель оцінювання повинна враховувати часові параметри, зокрема так званий «час перебування» (Dwell Time). Статистичні дані за 2024–2025 роки демонструють критичну важливість швидкості реакції: медіанний час натискання на фішингове посилання становить лише 21 секунду, а введення та відправка конфіденційних даних відбувається в середньому протягом 28 секунд після відкриття шкідливого листа [65]. Ці емпіричні дані свідчать про те, що когнітивний процес прийняття рішення відбувається майже миттєво, тому навчання має бути спрямоване на розвиток інстинктивних навичок ідентифікації загроз у критично короткі часові проміжки.

Впровадження метрики Real Dwell Time (реальний час перебування загрози в мережі до її виявлення) дозволяє оцінити ефективність взаємодії персоналу та команди реагування (SOC). Скорочення середнього часу звітування з годин до хвилин надає командам захисту можливість оперативно заблокувати

шкідливий домен або хеш файлу на рівні всієї організації ще до того, як наступний співробітник потенційно припуститься помилки, перетворюючи таким чином індивідуальну пильність на колективний імунітет [66].

Ефективна реалізація розробленої моделі оцінювання є неможливою без застосування спеціалізованих технологічних платформ, які забезпечують можливість проведення контрольованих та безпечних соціоінженерних атак. Сучасний ринок рішень у цій сфері демонструє чітку сегментацію на три основні категорії: комерційні платформи повного циклу (SaaS), відкрите програмне забезпечення (Open Source) та інтегровані модулі безпеки в екосистемах захисту периметра [67].

У сегменті комерційних рішень домінуючі позиції займають платформи, такі як KnowBe4, Proofpoint та Infosec IQ. Їхньою ключовою відмінністю є інтеграція функціоналу симуляцій з інструментами глибокої предиктивної аналітики, що базується на алгоритмах ML. Зокрема, платформа KnowBe4 володіє наймасштабнішою в індустрії бібліотекою навчального контенту (понад 1200 інтерактивних модулів), що дозволяє підтримувати стабільно високий рівень залученості персоналу та уникати ефекту «втоми від навчання» (training fatigue). Конкурентне рішення від Proofpoint вирізняється науково обґрунтованим підходом до корекції поведінки, пропонуючи концепцію «моментів навчання» (teachable moments). Ця методика передбачає надання мікро-навчання безпосередньо в момент допущення помилки співробітником, що, згідно з емпіричними дослідженнями, дозволяє знизити частоту повторних інцидентів.

Для організацій зі специфічними вимогами до конфіденційності, які обмежують використання хмарних сервісів, або за умов обмеженого бюджету, оптимальним вибором залишаються інструменти з відкритим кодом, лідером серед яких є Gophish. Цей інструментарій дозволяє створювати «піксельно ідеальні» шаблони атак, що повністю імітують реальні загрози, та відстежувати результати кампаній у реальному часі за допомогою кросплатформенних

бінарних файлів (Windows, macOS, Linux). Проте впровадження Gophish вимагає наявності високої внутрішньої експертизи для розробки власного навчального контенту та технічного налаштування інтеграції з поштовими шлюзами, оскільки система не є рішенням класу «з коробки» та не містить вбудованих освітніх модулів.

Ефективна модель оцінювання стійкості персоналу не може обмежуватися виключно аналізом зовнішніх проявів, а повинна інтегрувати діагностику глибинних психологічних предикторів поведінки. Застосування валідованих психометричних шкал дозволяє ідентифікувати латентні прогалини в культурі кібербезпеки на етапі, що передує їх реалізації у вигляді реальних інцидентів. Фундаментальними інструментами в цій площині виступають опитувальник людських аспектів інформаційної безпеки (HAIS-Q) та шкала сприйняття ризиків кібербезпеки (CRPS). Структура HAIS-Q базується на вимірюванні трьох ключових доменів за моделлю KAB: знань (Knowledge), установок (Attitude) та поведінки (Behavior). Емпіричні дослідження підтверджують існування феномену «розриву між знаннями та поведінкою» (Knowledge-Behavior Gap): статистика свідчить, що користувачі здатні демонструвати високі результати в теоретичних тестах (наприклад, середній бал 4.2/5 в домені інтернет-безпеки), проте при цьому виявляти критично низькі показники (2.3/5) у реальній практиці управління паролями. Цей дисонанс доводить, що освітні стратегії, сфокусовані лише на трансляції інформації, є малоефективними без формування стійких поведінкових патернів.

Детальний аналіз психометричних параметрів дозволяє виділити конкретні фактори впливу на рівень кіберстійкості індивіда. Зокрема, така особистісна риса як сумлінність (Conscientiousness) демонструє стійку кореляцію зі зниженням ризикованої активності в мережі та суворим дотриманням політик безпеки. На противагу цьому, висока толерантність до ризику спонукає суб'єктів віддавати перевагу зручності перед протоколами захисту, що перетворює їх на пріоритетні цілі для атак, сценарії яких базуються на пропозиціях «швидкої

вигоди». Суттєвою загрозою є когнітивне викривлення, відоме як «оптимізм щодо власної безпеки» (Optimism Bias), що проявляється у хибному переконанні співробітника щодо неможливості його зламу. У дослідженнях за шкалою CRPS цей параметр часто отримує низькі оцінки (на рівні 2.3/5), що сигналізує про неадекватне сприйняття особистої вразливості. Водночас, фактор сприйняття тяжкості загрози відіграє позитивну роль: співробітники, які чітко усвідомлюють масштаб потенційних наслідків інциденту для організації, демонструють вищий рівень комплаєнсу після проходження навчання .

Інтеграція результатів психометричного оцінювання у загальну модель стійкості дозволяє здійснити перехід від сегментації персоналу за формальними посадовими ознаками до кластеризації за психологічними профілями ризику. Такий підхід відкриває можливості для впровадження адаптивного навчання: для груп з високою толерантністю до ризику навчальний акцент зміщується на демонстрацію негативних наслідків інцидентів, тоді як для співробітників з високим рівнем тривожності пріоритетом стає надання чітких, алгоритмізованих інструкцій, що знижують невизначеність та підвищують впевненість у власних діях.

3.2 Розроблення моделі оцінювання ефективності навчання співробітників із протидії соціоінженерним атакам

Сучасні підходи до оцінювання ефективності навчання персоналу з питань інформаційної безпеки, зокрема у сфері протидії соціоінженерним атакам, характеризуються переважно статичним та фрагментарним характером. У більшості випадків вони зосереджуються на перевірці рівня засвоєння теоретичних знань шляхом тестування або аналізу результатів разових навчальних заходів, що не дозволяє адекватно відобразити реальний рівень стійкості персоналу до актуальних загроз. В умовах динамічного розвитку соціоінженерних методів атак та зростання ролі людського фактору в системах

управління інформаційною безпекою виникає потреба у розробленні більш комплексної та адаптивної моделі оцінювання.

У процесі дослідження встановлено, що класичні моделі оцінювання навчання, зокрема модель Д. Кіркпатріка та її модифікації, мають низку суттєвих обмежень при застосуванні в контексті кібербезпеки. Основним недоліком є їх лінійна структура та орієнтація на ретроспективний аналіз результатів навчання, що не враховує поведінкові та психологічні аспекти взаємодії співробітника з інформаційними системами у реальному часі. Крім того, такі підходи практично не інтегруються з технічними засобами моніторингу безпеки та не враховують контекстуальну критичність ролі конкретного працівника в організації.

З урахуванням зазначених недоліків у роботі запропоновано інтегральну багатофакторну модель оцінювання ефективності навчання співробітників із протидії соціоінженерним атакам, яка отримала назву «Багатофакторна модель поведінкової кіберстійкості» (Multifactor Behavioral Cyber Resilience Model, MBCR). Концептуально модель орієнтована не лише на контроль рівня знань, а на управління динамічною кіберстійкістю персоналу як елемента загальної системи захисту інформації підприємства.

Ключовим поняттям запропонованої моделі є індекс кіберстійкості (Cyber Resilience Index, CRI), який визначається як інтегральний кількісний показник здатності конкретного співробітника або організаційного підрозділу протидіяти соціоінженерним атакам з урахуванням знань, фактичної поведінки, психологічного стану та контексту виконуваних функцій. На відміну від традиційних підходів, індекс CRI розраховується не епізодично, а на безперервній основі з використанням актуальних даних з різних джерел.

Структурно модель MBCR базується на чотирьох взаємопов’язаних вимірах оцінювання: когнітивному, поведінковому, психологічному та контекстуальному. Кожен з цих вимірів формує окрему компоненту інтегрального індексу та відображає різні аспекти взаємодії співробітника з інформаційним середовищем.

Когнітивний вимір (K) характеризує рівень теоретичних знань співробітника у сфері інформаційної безпеки, зокрема розуміння принципів соціальної інженерії, внутрішніх політик безпеки, процедур реагування на інциденти та правил роботи з корпоративними інформаційними ресурсами. На відміну від класичних підходів, у межах моделі MBCR когнітивна складова оцінюється не через разові річні тестування, а за допомогою мікро-квізів формату Just-in-Time, а також аналізу звернень до служби підтримки та результатів коротких перевірок знань, інтегрованих у повсякденну діяльність користувачів. Такий підхід дозволяє враховувати ефект поступового забування інформації та забезпечує актуальність оцінки знань.

Поведінковий вимір (B) відображає реальні дії співробітника в інформаційних системах та є центральним елементом моделі. До основних метрик поведінкової складової належать показники частоти помилкових дій (Click Rate), активності повідомлення про підозрілі події (Reporting Rate), часу реагування на інциденти (Dwell Time), дотримання парольної політики, використання захищених каналів зв’язку та інших вимог політик безпеки. Інноваційним елементом моделі є впровадження концепції «людського сенсора», відповідно до якої співробітник отримує позитивне підкріплення не лише за відсутність помилок, а насамперед за активну участь у виявленні загроз шляхом своєчасного повідомлення про підозрілі події. Таким чином, модель стимулює проактивну поведінку персоналу та інтегрує людський фактор у процеси моніторингу безпеки.

Психологічний вимір (P) враховує психоемоційний стан співробітника, його ставлення до вимог інформаційної безпеки та рівень суб’єктивної впевненості у власних діях. Для оцінювання цієї складової використовуються результати стандартизованих психометричних опитувальників, зокрема індекси обізнаності та ставлення до безпеки (HAIS-Q), показники схильності до ризику та рівня «втоми від безпеки» (Security Fatigue). У межах моделі передбачається, що високий рівень стресу або емоційного вигорання може тимчасово знижувати

здатність співробітника адекватно реагувати на загрози. З огляду на це психологічна складова використовується як модифікатор інших параметрів, що дозволяє адаптувати навчальні та контрольні заходи до поточного стану працівника та уникнути ефекту блокування навчання внаслідок надмірного навантаження.

Контекстуальний вимір (C) реалізується у вигляді рольового коефіцієнта ризику, який відображає критичність помилок співробітника з точки зору бізнес-процесів та потенційного впливу на інформаційну безпеку організації. Значення цього коефіцієнта визначається на основі посади, рівня доступу до інформаційних ресурсів та участі у критичних процесах. Наприклад, для системних адміністраторів або фінансових працівників коефіцієнт має підвищене значення, тоді як для співробітників з обмеженим доступом — знижене. Такий підхід дозволяє зробити модель оцінювання більш справедливою та орієнтованою на реальний бізнес-ризик.

Інтегральний індекс кіберстійкості окремого співробітника у моделі MBCR визначається за формулою 3.1:

$$CRI_i = \frac{(K_i \cdot \omega_k) + (B_i \cdot \omega_b) + (P_i \cdot \omega_p)}{R_i} \cdot C_{role}, \qquad (3.1)$$

де i — ідентифікатор співробітника; K, B, P — відповідні значення когнітивної, поведінкової та психологічної складових; ω_k, ω_b, ω_p — вагові коефіцієнти, що відображають пріоритетність відповідних вимірів; R_i — рівень поточної зовнішньої загрози для підрозділу або організації; C_{role} — коефіцієнт критичності ролі.

У межах роботи обґрунтовано доцільність надання найбільшої ваги поведінковій складовій, оскільки саме реальні дії користувача визначають успішність або неуспішність соціоінженерної атаки.

Науковою новизною моделі є також введення параметра «періоду напіврозпаду навички», що описує зниження рівня кіберстійкості у разі відсутності практичного застосування знань та навичок. Згідно з цим підходом, значення індексу CRI з часом зменшується за експоненційним законом, що математично обґрунтовує необхідність безперервного навчання та регулярних коригуючих заходів.

Запропонована модель дозволяє подолати основні недоліки існуючих підходів до оцінювання ефективності навчання персоналу. Зокрема, замість статичної оцінки раз на рік реалізується динамічний підхід з постійним оновленням показників. Негативний психологічний ефект від каральних моделей контролю замінюється механізмами позитивного підкріплення та формування культури кіберстійкості. Прозорість метрик забезпечує зрозумілість результатів як для співробітників, так і для фахівців з інформаційної безпеки, а інтеграція з операційними процесами дозволяє використовувати результати оцінювання у реальному часі.

Таким чином, розроблена багатофакторна модель поведінкової кіберстійкості формує методологічне підґрунтя для переходу від формального оцінювання знань до комплексного управління людським фактором у системі інформаційної безпеки підприємства. Запропонований підхід забезпечує більш точне відображення реального рівня готовності персоналу до протидії соціоінженерним атакам та створює передумови для інтеграції навчальних процесів із загальною архітектурою кіберзахисту.

З метою забезпечення практичної застосовності запропонованої багатофакторної моделі поведінкової кіберстійкості доцільним є розроблення узагальненого плану її впровадження в інформаційну інфраструктуру абстрактної організації. Такий план має враховувати сучасні принципи побудови корпоративних інформаційних систем, вимоги до масштабованості, інтегрованості та сумісності з існуючими засобами управління інформаційною безпекою.

Запропоноване впровадження моделі MBCR базується на компонентно-сервісній архітектурі та передбачає чіткий розподіл функцій між клієнтською частиною, серверним ядром застосунку та зовнішньою екосистемою безпеки підприємства. Такий підхід дозволяє відокремити логіку взаємодії з користувачами від процесів оброблення даних, аналітики та інтеграції з корпоративними системами моніторингу.

Клієнтська частина системи (Frontend) виконує функцію основного інтерфейсу взаємодії персоналу та відповідальних осіб із моделлю MBCR. У її складі передбачається реалізація двох основних компонентів: кабінету користувача та адміністративної панелі. Кабінет користувача призначений для проходження навчальних матеріалів, мікро-тестувань, психометричних опитувальників, а також для перегляду власного індексу кіберстійкості та його динаміки. Така прозорість забезпечує підвищення усвідомленості персоналу та формування відповідального ставлення до вимог інформаційної безпеки.

Адміністративна панель орієнтована на фахівців з інформаційної безпеки, зокрема офіцерів безпеки (CISO) та представників кадрових підрозділів. Вона забезпечує доступ до агрегованої аналітики, візуалізації рівнів кіберстійкості за підрозділами, налаштування вагових коефіцієнтів моделі, а також управління навчальним контентом. Клієнтська частина взаємодіє з серверною інфраструктурою виключно через стандартизовані програмні інтерфейси, що забезпечує ізоляцію бізнес-логіки та підвищує рівень безпеки.

Ядро застосунку MBCR реалізується у вигляді серверної частини (Backend), побудованої за модульним принципом. Центральним елементом серверної інфраструктури є API Gateway, який виконує функції єдиної точки входу для клієнтських запитів, забезпечує автентифікацію, авторизацію та маршрутизацію трафіку до відповідних сервісів. Такий підхід дозволяє реалізувати принцип слабкої зв’язаності компонентів та спрощує масштабування системи.

Основним аналітичним компонентом серверної частини є сервіс розрахунків (Calculation Engine), у якому безпосередньо реалізується математичний апарат моделі MBCR та здійснюється обчислення індексу кіберстійкості. Цей сервіс функціонує як у режимі оброблення подій у реальному часі, так і за розкладом, перераховуючи значення показників на основі нових даних, що надходять із зовнішніх джерел. Саме в межах цього компонента реалізується логіка урахування когнітивних, поведінкових, психологічних та контекстуальних параметрів.

Окремим компонентом серверної частини є сервіс управління навчальним контентом та тестуванням (Testing and Content Manager). Його призначення полягає у зберіганні навчальних матеріалів, формуванні мікро-квізів, фіксації результатів тестувань та передачі відповідних даних до сервісу розрахунків. Така ізоляція дозволяє незалежно розвивати навчальну складову без втручання у ядро аналітичної логіки.

Ключову роль у забезпеченні інтеграції моделі MBCR з корпоративною інфраструктурою відіграє сервіс агрегації даних (Data Aggregation Service). Даний компонент відповідає за збір, нормалізацію та попередню обробку інформації, що надходить із зовнішніх систем, зокрема SIEM-платформ, HR-систем та інших джерел контекстної інформації. Сервіс агрегації виступає проміжною ланкою між зовнішнім середовищем та аналітичним ядром, забезпечуючи узгодженість форматів даних та зменшення навантаження на інші компоненти системи.

Для зберігання інформації про користувачів, результати навчання, поведінкові події та історичні значення індексу кіберстійкості використовується централізована база даних. У ній акумулюються як поточні, так і ретроспективні дані, що дозволяє формувати тренди, проводити аналіз динаміки та використовувати інформацію для подальшого вдосконалення моделі.

Важливою складовою запропонованого плану впровадження є інтеграція моделі MBCR з корпоративними SIEM-системами, які виконують функції

централізованого збору та кореляції подій безпеки. Така інтеграція реалізується на основі двонаправленого обміну даними. З одного боку, серверна частина MBCR передає до SIEM агреговані результати оцінювання у вигляді індексу кіберстійкості та пов’язаних з ним метаданих, використовуючи стандартизовані механізми передачі подій, зокрема REST API або протоколи структурованого логування. З іншого боку, сервіс агрегації періодично отримує з SIEM інформацію про інциденти, пов’язані з конкретними користувачами, що безпосередньо впливає на формування поведінкової складової індексу.

Окремо слід відзначити можливість використання SIEM як джерела контекстного збагачення даних. Передача до SIEM списків користувачів із підвищеним рівнем ризику дозволяє реалізувати механізми пріоритезації інцидентів у межах центру моніторингу безпеки. У такому випадку події, пов’язані з користувачами з низьким рівнем кіберстійкості, автоматично отримують вищий рівень критичності, що підвищує ефективність реагування.

У межах більш зрілих реалізацій модель MBCR може бути додатково інтегрована з платформами класу SOAR, що дозволяє автоматизувати процеси реагування на інциденти. У разі фіксації критичного зниження індексу кіберстійкості відповідні сценарії реагування можуть ініціювати тимчасове обмеження доступів користувача до окремих ресурсів через служби каталогів, такі як Active Directory або LDAP. Відновлення повних прав доступу здійснюється після проходження коригуючого навчання та підвищення значень відповідних компонентів моделі.

Додатковим джерелом контекстної інформації для моделі є кадрові системи підприємства, з яких отримуються дані про роль співробітника, підрозділ, періоди відпусток або підвищеного навантаження. Залучення таких даних дозволяє коректніше інтерпретувати поведінкові показники та уникати хибних висновків щодо рівня кіберстійкості персоналу. Повна можлива архітектура моделі MBCR зображена на рисунку 3.1.

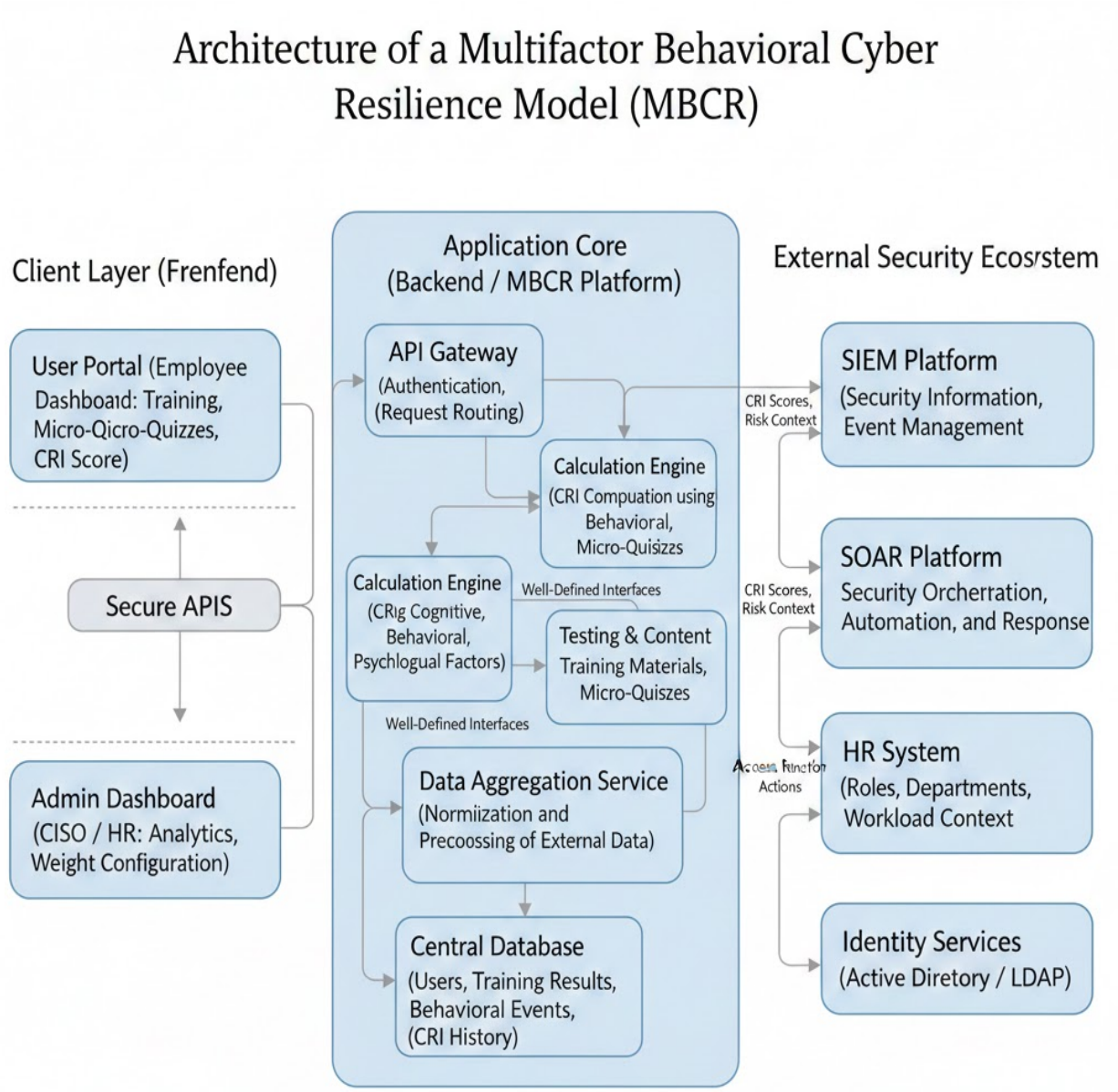

Рис. 3.1. Архітектура моделі MBCR

Запропонований план впровадження демонструє, що модель MBCR може функціонувати не як ізольований навчальний інструмент, а як повноцінний елемент корпоративної системи управління інформаційною безпекою. Компонентно-сервісна архітектура забезпечує гнучкість, масштабованість та можливість інтеграції з існуючими засобами моніторингу й реагування, що відповідає сучасним підходам до побудови систем класу Human Risk Management.

3.3. Розроблення рекомендацій щодо застосування моделі в системі управління інформаційною безпекою

Ефективність будь-якої теоретичної моделі, незалежно від рівня її математичної формалізації, визначається ступенем інтеграції в існуючі бізнес-процеси та контури управління безпекою організації. Розроблена у попередньому підрозділі багатофакторна модель поведінкової кіберстійкості (MBCR) належить до класу комплексних аналітичних інструментів, застосування яких потребує системного та поетапного підходу. Простого розгортання програмного забезпечення в цьому випадку є недостатньо, оскільки повноцінне функціонування моделі передбачає трансформацію підходів до управління ризиками, реагування на інциденти та контролю доступу до інформаційних ресурсів.

У даному підрозділі сформульовано науково-практичні рекомендації щодо імплементації моделі MBCR у систему управління інформаційною безпекою організації. Визначено етапність її впровадження, описано сценарії операційного застосування в екосистемі SOC/SIEM, а також обґрунтовано стратегічні переваги використання моделі для підвищення загального рівня зрілості системи управління інформаційною безпекою.

З метою мінімізації операційних ризиків та забезпечення поступової адаптації персоналу до нових методів оцінювання доцільно застосовувати ітераційний підхід до впровадження моделі MBCR. Запропонована методологія складається з чотирьох послідовних етапів: діагностичного, калібрувального, інтеграційного та етапу експлуатаційної оптимізації.

Етап 1. Діагностика та визначення базової лінії (Baseline Assessment). Початковим завданням є формування об’єктивного уявлення про поточний рівень кіберстійкості персоналу. На даному етапі модель MBCR функціонує в режимі пасивного спостереження без застосування керуючих впливів.

Здійснюється збір історичних даних із SIEM-систем, журналів поштових шлюзів, результатів попередніх навчальних програм та симуляцій соціоінженерних атак. Отримана інформація використовується для формування первинних поведінкових профілів користувачів.

Паралельно проводиться первинне психометричне профілювання персоналу шляхом анонімізованого опитування за методикою HAIS-Q, що дозволяє визначити загальний рівень культури безпеки в організації та ідентифікувати підрозділи з підвищеним рівнем «втоми від безпеки».

На основі зібраних даних здійснюється розрахунок початкового значення індексу кіберстійкості (CRI_0) для кожного співробітника без активного впливу з боку системи. Це дозволяє зафіксувати базову точку відліку для подальшого оцінювання ефективності впровадження моделі та аналізу економічної доцільності (ROI).

Етап 2. Калібрування вагових коефіцієнтів та параметризація.

Ключовим фактором успішного застосування моделі є адаптація її математичного апарату до специфіки діяльності конкретної організації. Використання універсальних значень вагових коефіцієнтів може призвести до викривлення результатів оцінювання.

Рекомендується здійснити налаштування вагових коефіцієнтів компонентів моделі з урахуванням галузевих особливостей. Для фінансових установ доцільним є підвищення ваги поведінкової складової, оскільки навіть поодинокі помилки можуть мати значні фінансові наслідки. Для науково-дослідних або креативних підрозділів, навпаки, рекомендовано зменшити жорсткість автоматичних обмежень з метою недопущення негативного впливу на інноваційні процеси.

На цьому ж етапі визначаються порогові значення індексу CRI, при досягненні яких система ініціює автоматизовані реакції. Доцільним є впровадження багаторівневої шкали ризику, зокрема «жовтої зони» ($CRI < 60\ \%$) та «червоної зони» ($CRI < 40\ \%$).

Додатково здійснюється кластеризація посадових ролей із присвоєнням коефіцієнтів критичності. Рекомендується виділяти щонайменше три групи: привілейовані користувачі та адміністратори, користувачі критичних бізнес-систем та загальний персонал.

Етап 3. Технічна інтеграція та пілотний запуск.

На даному етапі модель MBCR підключається до механізмів активного реагування. Налаштовується двонаправлений обмін даними з SIEM-системами, при якому індекс CRI використовується як елемент контекстного збагачення для кореляції подій безпеки.

Розробляються сценарії автоматизованого реагування (playbooks), які активуються у разі критичних змін поведінкових показників. Наприклад, у випадку різкого зниження індексу система може автоматично перевести обліковий запис користувача до групи з обмеженими правами доступу до моменту з’ясування обставин.

Для перевірки адекватності налаштувань рекомендується пілотний запуск моделі на обмеженій групі користувачів (5–10 % персоналу). Це дозволяє виявити потенційні конфлікти з бізнес-процесами та скоригувати параметри системи до масштабного впровадження.

Етап 4. Масштабування та експлуатаційна оптимізація.

Після успішного пілотування здійснюється повноцінне розгортання моделі на всю організацію з переходом до циклу безперервного вдосконалення (PDCA). Активується механізм експоненційного зниження індексу у разі відсутності навчальної активності, що стимулює підтримку знань у актуальному стані. Рекомендується періодичний перегляд параметрів моделі на основі аналізу реальних інцидентів.

Модель MBCR доцільно розглядати не лише як інструмент навчання персоналу, а як елемент стратегічного управління інформаційною безпекою, що забезпечує перехід від реактивного до проактивного захисту.

Впровадження моделі дозволяє реалізувати динамічний підхід до контролю доступу, при якому рівень довіри до користувача корелює з його поточним індексом кіберстійкості. Користувачі з високими значеннями CRI можуть отримувати розширені можливості доступу, тоді як зниження індексу автоматично активує додаткові механізми контролю, зокрема посилену багатофакторну автентифікацію.

Використання CRI як контекстної метрики дозволяє оптимізувати роботу центру моніторингу безпеки. Одна і та сама подія може мати різний рівень пріоритету залежно від профілю користувача, що зменшує кількість помилкових спрацьовувань та навантаження на аналітиків.

Накопичення поведінкових даних створює передумови для використання предиктивної аналітики. Застосування концепції «цифрового двійника співробітника» дозволяє моделювати реакції персоналу на потенційні атаки та проводити превентивні заходи без надмірного залучення користувачів.

Модель MBCR доцільно застосовувати протягом усього життєвого циклу співробітника в організації.

У процесі адаптації нових працівників модель забезпечує поетапне відкриття доступів відповідно до зростання індексу кіберстійкості, при цьому початкові помилки розглядаються як навчальні ситуації без адміністративних санкцій.

У разі інцидентів модель дозволяє гнучко поєднувати технічні заходи реагування з урахуванням поведінки та психологічного стану користувача, стимулюючи своєчасне повідомлення про помилки.

Для співробітників із стабільно високими показниками CRI модель забезпечує механізми заохочення та зменшення кількості перевірочних заходів, що сприяє формуванню культури безпеки та підвищенню мотивації.

Успішне функціонування моделі неможливе без дотримання принципів прозорості та захисту персональних даних. Рекомендується забезпечити розмежування доступу до психометричної інформації, при якому керівникам надається лише агрегований рівень ризику без деталізації психологічних показників.

Реалізація моделі потребує чіткого розподілу ролей між підрозділами інформаційної безпеки, управління персоналом та відповідальними за захист даних особами, що забезпечує баланс між безпекою, етикою та законодавчими вимогами.

Для верифікації результативності впровадження рекомендується використовувати систему ключових показників ефективності, серед яких динаміка середнього значення CRI, скорочення часу виявлення інцидентів, зменшення кількості помилкових спрацьовувань у SOC та економічна ефективність у вигляді зниження очікуваних річних втрат.

Практичне застосування багатофакторної моделі поведінкової кіберстійкості дозволяє здійснити перехід від формального виконання вимог до динамічного управління ризиками людського фактору. Запропонований підхід забезпечує персоналізацію заходів захисту, зменшує негативний вплив «втоми від безпеки» та інтегрує персонал у процеси виявлення і протидії загрозам. Таким чином, модель MBCR створює умови для перетворення людського фактору з джерела вразливостей на активний елемент системи кіберзахисту, що повністю відповідає меті та завданням магістерського дослідження.

Висновки до розділу 3

У третьому розділі розроблено та теоретично обґрунтовано авторську багатофакторну модель поведінкової кіберстійкості (Multifactor Behavioral Cyber Resilience Model, MBCR), яка дозволяє перейти від статичного оцінювання знань до динамічного управління ризиками людського фактору.

Визначено ключові параметри та інструменти оцінювання, де на основі моделей Д. Кіркпатріка та Дж. Філліпса запропоновано систему кількісних і якісних метрик. Доведено, що для об’єктивного аналізу стійкості необхідно враховувати не лише показник вразливості (Click Rate), а й показники активної оборони, такі як коефіцієнт звітування (Reporting Rate) та середній час реакції (MTTR). Обґрунтовано

використання психометричних інструментів (HAIS-Q, CRPS) для виявлення когнітивних упереджень, зокрема «оптимізму щодо власної безпеки».

Центральним результатом розділу є математична формалізація індексу кіберстійкості (Cyber Resilience Index, CRI). На відміну від існуючих аналогів, індекс CRI у моделі MBCR інтегрує чотири виміри:

1. Когнітивний (K): динамічне вимірювання знань через мікро-квізи.
2. Поведінковий (B): аналіз реальних дій користувача в інформаційних системах.
3. Психологічний (P): врахування стресостійкості та емоційного стану як модифікаторів ризику.
4. Контекстуальний (C): оцінка критичності посадової ролі та рівня доступу.

Запропоновано компонентно-сервісну архітектуру системи, що забезпечує безшовну інтеграцію моделі MBCR у існуючу екосистему безпеки підприємства. Розроблено схему взаємодії між ядром розрахунків (Calculation Engine), SIEM-платформою та службами каталогів (Active Directory/LDAP), що дозволяє реалізувати механізм автоматизованого реагування: від адаптивного навчання до динамічного обмеження прав доступу у разі критичного зниження рівня безпеки користувача.

Сформульовано науково-практичні рекомендації щодо етапного впровадження моделі (діагностика, калібрування, інтеграція, оптимізація). Обґрунтовано переваги переходу до стратегії «людського сенсора», де співробітник стає активним елементом системи виявлення загроз. Окрему увагу приділено етичним аспектам, зокрема захисту приватності психометричних даних та мінімізації негативного впливу стресових факторів на персонал.

Таким чином, розроблена модель MBCR є комплексним науково-прикладним інструментарієм, який дозволяє перетворити персонал із «найслабшої ланки» на активний «людський фаєрвол», забезпечуючи адаптивність системи управління інформаційною безпекою до новітніх соціоінженерних загроз.

ВИСНОВКИ

У кваліфікаційній роботі було проведено комплексне дослідження методів підготовки персоналу до протидії соціоінженерним впливам та розроблено багаторівневу модель оцінювання ефективності такого навчання. У ході виконання поставлених завдань було отримано низку результатів.

Розглянуто теоретичні аспекти та сучасний стан соціоінженерних атак, які у 2024–2025 роках трансформувалися у високотехнологічні операції. Встановлено, що використання генеративного ШІ (дипфейки, клонування голосу) дозволяє зловмисникам створювати бездоганні сценарії маніпуляцій, що робить людину критичним об'єктом захисту в системі інформаційної безпеки.

Досліджено роль людського фактору та встановлено, що традиційні підходи до навчання (лекції, тести) є малоефективними через ігнорування психофізіологічних особливостей сприйняття. Виявлено феномени «втоми від безпеки» та «когнітивних упереджень», які створюють розрив між теоретичними знаннями співробітника та його реальною поведінкою під час атаки.

Проаналізовано існуючі інструменти та платформи навчання (KnowBe4, Cyber Ranges, гейміфіковані симулятори). Аналіз показав, що для технічного персоналу найбільш ефективним є навчання на кіберполігонах, тоді як для загального штату критично важливим є використання адаптивного мікро-навчання в момент вчинення помилки.

Розроблено інтегральну багатофакторну модель поведінкової кіберстійкості (MBCR). Наукова новизна моделі полягає у впровадженні індексу кіберстійкості (CRI), який базується на чотирьох вимірах: когнітивному (знання), поведінковому (реальні дії), психологічному (емоційний стан) та контекстуальному (посадова роль).

Запропоновано архітектуру впровадження моделі, яка забезпечує автоматизовану взаємодію між освітньою платформою та системами моніторингу безпеки (SIEM/SOAR). Це дозволяє не лише оцінювати персонал, а

й динамічно змінювати права доступу користувачів залежно від їхнього поточного рівня кіберстійкості.

У кваліфікаційній роботі були запропоновані наступні рекомендації:

- відійти від практики щорічних формальних перевірок знань на користь безперервного моніторингу поведінкових метрик (Reporting Rate, Click Rate, MTTR);
- впровадити концепцію «людського сенсора», створивши систему позитивної мотивації та винагород для співробітників, які вчасно виявляють та звітують про підозрілі події;
- використовувати адаптивні сценарії симуляцій атак, що враховують психологічний профіль працівника та рівень його «втоми від безпеки» для уникнення емоційного вигорання;
- інтегрувати результати навчання з операційними процесами SOC, використовуючи індекс CRI для пріоритезації інцидентів та виявлення найбільш вразливих груп користувачів;
- запровадити практику Just-in-Time навчання, коли навчальний контент надається автоматично одразу після того, як співробітник припустився помилки під час симуляції, що забезпечує максимальне закріплення навички.

Таким чином, впровадження запропонованої моделі MBCR та наведених рекомендацій дозволяє трансформувати персонал з потенційного джерела вразливостей на активний елемент системи захисту («людський фаєрвол»), значно посилюючи загальну кіберстійкість організації в умовах сучасних гібридних загроз.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Жмурко О. Соціальна інженерія як загроза кібербезпеці: методи запобігання та захисту // PedBez. 2024. Т. 9, № 1. С. 37–42. DOI: https://doi.org/10.31649/2524-1079-2024-9-1-037-042

2. Social Engineering. URL: https://www.imperva.com/learn/application-security/social-engineering-attack/ (дата звернення: 15.12.2025).

3. Pallavi Pavithran. 5-Step Plan for Prevention of Social Engineering Attacks. URL: https://fidelissecurity.com/threatgeek/cyberattacks/social-engineering-prevention-plan/ (дата звернення: 15.12.2025).

4. Мітнік К. Д., Саймон В. Л. Мистецтво обману. М. : Компанія АйТі, 2004. 360 с.

5. An introduction to social engineering / CERT-UK. URL: https://info.publicintelligence.net/UK-CERT-SocialEngineering.pdf (дата звернення: 15.12.2025).

6. Granger S. Social engineering fundamentals, part I: hacker tactics. *Security Focus*. December 18, 2001.

7. Krombholz K., Hobel H., Huber M., Weippl E. Advanced social engineering attacks. *Journal of Information Security and Applications*. 2015. Vol. 22. P. 113–122.

8. Social Engineering Toolkit (SET): Manipulating the Human Element in Security | Overview, Features, and Why Ethical Hackers Use It. URL: https://www.webasha.com/blog/social-engineering-toolkit-set-manipulating-the-human-element-in-security-overview-features-and-why-ethical-hackers-use-it (дата звернення: 15.12.2025).

9. What is Pretexting? Attacks, Examples & Techniques — SentinelOne. URL: https://www.sentinelone.com/cybersecurity-101/cybersecurity/pretexting/ (дата звернення: 15.12.2025).

10. Spear Phishing vs. Phishing: What's the Difference? | IBM. URL: https://www.ibm.com/think/topics/spear-phishing-vs-standard-phishing (дата звернення: 15.12.2025).

11. What is Pretexting? | CrowdStrike. URL: https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/pretexting-attack/ (дата звернення: 15.12.2025).

12. What Is a Quid Pro Quo Attack? | Examples & Prevention Tips — SoSafe. URL: https://sosafe-awareness.com/glossary/quid-pro-quo-attacks/ (дата звернення: 15.12.2025).

13. Rajgopal P. R. AI Threat Countermeasures: Defending Against LLM-Powered Social Engineering // International Journal of IoT. 2025. Vol. 5, No. 02. P. 23–43. DOI: https://doi.org/10.55640/ijiot-05-02-03.

14. With generative AI, social engineering gets more dangerous—and harder to spot. URL: https://www.ibm.com/think/insights/generative-ai-social-engineering (дата звернення: 15.12.2025).

15. 85+ Social Engineering Statistics to Know for 2026 — Secureframe. URL: https://secureframe.com/blog/social-engineering-statistics (дата звернення: 15.12.2025).

16. Wijesinghe L. S. AI-Driven Social Engineering: Features and Evolution of Phishing, Vishing, and Smishing. URL: https://www.diva-portal.org/smash/get/diva2:2017124/FULLTEXT01.pdf (дата звернення: 15.12.2025).

17. Deepfake Attacks & AI-Generated Phishing: 2025 Statistics — ZeroThreat. URL: https://zerothreat.ai/blog/deepfake-and-ai-phishing-statistics (дата звернення: 15.12.2025).

18. From Deepfakes to Dark LLMs: 5 use-cases of how AI is Powering Cybercrime — Group-IB. URL: https://www.group-ib.com/blog/ai-cybercrime-usecases/ (дата звернення: 15.12.2025).

19. Deepfake Statistics 2025: AI Fraud Data & Trends — DeepStrike. URL: https://deepstrike.io/blog/deepfake-statistics-2025 (дата звернення: 15.12.2025).

20. Cyberthreat Predictions for 2026: Industrialized Cybercrime and the Acceleration of the Attack Life Cycle. URL: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/report-threat-predictions-2026.pdf (дата звернення: 15.12.2025).

21. Термін «Людський фактор». URL: https://zakon.rada.gov.ua/laws/term/53505:111454/sp:dark (дата звернення: 15.12.2025).

22. Koźmiński A. K., Jemielniak D. Management from the beginning. Academic coursebook. Warsaw : Wydawnictwa Akademickie i Profesjonalne, 2008.

23. Lent B. Managing processes of project management: Informatics and communication. Warsaw : Difin, 2005.

24. Wang Y. On cognitive properties of human factors and error models in engineering and socialization // International Journal of Cognitive Informatics and Natural Intelligence. 2008. Vol. 2, No. 4. P. 70–84.

25. Marinescu D. C. Cloud computing: Theory and practice. San Francisco : Morgan Kaufmann Publishers, 2017.

26. Three Types Of Insider Threats Every Company Should Know. *Forbes*. URL: https://www.forbes.com/councils/forbestechcouncil/2025/12/05/three-types-of-insider-threats-every-company-should-know/ (дата звернення: 15.12.2025).

27. Building a security culture in the workplace — Bitwarden. URL: https://bitwarden.com/blog/building-a-cybersecurity-culture-in-the-workplace/ (дата звернення: 15.12.2025).

28. Людський фактор у кібербезпеці: головна загроза та як її нейтралізувати. URL: https://cases.media/article/lyudskii-faktor-u-kiberbezpeci-golovna-zagroza-ta-yak-yiyi-neitralizuvati (дата звернення: 15.12.2025).

29. 2025 Data Breach Investigations Report: Small- and Medium-Sized Business Snapshot Report — Verizon. URL:

https://www.verizon.com/business/resources/infographics/2025-dbir-smb-snapshot.pdf (дата звернення: 15.12.2025).

30. Strengthening your NIST framework: A guide to closing the human risk gap — NetClean. URL: https://www.netclean.com/knowledge/insights-and-data/the-hidden-gap-in-nist-a-guide-to-strengthening-your-cybersecurity-framework (дата звернення: 15.12.2025).

31. Pipkin D. L. Information security: Protecting the global enterprise. Upper Saddle River, New Jersey : Prentice Hall PTR, 2000.

32. Human Risk Management and ISO 27001 — OutThink. URL: https://outthink.io/community/thought-leadership/blog/Human-Risk-Management-and-ISO-27001/ (дата звернення: 15.12.2025).

33. Creating a Company Culture for Security: What Actually Works. URL: https://hoxhunt.com/blog/creating-a-company-culture-for-security (дата звернення: 15.12.2025).

34. How to Build a Strong Cybersecurity Culture in Your Organization — Dataprise. URL: https://www.dataprise.com/resources/blog/how-to-build-a-strong-cybersecurity-culture-in-your-organization/ (дата звернення: 15.12.2025).

35. What real-world data reveals about the effectiveness of phishing simulations — SoSafe. URL: https://sosafe-awareness.com/blog/real-world-data-effectiveness-phishing-simulations/ (дата звернення: 15.12.2025).

36. Кіберстійкість через обізнаність: як Закон № 4336-IX змінює підходи до навчання у держсекторі. URL: https://cip.gov.ua/ua/news/kiberstiikist-cherez-obiznanist-yak-zakon-4336-ikh-zminyuye-pidkhodi-do-navchannya-u-derzhsektori (дата звернення: 15.12.2025).

37. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: https://ips.ligazakon.net/document/T102297 (дата звернення: 15.12.2025).

38. Про захист персональних даних : роз'яснення законодавства від 04.08.2022. URL: https://ips.ligazakon.net/document/JI05379B (дата звернення: 15.12.2025).

39. Про затвердження Вимог з кібербезпеки паливно-енергетичного сектору критичної інфраструктури : наказ від 15.12.2022 № 417. URL: https://zakononline.ua/documents/show/516460___794612 (дата звернення: 15.12.2025).

40. Кібербезпека та захист критичної інфраструктури — Портал управління знаннями. URL: https://pdp.nacs.gov.ua/courses/kiberbezpeka-ta-zakhyst-krytychnoi-infrastruktury-52 (дата звернення: 15.12.2025).

41. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України : постанова Правління Національного банку України від 28.09.2017 № 95. URL: https://ips.ligazakon.net/document/PB17146 (дата звернення: 15.12.2025).

42. Національний банк посилює вимоги до інформаційної безпеки та кіберзахисту в банках України. URL: https://bank.gov.ua/ua/news/all/natsionalniy-bank-posilyuye-vimogi-do-informatsiynoyi-bezpeki-ta-kiberzahistu-v-bankah-ukrayini (дата звернення: 15.12.2025).

43. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT) : ДСТУ ISO/IEC 27001:2015. URL: https://www.assistem.kiev.ua/doc/dstu_ISO-IEC_27001_2015.pdf (дата звернення: 15.12.2025).

44. Критерії оцінювання компетентності фахівців за кваліфікацією «Спеціаліст систем менеджменту інформаційної безпеки» : ДСТУ ISO/IEC 27001:2015 (ISO/IEC 27001:2013, IDT), ISO/IEC 27001:2013, ISO/IEC 27001:2022. URL: https://uaq-pcb.com/docs/f5580.pdf (дата звернення: 15.12.2025).

45. Освітня програма «Кібербезпека об’єктів критичної інфраструктури». 2024. URL: https://eog.kname.edu.ua/uk/osvitni-prohramy/bakalavr/kiberbezpeka (дата звернення: 15.12.2025).

46. Kish D., Carpenter P. Forecast Snapshot: Security Awareness Computer-Based Training, Worldwide. Gartner Research. ID G00324277. March 2017.

47. Othonas S., Fysarakis K., Spanoudakis G., Koshutanski H., Damiani E., Beckers K., Wortmann D., Bravos G., Ioannidis M. The TREAT-ARREST Cyber-Security Training Platform. In: Proceedings of the 1st Model-driven Simulation and Training Environments for Cybersecurity (MSTEC). Luxembourg, 27 September 2019.

48. Top 10 Cybersecurity Training Software Solutions for 2025. URL: https://www.paradisosolutions.com/blog/top-cybersecurity-training-software-solutions/ (дата звернення: 15.12.2025).

49. Why SIEM, SOC & SOAR Integration Is Critical for Cybersecurity. URL: https://emtech.ae/siem-soc-soar-integration-guide/ (дата звернення: 15.12.2025).

50. Johnstone M. N. Threat modelling with STRIDE and UML. In: Proceedings of the 8th Australian Information Security Management Conference (AISM). Perth, Western Australia, 30 November 2010. P. 18–27.

51. Chapter 1. Machine Learning Applications in Evaluation. URL: https://ieg.worldbankgroup.org/evaluations/machine-learning-evaluative-synthesis/chapter-1-machine-learning-applications (дата звернення: 15.12.2025).

52. CIRO Model: The Definitive Guide. URL: https://kodosurvey.com/blog/ciro-model-definitive-guide (дата звернення: 15.12.2025).

53. What is Clickstream Analysis? URL: https://www.macrometa.com/articles/what-is-clickstream-analysis (дата звернення: 15.12.2025).

54. New Study Reveals Gaps in Common Types of Cybersecurity Training. URL: https://cs.uchicago.edu/news/new-study-reveals-gaps-in-common-types-of-cybersecurity-training/ (дата звернення: 15.12.2025).

55. Ho G., et al. Understanding the Efficacy of Phishing Training in Practice. In: Proceedings of the IEEE Symposium on Security and Privacy (SP). San Francisco, CA, USA, 2025. P. 37–54. DOI: 10.1109/SP61157.2025.00076.

56. 2025 Phishing By Industry Benchmark Report. KnowBe4. URL: https://www.knowbe4.com/resources/reports/phishing-by-industry-benchmarking-report (дата звернення: 15.12.2025).

57. Steves M., Greene K., Theofanos M. Categorizing human phishing difficulty: a Phish Scale. Journal of Cybersecurity. 2020. Vol. 6, no. 1. Article tyaa009. DOI: https://doi.org/10.1093/cybsec/tyaa009.

58. What's a Good Phishing Simulation Click Rate? It's Not What You Think. URL: https://cybersierra.co/blog/good-phishing-simulation-click-rate/ (дата звернення: 15.12.2025).

59. Security Awareness Training Statistics 2025 [100+ Studies]. Brightside AI Blog. URL: https://www.brside.com/blog/security-awareness-training-statistics-2025-100-studies (дата звернення: 15.12.2025).

60. Why Enterprises Are Moving from Generic Cyber Training to Cyber Ranges. OffSec. URL: https://www.offsec.com/blog/enterprise-cyber-training-ranges/ (дата звернення: 15.12.2025).

61. Chaudhary S., Gkioulos V., Katsikas S. Developing metrics to assess the effectiveness of cybersecurity awareness program. Journal of Cybersecurity. 2022. Vol. 8, no. 1. Article tyac006. DOI: https://doi.org/10.1093/cybsec/tyac006.

62. Top AI Risk Training Platforms & Tools for 2025. Adaptive Security. URL: https://www.adaptivesecurity.com/blog/ai-security-training-platform-buying-guide (дата звернення: 15.12.2025).

63. Challenges and Risks Associated with AI-Driven Cybersecurity. Euro Training. URL: https://www.eurotraining.com/ai/015-03-Challenges-and-Risks-Associated-with-AI-Driven-Cybersecurity.php (дата звернення: 15.12.2025).

64. AI Risks: Exploring the Critical Challenges of Artificial Intelligence. Lakera. URL: https://www.lakera.ai/blog/risks-of-ai (дата звернення: 15.12.2025).

65. 70 Social Engineering Statistics for 2025. Spacelift. URL: https://spacelift.io/blog/social-engineering-statistics (дата звернення: 12.12.2025).

66. Security Awareness Training: Examples, Metrics & Frameworks (2025). Hoxhunt. URL: https://hoxhunt.com/guide/security-awareness-training (дата звернення: 16.12.2025).

67. Phishing Simulation Tools. Ironscales. URL: https://ironscales.com/guides/phishing-awareness-training/phishing-simulation-tools (дата звернення: 18.12.2025).