КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Автоматизації і інформаційних технологій
(факультет)

Кібербезпеки та комп'ютерної інженерії
(назва випускової кафедри)

КВАЛІФІКАЦІЙНА РОБОТА
ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ БАКАЛАВР

на тему:

Сценарії соціальної інженерії для перевірки стійкості персоналу до фішингових атак

Євтушенко Даніїл Юрійович
(прізвище, ім’я та по батькові здобувача повністю)

Київ 2026 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Автоматизації і інформаційних технологій
(факультет)

Кібербезпеки та комп'ютерної інженерії
(назва кафедри)

ЗАТВЕРДЖУЮ

Завідувач кафедри

Делембовський М. М.

„___” _____2026 року

КВАЛІФІКАЦІЙНА РОБОТА

ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ БАКАЛАВР

Сценарії соціальної інженерії для перевірки стійкості персоналу до фішингових атак
(назва)

Я як здобувач вищої освіти КНУБА розумію і підтримую політику закладу з академічної доброчесності. Я не надавав(-ла) і не одержував(-ла) недозволену допомогу під час підготовки цієї роботи. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

Здобувач Євтушенко Данііл Юрійович

125 «Кібербезпека»

(спеціальність)

«Безпека інформаційних і комунікаційних систем»

(освітня програма)

Група БІКС-22

Керівник Делембовський М. М., доцент

Рецензент_____

(прізвище та ініціали)

Ідентичність підтверджую

Київ 2026р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Факультет: Автоматизації і інформаційних технологій

Випускова кафедра: Кібербезпеки та комп'ютерної інженерії

Ступінь вищої освіти: бакалавр

Спеціальність: 125 «Кібербезпека»

Освітня програма: «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ

Завідувач кафедри

Делембовський М.М.

„___”_____2026 року

З А В Д А Н Н Я

ДО ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ БАКАЛАВР

Євтушенко Даніїл Юрійович

(прізвище, ім’я та по батькові здобувача)

1. Тема роботи: Сценарії соціальної інженерії для перевірки стійкості персоналу до фішингових атак

затверджена наказом ректора КНУБА № 576/52-15/13.2/26 від «14» травня 2026 року

2. Керівник роботи Делембовський Максим Михайлович, кандидат технічних наук, доцент

(прізвище, ім’я та по батькові, науковий ступінь, вчене звання)

3. Термін подання здобувачем роботи до захисту_____

4. Зміст пояснювальної записки за розділами:

Р. 1. Аналіз предметної області соціальної інженерії та фішингу

Р. 2. Обґрунтування та розроблення лабораторного стенду

Р. 3. Реалізація та аналіз результатів

5. Календарний план виконання роботи:

Види робіт та їх зміст	Дата виконання
Розділ 1	05.05.2026 року
Розділ 2	16.05.2026 року
Розділ 3	24.05.2026 року
Остаточне оформлення роботи	01.06.2026 року
Направлення роботи для перевірки на плагіат	05.06.2026 року
Попередній захист роботи	11.06.2026 року
Направлення роботи на рецензування	13.06.2026 року

6. Дата видачі завдання _____

Керівник _____ Делембовський М. М

Здобувач _____ Євтушенко Д. Ю.

РЕЗЮМЕ (SUMMARY) *до кваліфікаційної випускної роботи здобувача:*		Євтушенко Даніїл Юрійович Yevtushenko Daniil Yurievich *(ПІБ здобувача українською та англійською)*
ЗВО	Київський національний університет будівництва і архітектури	
Тема (українською та англійською)	Сценарії соціальної інженерії для перевірки стійкості персоналу до фішинговиг атак Social engineering scenarios to test staff resilience to phishing attacks	
Освітній ступінь	Бакалавр	
Факультет	Автоматизації і інформаційних технологій	
Випускова кафедра	Кібербезпеки та комп'ютерної інженерії	
Спеціальність	125 "Кібербезпека"	
Освітня програма	Безпека інформаційних і комунікаційних систем	
Керівник	Делембовський Максим Михайлович	
Обсяг роботи:	*пояснювальна записка, стор.*	*розділів*	*Слайдів презентації*
	93	3	12
Розділ 1	Аналіз предметної області соціальної інженерії та фішингу	
Розділ 2	Обґрунтування та розроблення лабораторного стенду	
Розділ 3	Реалізація та аналіз результатів	
Висновки по роботі:	У кваліфікаційній роботі розроблено та апробовано лабораторний стенд для моделювання фішингових атак на базі платформи Gophish як інструменту практичного оцінювання та підвищення стійкості персоналу до методів соціальної інженерії.	
Ключові слова: *Keywords:*	інформаційна безпека, кібербезпека, соціальна інженерія, фішингові атаки, людський фактор, кіберобізнаність, симуляція фішингу, моделювання кіберзагроз. information security, cybersecurity, social engineering, phishing attacks, human factor, cyber awareness, phishing simulation, cyber threat modeling.	

Здобувач_Євтушенко Д.Ю._

Керівник:__Делембовський М.М._

"__" _____20___

АНОТАЦІЯ

Кваліфікаційну роботу присвячено проблематиці захисту інформаційних систем від соціотехнічних кіберзагроз шляхом практичного оцінювання поведінкових вразливостей персоналу. У межах дослідження спроєктовано та розгорнуто ізольований програмно-апаратний лабораторний стенд для проведення контрольованих симуляцій фішингових атак (phishing simulation). На основі розробленої моделі тестування реалізовано комплекс адаптивних сценаріїв соціальної інженерії, що дозволило безпечно та об'єктивно виміряти рівень стійкості користувачів за допомогою стандартизованих метрик компрометації. За результатами практичного експерименту виявлено критичні прогалини у кібергігієні працівників та сформовано комплекс організаційно-технічних рекомендацій щодо підвищення загального рівня інформаційної безпеки і впровадження систем безперервного навчання у корпоративне середовище.

Ключові слова: інформаційна безпека, кібербезпека, соціальна інженерія, фішингові атаки, людський фактор, кіберобізнаність, симуляція фішингу, моделювання кіберзагроз.

ABSTRACT

The qualification work is devoted to the problem of protecting information systems from socio-technical cyber threats through the practical assessment of personnel behavioral vulnerabilities. As part of the research, an isolated software and hardware laboratory stand was designed and deployed to conduct controlled phishing simulations. Based on the developed testing model, a set of adaptive social engineering scenarios was implemented, which allowed for the safe and objective measurement of user resilience using standardized compromise metrics. Based on the results of the practical experiment, critical gaps in the cyber hygiene of employees were identified, and a set of organizational and technical recommendations was formed to improve the overall level of information security and implement continuous learning systems in the corporate environment.

Keywords: information security, cybersecurity, social engineering, phishing attacks, human factor, cyber awareness, phishing simulation, cyber threat modeling.

ЗМІСТ

ВСТУП

Сучасний етап розвитку інформаційних технологій характеризується стрімкою цифровізацією суспільства, активним впровадженням хмарних сервісів, систем електронного документообігу та віддалених форм взаємодії між користувачами. Інформаційні системи стали невід'ємною частиною діяльності державних установ, підприємств, фінансових організацій та освітніх закладів. Разом із розширенням цифрового середовища постійно зростає кількість кіберзагроз, здатних завдати значної шкоди інформаційним ресурсам, репутації організацій та фінансовій стабільності. Аналіз сучасних досліджень у сфері кібербезпеки свідчить, що значна частина успішних кібератак пов'язана не з експлуатацією технічних вразливостей програмного забезпечення, а з використанням людського фактора. Незважаючи на постійне вдосконалення засобів захисту інформації, впровадження систем моніторингу безпеки, багатофакторної автентифікації та сучасних механізмів контролю доступу, користувач залишається одним із найбільш уразливих елементів інформаційної інфраструктури. Саме тому питання оцінювання рівня підготовки персоналу до сучасних кіберзагроз набуває особливої актуальності. Звіти провідних міжнародних організацій у сфері кібербезпеки, зокрема Verizon, ENISA, Microsoft та IBM, демонструють стабільно високий рівень успішності атак, спрямованих на взаємодію з користувачем. Такі атаки дозволяють зловмисникам отримувати доступ до корпоративних ресурсів, компрометувати облікові записи, викрадати конфіденційні дані та створювати передумови для подальшого розвитку складних кіберінцидентів. У зв'язку з цим виникає необхідність створення ефективних методів перевірки рівня кіберобізнаності персоналу та практичного оцінювання його готовності протидіяти сучасним загрозам. Одним із найбільш ефективних підходів до оцінювання стійкості користувачів є використання спеціалізованих лабораторних стендів, які дозволяють моделювати реалістичні сценарії кіберзагроз у контрольованому середовищі. Використання подібних рішень

забезпечує можливість проведення безпечних експериментів, отримання статистичних даних щодо поведінки користувачів та формування обґрунтованих рекомендацій щодо підвищення рівня інформаційної безпеки організації. Актуальність теми дипломної роботи зумовлена необхідністю розробки та практичного впровадження лабораторного стенду для моделювання фішингових атак, який дозволяє оцінювати рівень стійкості персоналу до соціотехнічних загроз, виявляти наявні вразливості в поведінці користувачів та підвищувати ефективність програм навчання з кібербезпеки. Об'єктом дослідження є процес забезпечення інформаційної безпеки організації в умовах впливу соціотехнічних кіберзагроз. Предметом дослідження є методи оцінювання стійкості персоналу до фішингових атак із використанням спеціалізованого лабораторного стенду. Метою роботи є розробка та практична реалізація лабораторного стенду для моделювання фішингових атак з метою оцінювання рівня стійкості персоналу до методів соціальної інженерії та формування рекомендацій щодо підвищення рівня інформаційної безпеки.

Для досягнення поставленої мети необхідно вирішити такі завдання:

– провести аналіз сучасних кіберзагроз, пов'язаних із використанням методів соціальної інженерії та фішингу;

– дослідити фактори, що впливають на ефективність фішингових атак;

– проаналізувати існуючі підходи до оцінювання рівня кіберобізнаності персоналу;

– розробити модель оцінювання стійкості користувачів до фішингових атак;

– спроєктувати та реалізувати лабораторний стенд для проведення контрольованих фішингових кампаній;

– провести експериментальне тестування користувачів та виконати аналіз отриманих результатів;

– розробити практичні рекомендації щодо підвищення рівня кібербезпеки персоналу.

Практична значущість роботи полягає у створенні лабораторного стенду, який може використовуватися для проведення навчальних та дослідницьких заходів у сфері кібербезпеки, оцінювання рівня підготовки персоналу та вдосконалення програм підвищення кіберобізнаності користувачів. Структура роботи складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків. У першому розділі розглянуто теоретичні аспекти соціальної інженерії та фішингових атак. У другому розділі описано процес проєктування та розробки лабораторного стенду. У третьому розділі наведено результати практичної реалізації стенду, проведеного тестування персоналу та аналіз отриманих результатів.

РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ ТА ФІШИНГУ

1.1 Аналіз предметної області

У сучасних умовах стрімкого розвитку інформаційних технологій та цифровізації практично всіх сфер діяльності суспільства питання інформаційної безпеки набувають критично важливого значення. Організації, державні установи, комерційні підприємства та приватні користувачі дедалі більше залежать від інформаційних систем, електронного документообігу, мережевих сервісів, хмарних технологій та дистанційної комунікації. Разом із розвитком технологій постійно еволюціонують і методи кібератак, які стають більш складними, прихованими та адаптивними. Одним із найбільш небезпечних та водночас ефективних методів впливу на інформаційні системи є соціальна інженерія. На відміну від традиційних технічних атак, які спрямовані на пошук вразливостей у програмному забезпеченні або мережевій інфраструктурі, соціальна інженерія орієнтується насамперед на людський фактор. Саме людина часто стає найслабшою ланкою системи безпеки, оскільки навіть за наявності сучасних засобів захисту користувач може несвідомо надати конфіденційну інформацію, перейти за шкідливим посиланням, відкрити заражений файл або виконати дії, які призводять до компрометації системи. Актуальність проблеми соціальної інженерії зумовлена тим, що більшість сучасних кібератак містять елементи психологічного впливу. Зловмисники активно використовують людські емоції, довіру, страх, поспіх, цікавість або авторитет для досягнення своїх цілей. Найбільш поширеними прикладами таких атак є фішинг, spear phishing, vishing, smishing, baiting, pretexting та інші методи маніпуляції користувачами. Особливу небезпеку становить той факт, що подібні атаки можуть бути успішними навіть у добре захищених інформаційних системах. З розвитком цифрових комунікацій соціальна інженерія отримала нові можливості для масштабування. Електронна пошта, соціальні мережі, месенджери,

корпоративні платформи та мобільні пристрої стали основними каналами проведення атак. Сучасні фішингові кампанії часто імітують офіційні повідомлення банків, державних органів, популярних сервісів або внутрішніх корпоративних ресурсів. Вони можуть містити підроблені вебсторінки, що візуально майже не відрізняються від оригіналів, або використовувати персоналізовану інформацію про жертву для підвищення рівня довіри. Проблема соціальної інженерії є особливо актуальною для організацій, які працюють із конфіденційними даними, фінансовими ресурсами або критичною інфраструктурою. Успішна атака може призвести до витоку інформації, фінансових втрат, порушення роботи систем, репутаційних збитків та навіть до повного компрометування корпоративної мережі. У багатьох випадках наслідки таких інцидентів можуть бути значно серйознішими, ніж наслідки технічних атак. Окрему увагу слід приділити тому, що традиційні засоби захисту, такі як антивірусне програмне забезпечення, міжмережеві екрани чи системи виявлення вторгнень, не здатні повністю нейтралізувати загрозу соціальної інженерії. Навіть найсучасніші технічні рішення не гарантують безпеки у випадку, якщо користувач самостійно передає свої облікові дані або запускає шкідливий файл. Саме тому важливу роль відіграє комплексний підхід до забезпечення кібербезпеки, який включає не лише технічний захист, але й підвищення рівня обізнаності персоналу, проведення навчань, тестувань та моделювання реальних сценаріїв атак. У сучасних організаціях дедалі частіше використовуються спеціалізовані платформи для проведення симуляцій фішингових атак та оцінки поведінки користувачів. Одним із таких інструментів є Gophish - програмне забезпечення з відкритим кодом, призначене для моделювання фішингових кампаній, збору статистики та аналізу реакції користувачів. Подібні рішення дозволяють безпечно тестувати рівень готовності персоналу до реальних атак та визначати найбільш уразливі аспекти інформаційної безпеки організації. Таким чином, предметна область дослідження охоплює проблематику соціальної інженерії як одного з ключових інструментів сучасних кібератак, методи психологічного впливу на

користувачів, способи реалізації фішингових кампаній, а також засоби моделювання та аналізу атак для оцінки рівня захищеності користувачів та інформаційних систем.

1.2 Постановка задачі дослідження

У сучасному інформаційному середовищі проблема протидії соціальній інженерії є однією з найскладніших задач у сфері кібербезпеки. Незважаючи на постійне вдосконалення засобів технічного захисту, людський фактор залишається найбільш вразливим елементом будь-якої інформаційної системи. Значна частина успішних кібератак відбувається саме через помилки користувачів, недостатній рівень обізнаності або психологічний вплив з боку зловмисників. Основною проблемою є те, що користувачі часто не здатні своєчасно розпізнати ознаки фішингових повідомлень або інших маніпулятивних сценаріїв. Зловмисники активно використовують методи маскування, підробки офіційних ресурсів, створення терміновості та імітації довірених джерел інформації. У результаті користувач може добровільно надати конфіденційні дані, що створює серйозну загрозу для безпеки інформаційної системи. У межах даного дослідження необхідно вирішити задачу аналізу ефективності методів соціальної інженерії та оцінки поведінки користувачів під час взаємодії з фішинговими сценаріями. Для цього потрібно реалізувати тестове середовище, яке дозволить моделювати реальні атаки, збирати статистичні дані та аналізувати результати проведених кампаній.

Ключовими задачами дослідження є:

- дослідження сутності та принципів соціальної інженерії;
- аналіз основних методів і сценаріїв фішингових атак;
- вивчення психологічних механізмів впливу на користувачів;
- аналіз сучасних інструментів для проведення phishing simulation;

- розгортання тестового середовища для моделювання фішингових кампаній;
- проведення експериментального тестування;
- аналіз статистичних результатів та оцінка рівня вразливості користувачів;
- формування рекомендацій щодо підвищення рівня інформаційної безпеки.

Особливістю даної задачі є необхідність поєднання технічного та поведінкового аналізу. Недостатньо лише виявити факт успішної атаки - важливо зрозуміти причини, через які користувач став жертвою маніпуляції, а також визначити ефективні методи підвищення його стійкості до подібних загроз. Результати дослідження мають практичне значення для організацій, які прагнуть підвищити рівень кібербезпеки та зменшити ризики, пов’язані з людським фактором. Використання тестових фішингових кампаній дозволяє виявляти слабкі місця у підготовці персоналу та формувати більш ефективні програми навчання й захисту.

1.3 Об’єкт, предмет та мета дослідження

Об’єктом дослідження є процеси забезпечення інформаційної безпеки організацій у контексті протидії атакам соціальної інженерії. Предметом дослідження є методи соціальної інженерії, механізми реалізації фішингових атак, поведінкові особливості користувачів під час взаємодії з підозрілими повідомленнями, а також програмні засоби для моделювання та аналізу phishing simulation кампаній. Метою дослідження є аналіз методів соціальної інженерії, дослідження ефективності фішингових атак та створення тестового середовища для моделювання phishing simulation з метою оцінки рівня вразливості користувачів і формування рекомендацій щодо підвищення інформаційної безпеки.

Для досягнення поставленої мети необхідно виконати такі завдання:

- провести аналіз сучасних загроз соціальної інженерії;
- дослідити класифікацію та принципи реалізації фішингових атак;
- розглянути психологічні аспекти впливу на користувачів;
- дослідити сучасні інструменти для phishing simulation;
- реалізувати тестовий стенд для проведення фішингових кампаній;
- провести тестування та збір статистичних даних;
- виконати аналіз отриманих результатів;
- сформувати рекомендації щодо підвищення рівня кібербезпеки та обізнаності користувачів.

Практична цінність дослідження полягає у можливості використання створеного підходу для навчання персоналу, проведення внутрішніх аудитів безпеки та оцінки готовності організації до сучасних кіберзагроз.

1.4 Огляд літературних джерел

Проблематика соціальної інженерії та фішингових атак активно досліджується як українськими, так і зарубіжними науковцями, фахівцями з кібербезпеки та міжнародними організаціями. Значна кількість сучасних досліджень присвячена аналізу людського фактора в системах інформаційної безпеки, психологічним механізмам маніпуляції та методам протидії соціотехнічним атакам. У науковій літературі соціальна інженерія розглядається як комплекс методів психологічного впливу, спрямованих на отримання конфіденційної інформації або доступу до інформаційних систем шляхом маніпуляції людьми. Дослідники наголошують, що основною причиною успішності подібних атак є не технічна недосконаліть систем, а людські помилки, неуважність або недостатній рівень підготовки користувачів. Вагомий внесок у розвиток тематики соціальної інженерії зробив Kevin

Mitnick, який у своїх роботах детально описував принципи психологічного впливу та практичні методи обходу систем захисту через маніпуляцію людьми. Його праці стали одними з базових джерел у сфері дослідження соціальної інженерії. Сучасні наукові джерела також приділяють значну увагу фішинговим атакам як найбільш поширеному виду соціальної інженерії. У багатьох роботах аналізуються механізми створення підроблених вебресурсів, методи маскування електронних листів, використання брендингу популярних сервісів та технології збору облікових даних користувачів. Окремий напрям досліджень стосується поведінкового аналізу користувачів. Автори зазначають, що успішність фішингових кампаній часто залежить від психологічного стану людини, рівня її цифрової грамотності, стресу, поспіху або довіри до авторитетних джерел. Саме тому сучасні методики захисту дедалі частіше включають елементи навчання персоналу, регулярні тренування та симуляцію реальних атак. У технічній літературі значна увага приділяється інструментам для phishing simulation. Одним із найбільш відомих рішень є Gophish, який широко використовується для моделювання фішингових кампаній, створення шаблонів листів, відстеження взаємодії користувачів та аналізу статистики. Використання подібних платформ дозволяє організаціям оцінювати рівень готовності персоналу до реальних атак без створення загрози для інформаційної інфраструктури. Також у літературних джерелах значна увага приділяється сучасним концепціям інформаційної безпеки, таким як Zero Trust, поведінкова аналітика, системи SIEM та SOAR, які дозволяють своєчасно виявляти підозрілу активність та реагувати на потенційні загрози. Однак навіть за наявності подібних технологій автори підкреслюють необхідність постійного підвищення рівня обізнаності користувачів, оскільки саме людина залишається ключовою ціллю більшості атак соціальної інженерії. Аналіз літературних джерел показує, що проблема соціальної інженерії є комплексною та охоплює як технічні, так і психологічні аспекти кібербезпеки. Незважаючи на значну кількість досліджень, питання ефективного поєднання технічних засобів захисту з

навчанням користувачів залишається актуальним і потребує подальшого вивчення. Отже, проведений аналіз предметної області та літературних джерел дозволяє перейти до детального розгляду поняття соціальної інженерії, її сутності, принципів функціонування та основних методів реалізації в сучасному кіберпросторі.

1.5 Поняття та сутність соціальної інженерії

У сучасному цифровому середовищі соціальна інженерія стала одним із найбільш небезпечних та ефективних інструментів реалізації кібератак. На відміну від класичних технічних методів злому, які спрямовані на пошук вразливостей у програмному забезпеченні, мережевих сервісах або апаратному забезпеченні, соціальна інженерія базується на маніпуляції людиною та використанні психологічних особливостей її поведінки. Основною ціллю зловмисника є не безпосереднє подолання технічного захисту, а отримання необхідної інформації або доступу через вплив на користувача. Соціальна інженерія являє собою сукупність методів психологічного впливу, спрямованих на введення людини в оману з метою отримання конфіденційної інформації, несанкціонованого доступу до систем або виконання певних дій, вигідних для зловмисника. У більшості випадків атакуючий використовує довіру, емоції, неуважність або недостатню обізнаність жертви. Таким чином, людина стає основним об’єктом атаки, а її поведінка - ключовим елементом успішної реалізації загрози. Сутність соціальної інженерії полягає у використанні людського фактора як найслабшої ланки системи безпеки. Навіть за наявності сучасних засобів технічного захисту користувач може самостійно надати зловмиснику пароль, код підтвердження, доступ до системи або іншу критично важливу інформацію. Саме тому атаки соціальної інженерії часто є значно ефективнішими за складні технічні методи злому, оскільки вони дозволяють обійти системи захисту без необхідності експлуатації програмних вразливостей. Особливістю соціальної інженерії є те, що вона поєднує елементи психології, комунікації,

поведінкового аналізу та інформаційних технологій. Зловмисник заздалегідь аналізує потенційну жертву, її інтереси, соціальні зв’язки, стиль спілкування, місце роботи, посаду або звички. Для цього можуть використовуватись соціальні мережі, відкриті бази даних, електронна пошта, форуми та інші джерела інформації. На основі зібраних даних створюється сценарій атаки, який виглядає максимально правдоподібним для конкретної людини або групи людей. У більшості випадків процес соціальної інженерії проходить декілька основних етапів. Першим етапом є збір інформації про потенційну жертву. Зловмисник намагається отримати якомога більше даних для формування довіри та підвищення ефективності атаки. Другим етапом є встановлення контакту з жертвою через електронну пошту, телефонний дзвінок, соціальні мережі або інші канали комунікації. Третім етапом стає безпосередня маніпуляція користувачем шляхом створення певної емоційної або психологічної ситуації. Завершальним етапом є отримання необхідної інформації або виконання жертвою потрібних дій. Одним із найпоширеніших видів соціальної інженерії є фішинг. Даний метод передбачає використання підроблених повідомлень, вебсайтів або електронних листів, які імітують офіційні ресурси банків, державних установ, соціальних мереж або корпоративних сервісів. Основною метою фішингових атак є отримання логінів, паролів, банківських даних або іншої конфіденційної інформації. У сучасних умовах фішингові кампанії стали надзвичайно складними та переконливими, оскільки використовують професійний дизайн, персоналізацію повідомлень та навіть елементи штучного інтелекту. Окрім класичного фішингу, існує велика кількість інших методів соціальної інженерії. До них належать spear phishing - цільові атаки на конкретну особу або організацію; vishing - телефонне шахрайство; smishing - атаки через SMS-повідомлення; baiting - використання приманки для заохочення користувача до певних дій; pretexting - створення вигаданого сценарію або легенди для отримання довіри; tailgating - фізичне проникнення до приміщень шляхом використання людської неуважності або ввічливості. Важливою особливістю

соціальної інженерії є її адаптивність. Зловмисники постійно змінюють сценарії атак відповідно до сучасних подій, інформаційного фону та суспільних тенденцій. Наприклад, під час глобальних криз, пандемій або військових конфліктів різко збільшується кількість фішингових кампаній, які використовують тематику гуманітарної допомоги, банківських виплат, державних сервісів або термінових повідомлень. Подібний підхід дозволяє підвищити рівень довіри та створити емоційний тиск на користувача. Соціальна інженерія активно використовується не лише кіберзлочинцями, але й у межах тестування систем безпеки. У сучасних організаціях проводяться контрольовані phishing simulation кампанії, які дозволяють оцінити рівень підготовки персоналу до реальних загроз. Для цього використовуються спеціалізовані платформи, серед яких однією з найбільш популярних є Gophish. Подібні інструменти дають можливість створювати тестові сценарії атак, аналізувати поведінку користувачів та формувати статистичні звіти щодо ефективності навчання персоналу. Небезпека соціальної інженерії полягає ще й у тому, що вона практично не має технічних обмежень. Якщо технічні атаки часто залежать від конкретних вразливостей або конфігурації системи, то соціальна інженерія базується на універсальних людських рисах: довірі, емоційності, бажанні допомогти, страху або цікавості. Саме тому навіть висококваліфіковані спеціалісти можуть стати жертвами добре підготовленої атаки. У сучасній кібербезпеці соціальна інженерія розглядається як комплексна міждисциплінарна проблема, яка потребує не лише технічних засобів захисту, але й глибокого розуміння людської психології. Ефективна протидія подібним атакам неможлива без регулярного навчання користувачів, розвитку критичного мислення, формування культури інформаційної безпеки та постійного аналізу поведінкових факторів. Саме психологічний аспект є основою більшості атак соціальної інженерії, оскільки головним інструментом впливу виступають людські емоції, когнітивні особливості та поведінкові реакції. Для розуміння причин успішності подібних атак необхідно детально розглянути психологічні механізми впливу на користувача, які

використовуються зловмисниками для маніпуляції свідомістю та прийняттям рішень.

1.6 Психологічні механізми впливу на користувача

Соціальна інженерія є не лише технічним або організаційним явищем, а насамперед складним психологічним процесом, у межах якого зловмисник впливає на мислення, емоції та поведінку людини з метою отримання необхідної інформації або спонукання її до виконання певних дій. Основною причиною успішності більшості атак соціальної інженерії є здатність атакуючого використовувати особливості людської психології, когнітивні помилки, емоційні реакції та поведінкові шаблони [4, 5]. Саме тому сучасні методи кіберзахисту дедалі більше орієнтуються не лише на технічну безпеку, але й на вивчення людського фактора. У науковій та технічній літературі питання психологічного впливу розглядається як один із ключових елементів соціальної інженерії. У працях Kevin Mitnick та Christopher Hadnagy [6, 7] зазначається, що головним інструментом соціального інженера є не програмне забезпечення чи технічні засоби, а здатність правильно впливати на поведінку людини. Зловмисник фактично маніпулює природними реакціями користувача, змушуючи його діяти швидко, емоційно та без належного аналізу ситуації. Одним із найважливіших психологічних механізмів є довіра. Люди за своєю природою схильні довіряти авторитетним джерелам, знайомим брендам, офіційним повідомленням або особам, які демонструють впевненість і компетентність. Саме тому зловмисники часто маскуються під представників банків, державних установ, технічної підтримки, керівництва компанії або популярних онлайн-сервісів. Використання офіційної символіки, логотипів, корпоративного стилю та формального тону значно підвищує рівень довіри користувача до повідомлення. Особливо ефективним є використання авторитету як психологічного інструменту впливу. Людина схильна підкорятися особам або структурам, які мають вищий статус або офіційні повноваження. Зловмисники активно експлуатують цей механізм, створюючи

сценарії, у яких користувач отримує повідомлення нібито від керівника організації, адміністратора системи або представника служби безпеки. У подібних ситуаціях жертва часто не ставить під сумнів отриману інформацію через страх порушити субординацію або створити конфлікт. Іншим важливим механізмом є створення відчуття терміновості. Людська психіка в умовах стресу або обмеженого часу значно гірше аналізує інформацію та приймає менш раціональні рішення. Саме тому фішингові повідомлення часто містять фрази на кшталт «Ваш акаунт буде заблоковано», «Необхідно терміново підтвердити дані», «Ваш платіж скасовано», «Виявлено підозрілу активність» або «Негайно змініть пароль». Подібні повідомлення викликають емоційну реакцію та змушують користувача діяти імпульсивно, не перевіряючи достовірність інформації. Страх є одним із найсильніших психологічних факторів, який активно використовується у соціальній інженерії. Людина прагне уникнути небезпеки або негативних наслідків, тому повідомлення про можливу втрату доступу до акаунту, фінансові проблеми, юридичні наслідки чи загрозу безпеці часто сприймаються особливо серйозно. У результаті користувач концентрується не на аналізі повідомлення, а на бажанні якнайшвидше усунути проблему. Не менш важливу роль відіграє цікавість. Люди природно прагнуть отримувати нову інформацію, особливо якщо вона стосується їх особисто або викликає сильний емоційний інтерес. Зловмисники використовують цей фактор, надсилаючи повідомлення із провокативними темами, наприклад: «Ваша фотографія», «Ви отримали новий документ», «Результати перевірки», «Конфіденційна інформація» або «Ваші дані були опубліковані». Бажання дізнатися зміст повідомлення часто переважає обережність, що призводить до переходу за шкідливими посиланнями або відкриття заражених вкладень. Окрему роль у соціальній інженерії відіграє психологічний механізм жадібності або прагнення до вигоди. Люди схильні позитивно реагувати на можливість отримати винагороду, подарунок, знижку або іншу перевагу. Саме тому популярними є фішингові кампанії, які обіцяють виграш, бонуси, повернення коштів або ексклюзивні пропозиції. У подібних

ситуаціях користувачі часто ігнорують базові правила безпеки через емоційне бажання отримати вигоду. Соціальні інженери також активно використовують механізм співчуття та бажання допомогти. Людина може надати інформацію або виконати певні дії, якщо вважає, що допомагає колезі, знайомому або клієнту. У корпоративному середовищі це особливо небезпечно, оскільки працівники часто взаємодіють із великою кількістю людей та прагнуть швидко вирішувати робочі питання. Зловмисники можуть представлятися новими співробітниками, технічною підтримкою або партнерами компанії для отримання доступу до інформації. Ще одним важливим фактором є звичка та автоматизм поведінки. У сучасному цифровому середовищі користувачі щоденно отримують десятки повідомлень, листів та сповіщень, через що значна частина дій виконується автоматично. Людина часто не аналізує URL-адресу сайту, адресу відправника або зміст повідомлення, якщо воно візуально нагадує знайомий сервіс. Саме ця автоматизація поведінки значно спрощує реалізацію фішингових атак. Психологічний вплив значно посилюється завдяки персоналізації. Сучасні атаки соціальної інженерії дедалі частіше використовують персональні дані користувача: ім’я, посаду, місце роботи, контакти, інтереси або інформацію із соціальних мереж. Коли повідомлення містить знайомі дані, рівень довіри автоматично підвищується. Саме тому spear phishing атаки є значно ефективнішими за масові фішингові кампанії. У сучасних умовах особливу небезпеку становить використання технологій штучного інтелекту для посилення психологічного впливу. Зловмисники можуть автоматично генерувати переконливі тексти, підробляти голос, створювати deepfake-відео або адаптувати повідомлення під конкретну аудиторію. Це значно ускладнює виявлення атак та підвищує їхню ефективність. Для систематизації наведених даних основні психологічні механізми та фактори впливу, які експлуатуються в рамках соціальної інженерії, узагальнено у таблиці 1.1.

Таблиця 1.1. Психологічні механізми та фактори впливу в соціальній інженерії

Психологічний механізм / Фактор впливу	**Суть механізму (психологічний аспект)**	**Приклади реалізації та мовні шаблони**
Довіра	Експлуатація природної схильності людей довіряти знайомим брендам, офіційним джерелам або компетентним особам.	Маскування під представників банків, держустанов чи техпідтримки. Використання офіційних логотипів та корпоративного стилю.
Авторитет	Підкорення особам або структурам із вищим статусом чи офіційними повноваженнями через страх порушити субординацію чи створити конфлікт.	Фейкові повідомлення нібито від керівника компанії, системного адміністратора чи представника служби безпеки.

Продовження таблиц таблиця 1.1.

Відчуття терміновості	Створення штучного дефіциту часу та стресу, за яких психіка гірше аналізує інформацію та приймає імпульсивні, нераціональні рішення.	Заклики до негайної дії: «Ваш акаунт буде заблоковано», «Необхідно терміново підтвердити дані», «Негайно змініть пароль».
Страх	Вплив на базове прагнення людини уникнути небезпеки, втрат або негативних юридичних та фінансових наслідків.	Сповіщення про несанкціоноване списання коштів, загрозу правових наслідків або критичне порушення безпеки профілю.
Цікавість	Використання природного бажання людини отримати нову, ексклюзивну або конфіденційну інформацію, яка викликає емоційний інтерес.	Листи із провокативними темами: «Ваша фотографія», «Ви отримали новий документ», «Ваші дані були опубліковані в мережі».

Продовження таблиц таблиця 1.1.

Жадібність / Прагнення до вигоди	Орієнтація на позитивну емоційну реакцію користувача щодо отримання матеріальної винагороди, легкого прибутку чи знижки.	Фішингові розсилки з обіцянками виграшів, безкоштовних бонусів, легкого заробітку, кешбеку чи ексклюзивних акційних пропозицій.
Співчуття / Бажання допомогти	Експлуатація альтруїстичних намірів людини допомогти колезі, клієнту чи знайомому, що послаблює пильність (особливо в робочому середовищі).	Звернення від імені «нового співробітника» чи партнера, якому терміново потрібна допомога з доступом для вирішення робочої проблеми.
Звичка та автоматизм поведінки	Використання щоденної рутини в цифровому середовищі, коли через великий потік повідомлень дії виконуються автоматично, без аналізу деталей.	Створення підроблених сторінок авторизації (інтерфейсів), які візуально повністю копіюють знайомі користувачу сервіси.

Продовження таблиц таблиця 1.1.

Персоналізація	Суттєве підвищення довіри до повідомлення за рахунок використання реальних персональних даних конкретної жертви.	Цільовий фішинг (spear phishing): звернення на ім'я, згадування точної посади, поточних проектів чи інформації з особистих соцмереж.
Штучний інтелект (ШІ)	Технологічне посилення психологічного тиску за допомогою високоточної автоматизованої адаптації контенту під жертву.	Генерація реалістичних текстів без помилок, клонування голосу (vishing), створення deepfake-відео.

Згідно з рекомендаціями National Institute of Standards and Technology у документах NIST SP 800-50 [3] та NIST SP 800-61 [2], одним із найважливіших напрямів захисту від соціальної інженерії є формування культури інформаційної безпеки та регулярне навчання персоналу. Аналогічний підхід підтримується стандартом International Organization for Standardization ISO/IEC 27001 [1], у якому підкреслюється необхідність врахування людського фактора під час побудови систем управління інформаційною безпекою. Сучасні аналітичні звіти компаній Verizon DBIR 2024 [8], CrowdStrike Global Threat Report [9], IBM X-Force Threat Intelligence Index [11] та Microsoft Digital Defense Report [12] демонструють, що значна частина сучасних інцидентів інформаційної безпеки прямо або опосередковано пов’язана з людським фактором. Це підтверджує, що навіть за наявності сучасних систем захисту користувач залишається основною ціллю атакуючих. Для протидії подібним загрозам використовуються спеціалізовані платформи для навчання та

поведінкового аналізу користувачів, зокрема KnowBe4 [21], Gophish [16], Microsoft Sentinel [23], IBM QRadar [20] та Splunk Enterprise Security [25]. Дані рішення дозволяють не лише моделювати атаки, але й аналізувати поведінку користувачів, виявляти ризикові дії та формувати адаптивні програми навчання. Таким чином, психологічні механізми є фундаментальною основою соціальної інженерії. Саме через вплив на емоції, когнітивні процеси та поведінкові особливості людини зловмисники отримують можливість обходити навіть складні технічні системи захисту. Розуміння цих механізмів є необхідною умовою для побудови ефективної системи інформаційної безпеки та формування стійкості користувачів до сучасних кіберзагроз. Однак для повного розуміння небезпеки соціальної інженерії недостатньо лише аналізу психологічних методів впливу. Важливо також дослідити, чому подібні атаки залишаються надзвичайно ефективними навіть у сучасних умовах розвитку кібербезпеки та які фактори сприяють їхній успішній реалізації. Саме тому наступним етапом дослідження є аналіз причин ефективності атак соціальної інженерії.

1.7 Причини ефективності атак соціальної інженерії

У сучасному цифровому середовищі атаки соціальної інженерії залишаються одними з найбільш ефективних та небезпечних методів компрометації інформаційних систем. Незважаючи на стрімкий розвиток засобів кіберзахисту, впровадження сучасних систем моніторингу, багаторівневих механізмів автентифікації та технологій штучного інтелекту, зловмисники продовжують успішно використовувати людський фактор для отримання доступу до конфіденційної інформації та корпоративних ресурсів. Причини високої ефективності соціальної інженерії мають комплексний характер і охоплюють психологічні, організаційні, технічні та соціальні аспекти [4, 5]. Одній з головних причин успішності атак соціальної інженерії є те, що людина є найменш захищеним елементом системи інформаційної безпеки. Технічні засоби захисту можуть бути модернізовані, оновлені або

замінені, однак людська поведінка залишається складною, емоційною та непередбачуваною. Саме тому більшість сучасних атак орієнтується не на безпосередній злом системи, а на маніпуляцію користувачем. У працях Kevin Mitnick та Christopher Hadnagy [6, 7] підкреслюється, що злам людини часто є простішим та ефективнішим, ніж злам складної інформаційної системи. Значну роль відіграє недостатній рівень обізнаності користувачів у сфере інформаційної безпеки. У багатьох організаціях працівники не мають достатніх знань щодо сучасних кіберзагроз, принципів роботи фішингових атак або методів перевірки достовірності електронних повідомлень. Документ National Institute of Standards and Technology NIST SP 800-50 [3] наголошує, що ефективна система кібербезпеки неможлива без регулярного навчання персоналу та формування культури інформаційної безпеки. Водночас у реальних умовах користувачі часто нехтують базовими правилами безпеки через поспіх, втому або впевненість у власній неуразливості. Ще однією важливою причиною є високий рівень психологічного впливу, який використовується у соціальній інженерії. Зловмисники навмисно створюють ситуації, що викликають страх, стрес, цікавість, довіру або відчуття терміновості. Під впливом емоцій людина значно гірше аналізує інформацію та частіше приймає імпульсивні рішення. Саме тому повідомлення із загрозою блокування акаунта, втратою доступу або фінансовими санкціями мають настільки високий рівень успішності. Суттєвим фактором є й автоматизація повсякденної цифрової поведінки. Сучасні користувачі щодня взаємодіють із великою кількістю повідомлень, сервісів, електронних листів та вебресурсів. Через це значна частина дій виконується автоматично без глибокого аналізу інформації. Люди звикають швидко відкривати листи, переходити за посиланнями, завантажувати вкладення або вводити облікові дані. Соціальні інженери активно використовують цю особливість, створюючи повідомлення, які зовні практично не відрізняються від легітимних. Окрему роль відіграє розвиток сучасних технологій, які значно спрощують підготовку та проведення атак. Якщо раніше для створення переконливих фішингових кампаній були

потрібні значні технічні знання, то сьогодні існує велика кількість відкритих інструментів та платформ, які автоматизують процес проведення атак. Одним із прикладів є Gophish [16] - спеціалізована платформа для моделювання фішингових кампаній, створення шаблонів електронних листів та збору статистики. Подібні інструменти можуть використовуватись як для навчання персоналу, так і зловмисниками для реалізації реальних атак. Високу ефективність соціальної інженерії також забезпечує доступність великої кількості персональної інформації у відкритих джерелах. Соціальні мережі, професійні платформи, форуми та публічні бази даних містять значний обсяг інформації про користувачів: місце роботи, посаду, контакти, коло спілкування, інтереси та навіть елементи повсякденного життя. На основі цих даних зловмисники можуть створювати highly personalized spear phishing атаки, які виглядають максимально правдоподібно для конкретної жертви. Сучасні аналітичні звіти підтверджують критичну роль людського фактора у більшості інцидентів інформаційної безпеки. Згідно з Verizon DBIR 2024 [8], значна частина витоків даних пов’язана саме з використанням методів соціальної інженерії, фішингу або компрометації облікових записів. Аналогічні тенденції описані у CrowdStrike Global Threat Report [9] та Microsoft Digital Defense Report [12], де зазначається, що атаки, орієнтовані на користувача, залишаються одним із головних інструментів сучасних кіберзлочинців. Особливо небезпечним фактором є використання штучного інтелекту та автоматизованих систем генерації контенту. Сучасні технології дозволяють створювати граматично правильні, стилістично переконливі та персоналізовані повідомлення практично без участі людини. Крім того, активно розвиваються технології deepfake, синтезу голосу та автоматичного аналізу поведінки користувачів. Це суттєво ускладнює процес розпізнавання атак та підвищує рівень їхньої ефективності. Ще однією причиною є недостатня увага організацій до поведінкової безпеки. Багато компаній концентруються переважно на технічних аспектах захисту: антивірусному програмному забезпеченні, міжмережевих екранах, системах IDS/IPS або

SIEM-рішеннях, однак приділяють недостатньо уваги підготовці персоналу. Стандарт International Organization for Standardization ISO/IEC 27001:2015 [1] прямо вказує на необхідність врахування людського фактора під час побудови систем управління інформаційною безпекою. Проте на практиці багато організацій досі не впроваджують регулярні phishing simulation кампанії або програми навчання користувачів. Важливим фактором також є складність своєчасного виявлення атак соціальної інженерії. На відміну від технічних атак, які можуть бути зафіксовані системами моніторингу або журналами подій, соціальна інженерія часто не залишає очевидних технічних слідів на початковому етапі. Якщо користувач добровільно передає свої облікові дані, система може сприймати подальші дії зловмисника як легітурну активність. Саме тому сучасні рішення дедалі частіше використовують поведінкову аналітику та технології UEBA. Для виявлення аномальної активності активно використовуються такі рішення, як Splunk User Behavior Analytics [26], Darktrace [19], Microsoft Defender XDR [22], Wazuh [27] та Cisco Secure [28]. Дані системи аналізують поведінку користувачів, виявляють нетипові дії та дозволяють оперативно реагувати на потенційні інциденти безпеки. Суттєвим фактором ефективності соціальної інженерії є також низька вартість проведення атак порівняно з потенційними результатами. Для реалізації фішингової кампанії часто достатньо доменного імені, поштового сервера та готових шаблонів повідомлень. При цьому успішна атака може призвести до значних фінансових втрат, витоку конфіденційної інформації або повної компрометації корпоративної мережі. Саме через високу рентабельність подібні атаки залишаються надзвичайно популярними серед кіберзлочинців. У сучасному кіберпросторі соціальна інженерія фактично стала універсальним інструментом для реалізації різних типів загроз: від масового фішингу до цільових атак на критичну інфраструктуру або державні установи. Її ефективність базується на поєднанні психологічного впливу, недостатньої підготовки користувачів, доступності інформації та стрімкого розвитку технологій. Таким чином, причини ефективності атак соціальної інженерії

мають комплексний характер та охоплюють як людські, так і технологічні фактори. Саме через це боротьба з подібними загрозами потребує багаторівневого підходу, який включає технічний захист, навчання персоналу, поведінкову аналітику та постійне вдосконалення політик інформаційної безпеки. Оскільки соціальна інженерія охоплює велику кількість різних методів і сценаріїв впливу на користувача, для подальшого дослідження необхідно систематизувати існуючі типи атак та розглянути їхні особливості, принципи реалізації й характерні ознаки. Саме тому наступним етапом роботи є розгляд класифікації атак соціальної інженерії. Ось ваш текст підрозділу 1.8 із правильно розставленими посиланнями на літературу у квадратних дужках відповідно до академічних вимог та наданого вами списку джерел:

1.8 Класифікація атак соціальної інженерії

Соціальна інженерія є комплексним напрямом у сфері кіберзагроз, який охоплює велику кількість методів психологічного впливу на людину з метою отримання конфіденційної інформації, доступу до інформаційних систем або спонукання користувача до виконання певних дій. У сучасному цифровому середовищі атаки соціальної інженерії постійно еволюціонують, адаптуються до нових технологій, змінюють канали поширення та методи впливу. Саме тому для ефективного розуміння природи подібних загроз важливо систематизувати існуючі типи атак та визначити їхні особливості. У сучасній науковій літературі та практиці кібербезпеки класифікація атак соціальної інженерії здійснюється за різними критеріями: за способом комунікації, методом психологічного впливу, рівнем персоналізації, каналом доставки, технічними особливостями реалізації та характером взаємодії із жертвою. У працях Kevin Mitnick та Christopher Hadnagy [6, 7] підкреслюється, що ефективність соціальної інженерії базується саме на здатності комбінувати різні психологічні та технічні методи впливу залежно від цільової аудиторії. Однією з основних категорій є атаки, що здійснюються через електронну пошту. Саме електронна пошта залишається одним із найпоширеніших каналів

реалізації соціальної інженерії через її доступність, масштабованість та можливість масового розповсюдження повідомлень. Найбільш типовим прикладом є фішинг - розсилання підроблених листів, які імітують офіційні повідомлення банків, державних установ, корпоративних сервісів або популярних онлайн-платформ. Метою таких атак є отримання логінів, паролів, банківських реквізитів або іншої конфіденційної інформації. Окремим видом є spear phishing - цільовий фішинг, орієнтований на конкретну особу, компанію або групу користувачів. На відміну від масових фішингових кампаній, spear phishing базується на попередньому зборі інформації про жертву. Зловмисники використовують персональні дані, службову інформацію, соціальні зв’язки та особливості корпоративної структури для створення максимально переконливого сценарію атаки. Подібні атаки є значно небезпечнішими, оскільки рівень довіри до персоналізованих повідомлень суттєво вищий. Ще одним різновидом є whaling - атаки, спрямовані на керівників компаній, топменеджмент або осіб із високим рівнем доступу до корпоративних ресурсів. У таких випадках атакуючі можуть використовувати складні сценарії, пов’язані з фінансовими операціями, корпоративними документами або критично важливою інформацією. Компрометація облікового запису керівника часто призводить до масштабних наслідків для всієї організації. Окрему категорію становлять атаки через телефонний зв’язок, відомі як vishing. У межах таких атак зловмисники телефонують жертві та представляються співробітниками банку, служби безпеки, технічної підтримки або державних органів. Основною метою є отримання конфіденційної інформації, кодів підтвердження, паролів або здійснення певних фінансових операцій. Особливу небезпеку vishing становить через прямий психологічний контакт із жертвою, який дозволяє зловмиснику оперативно реагувати на поведінку людини та посилювати емоційний тиск. Поширеним видом соціальної інженерії є smishing - атаки через SMS-повідомлення або месенджери. Подібні повідомлення зазвичай містять шкідливі посилання, повідомлення про виграш, блокування акаунта або необхідність термінового підтвердження

даних. Через обмежений обсяг тексту та високу довіру користувачів до мобільних повідомлень ефективність подібних атак залишається надзвичайно високою. Окрему категорію становлять атаки типу pretexting, які базуються на створенні вигаданої історії або сценарію для отримання довіри жертви. У межах подібних атак зловмисник створює певну легенду та поступово переконує користувача надати необхідну інформацію. Наприклад, атакуючий може представлятися працівником служби підтримки, співробітником відділу безпеки або новим працівником компанії. Головною особливістю pretexting є тривалий психологічний вплив та формування довірчих відносин із жертвою. Досить поширеним методом є baiting - атака з використанням приманки. У цьому випадку користувачу пропонується певна вигода або об’єкт, який викликає інтерес. Це можуть бути безкоштовні програми, файли, накопичувачі, бонуси або ексклюзивний контент. Основною метою є спонукання користувача до запуску шкідливого програмного забезпечення або переходу на підроблений ресурс. Людська цікавість та прагнення до вигоди роблять baiting одним із ефективних методів соціальної інженерії. Окремий тип становлять фізичні атаки соціальної інженерії. До них належить tailgating - несанкціоноване проникнення до захищених приміщень шляхом використання людської ввічливості або неуважності. Наприклад, зловмисник може пройти до офісу разом із працівником, який відкрив двері за допомогою електронної картки доступу. Подібні атаки демонструють, що соціальна інженерія виходить далеко за межі цифрового простору та активно використовується у фізичному середовищі. Сучасні атаки соціальної інженерії дедалі частіше комбінуються між собою та поєднуються з технічними методами компрометації. Наприклад, фішингове повідомлення може містити шкідливе вкладення, яке після відкриття встановлює malware або ransomware. Подібний підхід дозволяє атакуючим не лише отримати доступ до облікових даних, але й повністю скомпрометувати інформаційну систему. У сучасних аналітичних звітах Verizon DBIR 2024 [8], ENISA Threat Landscape [10] та IBM X-Force Threat Intelligence Index [11] підкреслюється, що соціальна інженерія є ключовим

елементом більшості сучасних кібератак. Особливо активно подібні методи використовуються під час атак на корпоративний сектор, фінансові установи, державні організації та критичну інфраструктуру. Важливим напрямом сучасної класифікації є поділ атак за рівнем автоматизації. Раніше більшість сценаріїв соціальної інженерії виконувались вручну, однак сьогодні активно використовуються автоматизовані системи розсилки, генерації повідомлень та поведінкового аналізу користувачів. Платформи на кшталт Gophish [16] дозволяють автоматизувати проведення phishing simulation кампаній, створювати шаблони листів, відстежувати реакцію користувачів та збирати статистику. Аналогічні можливості реалізовані у KnowBe4 [21] та інших сучасних рішеннях для навчання персоналу. У контексті сучасних систем захисту окрему увагу приділяють класифікації атак за способом виявлення та реагування. Для протидії атакам соціальної інженерії використовуються SIEM, SOAR, UEBA та XDR-рішення, серед яких IBM QRadar [20], Microsoft Sentinel [23], Splunk Enterprise Security [25], Darktrace [19] та Wazuh [27]. Дані системи дозволяють виявляти аномальну поведінку користувачів, аналізувати журнали подій та оперативно реагувати на інциденти безпеки. Значна увага проблемі класифікації атак приділяється і в нормативних документах. Стандарт International Organization for Standardization ISO/IEC 27001:2015 [1] визначає необхідність комплексного підходу до управління ризиками інформаційної безпеки, включаючи загрози, пов’язані з людським фактором. Документи National Institute of Standards and Technology NIST SP 800-50 [3] та NIST SP 800-61 [2] наголошують на важливості підготовки персоналу, класифікації інцидентів та впровадження процедур реагування на соціотехнічні атаки. Таким чином, атаки соціальної інженерії мають надзвичайно широкий спектр реалізації та можуть використовувати різні канали комунікації, психологічні механізми та технічні інструменти. Їхня класифікація дозволяє краще зрозуміти принципи роботи сучасних кіберзагроз, визначити характерні ознаки конкретних типів атак та сформувати ефективні методи протидії. Попри велику кількість різновидів соціальної інженерії, саме фішинг сьогодні

залишається найбільш поширеним, універсальним та ефективним інструментом атак. Масовість використання електронної пошти, вебресурсів та цифрових сервісів зробила фішингові кампанії основним методом отримання конфіденційної інформації та первинного доступу до інформаційних систем. Саме тому наступним етапом дослідження є детальний розгляд фішингу як основного інструменту атак соціальної інженерії.

1.9 Фішинг як основний інструмент атак

У сучасному цифровому середовищі фішинг є одним із найбільш поширених, ефективних та небезпечних інструментів реалізації атак соціальної інженерії. Саме фішингові кампанії сьогодні становлять основу значної частини кіберзагроз, оскільки дозволяють зловмисникам отримувати конфіденційну інформацію, компрометувати облікові записи користувачів, поширювати шкідливе програмне забезпечення та здійснювати первинне проникнення до корпоративних інформаційних систем. Масовість використання електронної пошти, вебсервісів, соціальних мереж та мобільних технологій створила ідеальні умови для масштабування подібних атак. Фішинг являє собою метод соціальної інженерії, заснований на створенні підроблених повідомлень, вебресурсів або цифрових сервісів, які імітують легітимні джерела інформації з метою введення користувача в оману. Основною задачею атакуючого є змусити жертву добровільно передати конфіденційні дані, перейти за шкідливим посиланням, відкрити заражене вкладення або виконати інші дії, що призводять до компрометації системи безпеки. Особливість фішингу полягає у тому, що дана категорія атак орієнтується не на технічні вразливості програмного забезпечення, а на психологічні особливості людини. Саме тому фішингові атаки залишаються ефективними навіть у середовищах із високим рівнем технічного захисту. У працях Kevin Mitnick та Christopher Hadnagy [6, 7] зазначається, що головною ціллю фішингу є маніпуляція поведінкою користувача через використання довіри, страху, терміновості або цікавості. У більшості випадків фішингові атаки реалізуються через

електронну пошту. Користувач отримує повідомлення, яке візуально нагадує офіційний лист від банку, державної установи, корпоративного сервісу, соціальної мережі або іншого довіреного джерела. Подібні листи часто містять повідомлення про блокування акаунта, необхідність підтвердження особистих даних, фінансові операції, оновлення пароля або інші ситуації, які потребують термінової реакції. Основною метою є створення емоційного тиску та спонукання користувача до швидких дій без детального аналізу повідомлення. Фішингові кампанії можуть мати як масовий, так і цільовий характер. Масовий фішинг передбачає одночасне розсилання великої кількості повідомлень випадковим користувачам із розрахунком на те, що певний відсоток жертв виконає необхідні дії. Подібний підхід є відносно дешевим та простим у реалізації, що робить його популярним серед кіберзлочинців. Набагато небезпечнішим різновидом є spear phishing - цільові фішингові атаки, спрямовані на конкретну особу або організацію. У таких випадках атакуючий заздалегідь збирає інформацію про жертву: ім’я, посаду, місце роботи, корпоративну структуру, службові контакти або особисті інтереси. На основі цих даних формується персоналізований сценарій атаки, який виглядає максимально правдоподібно. Саме персоналізація значно підвищує рівень довіри до повідомлення та ефективність атаки. Окрему категорію становить whaling - атаки на керівництво компаній або осіб із привілейованим доступом. У подібних сценаріях зловмисники можуть імітувати повідомлення від фінансових партнерів, державних органів або внутрішніх підрозділів організації. Метою є отримання доступу до критично важливих ресурсів, фінансових операцій або корпоративної інформації. Фішинг також активно використовується як початковий етап складних багаторівневих атак. Отримавши облікові дані користувача або доступ до робочої станції, зловмисник може здійснювати lateral movement у корпоративній мережі, підвищувати привілеї, отримувати доступ до серверів, баз даних або систем управління. Саме тому фішингові атаки часто стають відправною точкою для ransomware-інцидентів, витоку даних або компрометації критичної

інфраструктури. Сучасні фішингові кампанії дедалі частіше поєднуються з використанням шкідливого програмного забезпечення. У повідомлення можуть вбудовуватись заражені вкладення у форматах PDF, DOCX, XLSX, ZIP або EXE. Після відкриття такого файлу на пристрій жертви може встановлюватися malware, spyware, trojan або ransomware. Таким чином фішинг стає не лише методом збору інформації, але й інструментом доставки шкідливого програмного забезпечення. У сучасних аналітичних звітах Verizon DBIR 2024 [8], CrowdStrike Global Threat Report [9], Microsoft Digital Defense Report [12] та IBM X-Force Threat Intelligence Index [11] підкреслюється, що фішинг залишається одним із головних методів первинного доступу до корпоративних систем. Значна частина сучасних кіберінцидентів починається саме з компрометації користувача через фішингове повідомлення. Особливо небезпечним є використання технологій штучного інтелекту для автоматизації фішингових кампаній. Сучасні генеративні моделі дозволяють створювати граматично правильні, стилістично переконливі та персоналізовані повідомлення різними мовами. Крім того, атакуючі активно використовують deepfake-технології, підробку голосу та автоматизовану генерацію контенту, що значно ускладнює розпізнавання атак. Важливу роль у розвитку фішингу відіграє доступність інструментів для автоматизації атак. Одним із найбільш відомих рішень є Gophish [16] - платформа з відкритим кодом, яка дозволяє створювати фішингові кампанії, формувати шаблони електронних листів, розгортати підроблені вебсторінки та аналізувати реакцію користувачів. У межах тестування безпеки подібні рішення використовуються для phishing simulation та оцінки готовності персоналу до реальних загроз. Для розгортання лабораторних середовищ та тестових стендів часто застосовуються Kali Linux [15] та VMware Workstation Pro [17], які дозволяють моделювати фішингові кампанії у безпечному ізольованому середовищі. Подібний підхід широко використовується під час навчання фахівців із кібербезпеки та проведення внутрішніх аудитів інформаційної безпеки. Значну увагу проблемі фішингу приділяють міжнародні стандарти та нормативні документи. Стандарт

International Organization for Standardization ISO/IEC 27001:2015 [1] визначає необхідність комплексного управління ризиками інформаційної безпеки, включаючи ризики, пов’язані з людським фактором та соціальною інженерією. Документи National Institute of Standards and Technology NIST SP 800-50 [3] та NIST SP 800-61 [2] підкреслюють важливість навчання персоналу, реагування на інциденти та створення програм підвищення обізнаності користувачів щодо фішингових загроз. Для протидії фішинговим атакам сучасні організації використовують комплексні системи захисту: SIEM, SOAR, XDR, системи поведінкової аналітики та рішення для аналізу електронної пошти. Серед найбільш поширених платформ можна виділити Microsoft Defender XDR [22], Microsoft Sentinel [23], IBM QRadar [20], Splunk Enterprise Security [25], Darktrace [19], Proofpoint [24] та CrowdStrike Falcon [18]. Дані рішення дозволяють аналізувати поведінку користувачів, виявляти фішингові повідомлення, блокувати шкідливу активність та оперативно реагувати на інциденти. Водночас технічний захист сам по собі не гарантує повної безпеки. Одним із ключових елементів протидії фішингу залишається навчання користувачів та формування культури інформаційної безпеки. Саме тому сучасні організації активно використовують phishing simulation платформи, серед яких KnowBe4 [21], для проведення тестових кампаній та оцінки рівня підготовки персоналу. Таким чином, фішинг сьогодні є основним інструментом реалізації атак соціальної інженерії через свою універсальність, низьку вартість, високий рівень ефективності та можливість масштабування. Постійний розвиток цифрових технологій, автоматизація процесів та активне використання психологічних механізмів впливу роблять фішингові атаки однією з головних загроз сучасної кібербезпеки. Для повного розуміння принципів роботи фішингових кампаній необхідно детально розглянути канали їх реалізації, а також методи маскування, які використовуються зловмисниками для обходу систем захисту та введення користувачів в оману. Саме тому наступним етапом дослідження є аналіз каналів реалізації та способів маскування фішингових атак.

1.10 Канали реалізації та способи маскування фішингових атак

У сучасному цифровому середовищі фішинг став одним із найбільш поширених та ефективних інструментів реалізації атак соціальної інженерії. Його головна небезпека полягає у здатності зловмисників використовувати різноманітні канали комунікації для доставки шкідливого контенту та водночас успішно маскувати атаки під легітимні повідомлення, сервіси або дії. Постійний розвиток інформаційних технологій, масове використання електронної пошти, соціальних мереж, мобільних пристроїв та хмарних платформ створили сприятливі умови для масштабування фішингових кампаній та ускладнили процес їх своєчасного виявлення. Одним із головних каналів реалізації фішингових атак залишається електронна пошта. Саме email-комунікація є найбільш популярним способом доставки фішингових повідомлень через простоту реалізації, можливість автоматизованої масової розсилки та високий рівень довіри користувачів до корпоративної електронної пошти. Зловмисники надсилають листи, які імітують офіційні повідомлення банків, державних установ, онлайн-сервісів, маркетплейсів або внутрішніх корпоративних систем. Подібні повідомлення часто містять посилання на підроблені вебсайти, заражені вкладення або заклики до термінових дій. Особливу небезпеку становлять spear phishing кампанії, які реалізуються через персоналізовані email-повідомлення. У цьому випадку атакуючі попередньо збирають інформацію про жертву: ім’я, посаду, місце роботи, контакти, професійні зв’язки та навіть стиль спілкування. На основі цих даних створюється максимально правдоподібне повідомлення, яке значно складніше розпізнати як шахрайське. Подібний підхід активно використовується під час атак на корпоративний сектор, фінансові установи та державні організації. Ще одним важливим каналом реалізації є SMS-повідомлення та мобільні месенджери. Подібний тип атак отримав назву smishing. У сучасних умовах мобільні пристрої стали невід’ємною частиною повсякденного життя, а користувачі часто мають вищий рівень довіри до повідомлень, отриманих

через телефон. Зловмисники використовують SMS із повідомленнями про блокування банківської картки, підтвердження доставки, отримання бонусів або необхідність термінового оновлення даних. Через обмежений обсяг тексту та звичку користувачів швидко реагувати на мобільні повідомлення ефективність smishing атак залишається дуже високою. Поширеним каналом реалізації фішингових атак стали соціальні мережі та месенджери. Платформи для спілкування дозволяють атакуючим створювати фальшиві акаунти, імітувати знайомих осіб або представників організацій та надсилати шкідливі повідомлення безпосередньо користувачам. Особливо небезпечними є атаки через професійні соціальні мережі, де користувачі публікують значний обсяг особистої та професійної інформації. Це дозволяє зловмисникам створювати highly personalized сценарії соціальної інженерії. Окрему категорію становлять фішингові атаки через вебресурси. У цьому випадку створюються підроблені вебсайти, які зовні майже повністю копіюють легітимні ресурси банків, державних сервісів, хмарних платформ або корпоративних порталів. Основною метою є отримання логінів, паролів, банківських реквізитів або іншої конфіденційної інформації. Сучасні технології веброзробки дозволяють створювати практично ідентичні копії оригінальних сайтів, через що навіть досвідчені користувачі можуть не помітити підробку. Особливої уваги заслуговують атаки через телефонний зв’язок, відомі як vishing. У межах таких атак зловмисники використовують прямий голосовий контакт із жертвою, представляючись працівниками банків, служб безпеки, державних органів або технічної підтримки. Основною перевагою vishing є можливість психологічного впливу в режимі реального часу. Атакуючий може адаптувати сценарій відповідно до реакції користувача, створювати додатковий тиск або маніпулювати емоціями людини. У сучасних умовах активно використовуються також QR-фішинг атаки. Зловмисники створюють підроблені QR-коди, які ведуть на фішингові ресурси або автоматично ініціюють шкідливі дії на мобільному пристрої. Подібні методи особливо активно поширилися після популяризації безконтактних платежів та

мобільних сервісів. Суттєву небезпеку становлять і фішингові атаки через хмарні сервіси. Зловмисники використовують підроблені сторінки авторизації популярних платформ, таких як корпоративні хмарні сховища, сервіси електронної пошти або системи дистанційної роботи. Через масове використання віддаленого доступу та хмарної інфраструктури подібні атаки стали одним із ключових інструментів компрометації корпоративних акаунтів. Окрім каналів реалізації, надзвичайно важливу роль у фішингових атаках відіграють методи маскування. Саме здатність приховувати справжню природу атаки робить фішинг настільки небезпечним та ефективним. Одним із найбільш поширених способів маскування є spoofing - підробка адреси відправника. У цьому випадку зловмисник формує лист таким чином, щоб він виглядав як повідомлення від легітимної організації або знайомого користувача. Широко використовується також маскування доменних імен. Атакуючі реєструють домени, які візуально схожі на офіційні ресурси. Наприклад, можуть використовуватись схожі символи, додаткові літери, інші доменні зони або Unicode-символи, які важко відрізнити візуально. Подібний метод дозволяє створювати підроблені вебсайти, що практично не відрізняються від оригіналів. Важливим методом є використання SSL/TLS-сертифікатів для фішингових сайтів. Багато користувачів помилково вважають, що наявність HTTPS-з'єднання автоматично гарантує безпечність ресурсу. Зловмисники активно використовують безкоштовні сертифікати для створення ілюзії легітимності фішингових вебресурсів. Сучасні фішингові кампанії також активно використовують графічне та стилістичне маскування. Повідомлення створюються з використанням офіційної символіки, корпоративного дизайну, логотипів, підписів та шаблонів реальних компаній. Часто копіюється навіть структура електронних листів, службові повідомлення та елементи інтерфейсу. Подібна візуальна правдоподібність значно підвищує рівень довіри користувачів. Окрему небезпеку становить використання технологій штучного інтелекту для автоматичного створення переконливих повідомлень. Сучасні AI-системи дозволяють генерувати

граматично правильні, стилістично адаптовані та персоналізовані тексти, які складно відрізнити від реального листування. Крім того, активно розвиваються технології deepfake та синтезу голосу, що створює нові ризики для телефонних та відеоатак соціальної інженерії. Згідно зі звітами Verizon DBIR 2024 [8], Microsoft Digital Defense Report [12] та ENISA Threat Landscape [10], фішинг залишається одним із основних каналів первинного проникнення до корпоративних мереж та компрометації облікових записів. Особливо активно подібні атаки використовуються для розповсюдження ransomware, викрадення даних та отримання доступу до хмарної інфраструктури. Для виявлення та протидії фішинговим атакам використовуються сучасні системи моніторингу та аналізу поведінки користувачів. До них належать Microsoft Defender XDR [22], Microsoft Sentinel [23], IBM QRadar [20], Darktrace [19], Splunk Enterprise Security [25] та Cisco Secure [28]. Дані рішення дозволяють аналізувати мережеву активність, виявляти аномалії та оперативно реагувати на підозрілі дії користувачів. Важливе місце займають також платформи для навчання персоналу та проведення phishing simulation кампаній, серед яких KnowBe4 [21] та Gophish [16]. Подібні інструменти дозволяють моделювати реальні сценарії атак, оцінювати поведінку користувачів та підвищувати рівень їхньої обізнаності у сфері інформаційної безпеки. Нормативні документи International Organization for Standardization ISO/IEC 27001:2015 [1] та рекомендації National Institute of Standards and Technology NIST SP 800-50 [3] і NIST SP 800-61 [2] підкреслюють необхідність комплексного підходу до захисту від соціальної інженерії, який повинен включати технічні засоби захисту, моніторинг інцидентів, навчання персоналу та формування культури інформаційної безпеки. Таким чином, сучасні фішингові атаки використовують широкий спектр каналів реалізації та складні методи маскування, що робить їх надзвичайно небезпечними навіть для добре захищених інформаційних систем. Їхня ефективність базується не лише на технічних інструментах, але й на здатності маніпулювати людською поведінкою та експлуатувати помилки користувачів. Саме людський фактор у

більшості випадків стає ключовою причиною успішності фішингових атак та інших методів соціальної інженерії. Навіть найсучасніші системи захисту можуть бути обійдені через неуважність, недостатню підготовку або психологічний вплив на користувача. Тому для повного розуміння проблематики соціальної інженерії необхідно детально розглянути роль людського фактора в системі інформаційної безпеки.

1.11 Роль людського фактора в системі інформаційної безпеки

У сучасних умовах розвитку цифрових технологій роль людського фактора в системі інформаційної безпеки набуває критично важливого значення. Незважаючи на постійне вдосконалення технічних засобів захисту, впровадження сучасних систем моніторингу, багаторівневих механізмів автентифікації та технологій штучного інтелекту, саме людина продовжує залишатися одним із найбільш уразливих елементів будь-якої інформаційної системи. Більшість сучасних кіберінцидентів прямо або опосередковано пов’язані з помилками користувачів, недостатнім рівнем обізнаності персоналу або порушенням політик безпеки. Людський фактор у сфері інформаційної безпеки охоплює сукупність поведінкових, психологічних, організаційних та соціальних аспектів діяльності людини, які можуть впливати на рівень захищеності інформаційних систем. На відміну від технічних компонентів, поведінка користувача не завжди є прогнозованою, а його рішення часто залежать від емоційного стану, рівня навантаження, стресу, втоми, мотивації або особистого досвіду. Саме ця особливість робить людину ключовою ціллю атак соціальної інженерії. У працях Kevin Mitnick та Christopher Hadnagy [6, 7] підкреслюється, що найскладніші системи захисту можуть бути скомпрометовані через одну помилку користувача. Зловмисники активно використовують психологічні механізми впливу, маніпулюють довірою, страхом, терміновістю або цікавістю людини для отримання необхідної інформації чи доступу до системи. Таким чином, навіть за наявності сучасного технічного захисту людський фактор може нівелювати

ефективність усієї системи інформаційної безпеки. Однією з основних проблем є недостатній рівень підготовки користувачів у сфері кібербезпеки. У багатьох організаціях працівники не мають достатнього розуміння сучасних загроз, принципів роботи фішингових атак або правил безпечної роботи з інформацією. Через це користувачі можуть відкривати підозрілі вкладення, переходити за шкідливими посиланнями, використовувати слабкі паролі або передавати конфіденційну інформацію стороннім особам. Документ National Institute of Standards and Technology NIST SP 800-50 [3] наголошує, що формування культури інформаційної безпеки та регулярне навчання персоналу є критично важливими елементами системи захисту. У даному документі зазначається, що користувач повинен не лише знати правила безпеки, але й усвідомлювати потенційні наслідки власних дій. Аналогічний підхід підтримується стандартом International Organization for Standardization ISO/IEC 27001:2015 [1], який визначає необхідність врахування людського фактора під час побудови систем управління інформаційною безпекою. Особливу небезпеку становить так званий «ефект рутини». У сучасному цифровому середовищі користувачі щоденно взаємодіють із великою кількістю повідомлень, сервісів, електронних листів та інформаційних ресурсів. Через це значна частина дій виконується автоматично, без належного аналізу інформації. Людина звикає швидко відкривати вкладення, підтверджувати запити, вводити облікові дані або переходити за посиланнями, якщо вони зовні виглядають знайомими. Саме ця автоматизація поведінки активно використовується у фішингових кампаніях. Не менш важливим фактором є психологічний стан користувача. Втома, стрес, високий рівень навантаження або дефіцит часу суттєво знижують здатність людини аналізувати інформацію та приймати раціональні рішення. Саме тому зловмисники часто створюють ситуації терміновості або емоційного тиску, змушуючи жертву діяти швидко та імпульсивно. Важливу роль відіграє також рівень цифрової грамотності користувачів. Люди, які не мають достатніх знань про сучасні методи кібератак, значно частіше стають жертвами соціальної інженерії. Особливо це

стосується працівників, діяльність яких безпосередньо не пов’язана з інформаційними технологіями. У багатьох випадках користувачі не здатні відрізнити підроблений вебресурс від справжнього, не перевіряють адресу відправника електронного листа або не звертають уваги на ознаки компрометації повідомлення. Сучасні аналітичні звіти підтверджують критичну роль людського фактора у більшості інцидентів інформаційної безпеки. У Verizon DBIR 2024 [8] зазначається, що значна частина витоків даних та компрометацій облікових записів пов’язана саме з використанням соціальної інженерії та помилками користувачів. Аналогічні висновки містяться у Microsoft Digital Defense Report [12], IBM X-Force Threat Intelligence Index [11] та ENISA Threat Landscape [10], де людський фактор розглядається як один із ключових ризиків сучасної кібербезпеки. Суттєвою проблемою є також нехтування політиками безпеки. Навіть у добре захищених організаціях користувачі можуть використовувати прості паролі, повторно застосовувати однакові облікові дані, вимикати засоби захисту або передавати службову інформацію через незахищені канали зв’язку. Подібні дії часто пов’язані з бажанням спростити робочі процеси або зекономити час, однак саме вони створюють додаткові вразливості для атакуючих. Окрему увагу необхідно приділити внутрішнім загрозам. Людський фактор становить небезпеку не лише через помилки або необережність, але й через навмисні дії працівників. Внутрішні інциденти можуть бути пов’язані з витоком інформації, саботажем, перевищенням повноважень або співпрацею зі зловмисниками. Саме тому сучасні системи безпеки дедалі більше орієнтуються на контроль поведінки користувачів та моніторинг аномальної активності. Для мінімізації ризиків, пов’язаних із людським фактором, організації активно використовують системи поведінкової аналітики та рішення класу UEBA, SIEM, XDR і SOAR. Серед найбільш поширених платформ можна виділити Splunk User Behavior Analytics [26], Microsoft Sentinel [23], IBM QRadar [20], Darktrace [19], CrowdStrike Falcon [18] та Wazuh [27]. Дані рішення дозволяють аналізувати поведінку користувачів, виявляти

підозрілі дії та оперативно реагувати на потенційні загрози. Водночас технічні системи не здатні повністю усунути ризики, пов’язані з людським фактором. Саме тому важливим елементом сучасної інформаційної безпеки є формування культури кібергігієни. Працівники повинні регулярно проходити навчання, брати участь у тестових phishing simulation кампаніях та вивчати сучасні методи атак соціальної інженерії. Для цього активно використовуються спеціалізовані платформи, серед яких KnowBe4 [21] та Gophish [16]. Важливим напрямом є також створення чітких політик інформаційної безпеки, які регламентують порядок роботи з конфіденційною інформацією, використання електронної пошти, управління доступом та реагування на інциденти. Документ National Institute of Standards and Technology NIST SP 800-61 [2] підкреслює необхідність створення процедур реагування на інциденти безпеки та підготовки персоналу до дій у разі виявлення підозрілої активності. У сучасному кіберпросторі людський фактор фактично став центральним елементом системи інформаційної безпеки. Саме від рівня підготовки користувачів, їхньої уважності, дисципліни та обізнаності залежить ефективність більшості механізмів захисту. Тому сучасний підхід до кібербезпеки передбачає комплексне поєднання технічних рішень, організаційних заходів та постійного навчання персоналу. Таким чином, роль людського фактора в системі інформаційної безпеки є визначальною. Людина може виступати як найслабшою ланкою захисту, так і одним із ключових елементів протидії сучасним кіберзагрозам. Саме тому ефективний захист від фішингових атак та інших методів соціальної інженерії потребує не лише використання сучасних технологій, але й формування високого рівня обізнаності користувачів та розвитку культури інформаційної безпеки. Для забезпечення комплексного захисту інформаційних систем необхідно детально розглянути сучасні методи протидії фішинговим атакам, які включають технічні, організаційні та поведінкові механізми безпеки. Саме тому наступним етапом дослідження є аналіз методів захисту від фішингових атак.

1.12 Методи захисту від фішингових атак

Фішингові атаки залишаються одним із найбільш поширених та ефективних інструментів компрометації інформаційних систем. Постійне вдосконалення методів соціальної інженерії, поява нових каналів комунікації та використання сучасних технологій для маскування шкідливих повідомлень суттєво ускладнюють процес їх виявлення. Саме тому забезпечення захисту від фішингових атак потребує комплексного підходу, який поєднує організаційні, технічні та освітні заходи [4, 5].

Відповідно до вимог ДСТУ ISO/IEC 27001:2015 [1], ефективна система управління інформаційною безпекою повинна передбачати постійний контроль ризиків, пов’язаних із людським фактором, а також впровадження заходів щодо підвищення обізнаності користувачів. У випадку протидії фішинговим атакам така модель передбачає не лише застосування технічних засобів фільтрації повідомлень, але й формування належного рівня кіберобізнаності персоналу. Одним із найбільш поширених методів захисту є використання систем фільтрації електронної пошти. Сучасні поштові шлюзи аналізують повідомлення за великою кількістю параметрів, включаючи репутацію відправника, структуру вкладень, наявність підозрілих посилань та відповідність доменних записів політикам SPF, DKIM та DMARC. Такі механізми дозволяють блокувати значну частину фішингових повідомлень ще до їх потрапляння до поштової скриньки користувача. Важливу роль відіграють технології автентифікації електронної пошти. Використання протоколів SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) та DMARC (Domain-based Message Authentication, Reporting and Conformance) дозволяє підтверджувати автентичність відправника та значно ускладнює реалізацію атак із підміною адрес електронної пошти. Саме підробка корпоративних адрес є одним із найбільш поширених інструментів атак типу Business Email Compromise (BEC). Окреме місце серед методів захисту займають рішення класу Secure Email Gateway (SEG), які використовуються

для автоматизованого аналізу поштового трафіку. Подібні системи реалізовані в продуктах Proofpoint [24], Cisco Secure Email [28], Microsoft Defender for Office 365 [22] та інших корпоративних рішеннях. Вони використовують технології машинного навчання, поведінковий аналіз та механізми репутаційного контролю для виявлення підозрілих повідомлень. Суттєвого поширення набули сучасні системи класу XDR та SIEM, які забезпечують централізований моніторинг подій безпеки та дозволяють оперативно виявляти ознаки фішингових атак. Рішення Microsoft Defender XDR [22], Microsoft Sentinel [23], IBM QRadar [20], Splunk Enterprise Security [25] та Wazuh [27] дозволяють корелювати інформацію з різних джерел та автоматично формувати сповіщення про потенційні інциденти інформаційної безпеки. Важливим напрямом захисту є використання багатофакторної автентифікації (MFA). Навіть у випадку успішного викрадення облікових даних під час фішингової атаки додатковий фактор підтвердження суттєво ускладнює несанкціонований доступ до інформаційних ресурсів організації. Саме тому сучасні стандарти інформаційної безпеки рекомендують впроваджувати MFA для всіх критично важливих інформаційних систем. Не менш важливими є засоби захисту кінцевих точок (Endpoint Protection Platforms та Endpoint Detection and Response). Такі рішення дозволяють виявляти спроби запуску шкідливого програмного забезпечення, яке часто використовується як додатковий етап після успішної реалізації фішингової атаки. До подібних платформ належать CrowdStrike Falcon [18], Microsoft Defender for Endpoint [22] та інші сучасні EDR-рішення. Попри високу ефективність технічних засобів захисту, численні дослідження демонструють, що вони не здатні повністю усунути ризик успішного фішингу. Значна частина сучасних атак створюється індивідуально для конкретних організацій або користувачів, що дозволяє обходити автоматизовані механізми виявлення. Саме тому особливого значення набувають організаційні заходи безпеки. Одним із найефективніших організаційних механізмів є впровадження політик інформаційної безпеки. Такі документи повинні регламентувати порядок

роботи з електронною поштою, правила перевірки підозрілих повідомлень, процедури повідомлення про інциденти та відповідальність працівників за дотримання встановлених вимог. Наявність чітких процедур дозволяє значно скоротити кількість помилок користувачів під час взаємодії з потенційно небезпечними повідомленнями [2] Особливе місце серед методів захисту займає навчання персоналу. Відповідно до рекомендацій NIST SP 800-50 [3], ефективна система інформаційної безпеки повинна включати постійні програми підвищення обізнаності користувачів щодо актуальних кіберзагроз. Працівники повинні вміти розпізнавати ознаки фішингових повідомлень, перевіряти справжність посилань, оцінювати ризики відкриття вкладень та своєчасно повідомляти про підозрілі інциденти. Сучасним та найбільш ефективним підходом до навчання користувачів є проведення контрольованих фішингових кампаній (phishing simulation). Використання спеціалізованих платформ, таких як Gophish [16] або KnowBe4 [21], дозволяє моделювати реальні сценарії атак у безпечному середовищі та оцінювати рівень підготовки персоналу на практиці. Подібні тренування сприяють формуванню стійких навичок безпечної поведінки та дозволяють виявляти категорії користувачів, які потребують додаткового навчання. Таким чином, ефективний захист від фішингових атак можливий лише за умови комплексного використання технічних, організаційних та освітніх заходів. Жоден окремий механізм не здатний повністю усунути ризики, пов'язані з людським фактором. Саме тому сучасні підходи до інформаційної безпеки дедалі більше орієнтуються на поєднання засобів автоматизованого захисту з регулярним навчанням персоналу та практичним оцінюванням рівня його кіберобізнаності [1, 3]. Логічним продовженням розгляду проблематики захисту від фішингових атак є аналіз підходів до оцінювання ефективності таких заходів. Навіть за наявності сучасних систем захисту та програм навчання виникає питання визначення реального рівня готовності користувачів до протидії соціотехнічним загрозам. Саме тому наступний підрозділ присвячено

дослідженню проблематики оцінювання стійкості персоналу до фішингових атак та методів соціальної інженерії.

1.13 Проблематика оцінювання стійкості персоналу

У сучасних умовах цифровізації суспільства та стрімкого розвитку кіберзагроз питання оцінювання стійкості персоналу до атак соціальної інженерії набуває критично важливого значення. Незважаючи на активний розвиток технічних засобів захисту, саме людський фактор продовжує залишатися одним із головних джерел ризику для інформаційної безпеки організацій. Більшість сучасних кібератак прямо або опосередковано орієнтовані на маніпуляцію поведінкою користувача, а тому рівень підготовки персоналу та його здатність протистояти соціотехнічним загрозам стають важливими елементами комплексної системи кібербезпеки. Проблематика оцінювання стійкості персоналу полягає у складності визначення реального рівня готовності користувачів до сучасних атак соціальної інженерії. На відміну від технічних систем, ефективність яких можна оцінити за допомогою конкретних параметрів, людська поведінка є динамічною, залежить від психологічного стану, зовнішніх факторів, рівня навантаження, досвіду та багатьох інших змінних. Саме тому визначення реального рівня стійкості користувачів є складною міждисциплінарною задачею, яка поєднує технічні, психологічні та організаційні аспекти. У сучасній кібербезпеці персонал розглядається не лише як потенційна вразливість, але й як активний елемент системи захисту. Документ National Institute of Standards and Technology NIST SP 800-50 [3] наголошує, що ефективна програма інформаційної безпеки повинна включати постійне навчання користувачів, оцінювання їхньої обізнаності та перевірку готовності до реагування на інциденти. Аналогічний підхід підтримується стандартом International Organization for Standardization ISO/IEC 27001:2015 [1], у якому людський фактор визначається одним із ключових елементів системи управління інформаційною безпекою. Однією з основних проблем оцінювання стійкості персоналу є відсутність

універсальних критеріїв оцінки. У більшості випадків організації використовують тестування знань, навчальні курси або симуляції фішингових атак, однак подібні методи не завжди дозволяють об’єктивно оцінити поведінку користувача в реальних умовах. Людина може демонструвати високі результати під час тестування, але при цьому стати жертвою реальної атаки через стрес, поспіх або емоційний вплив. Суттєвою проблемою є також різниця між теоретичною обізнаністю та практичною поведінкою користувачів. Багато працівників знають базові правила кібергігієни, однак не застосовують їх на практиці. Наприклад, користувач може розуміти небезпеку фішингових повідомлень, але все одно перейти за шкідливим посиланням через втому, автоматизм дій або високий рівень навантаження. Саме тому традиційні методи навчання часто виявляються недостатньо ефективними без проведення практичних тестувань та моделювання реальних сценаріїв атак. Окрему складність створює психологічний аспект поведінки людини. Реакція користувача на атаку соціальної інженерії значною мірою залежить від емоційного стану, рівня стресу, авторитету джерела повідомлення та контексту ситуації. Зловмисники активно використовують терміновість, страх, цікавість або довіру для маніпуляції жертвою. Через це навіть досвідчені користувачі можуть допускати помилки в умовах психологічного тиску. У працях Christopher Hadnagy та Kevin Mitnick [6, 7] зазначається, що головною перевагою соціальної інженерії є непередбачуваність людської поведінки. Саме тому ефективність атак часто залежить не від складності технічних методів, а від здатності атакуючого правильно обрати момент, психологічний підхід та форму подання інформації. Важливою проблемою є також швидка еволюція сучасних фішингових кампаній. З розвитком цифрових технологій атакуючі почали використовувати персоналізовані сценарії, автоматизовану генерацію повідомлень, штучний інтелект та deepfake-технології. Це суттєво ускладнює процес оцінювання готовності персоналу, оскільки користувачі повинні адаптуватися до нових типів загроз та постійно оновлювати свої знання. Згідно з даними Verizon DBIR 2024 [8], значна частина сучасних

інцидентів інформаційної безпеки пов’язана саме з помилками користувачів або успішними фішинговими атаками. Аналогічні висновки містяться у Microsoft Digital Defense Report [12], CrowdStrike Global Threat Report [9] та IBM X-Force Threat Intelligence Index [11], де людський фактор визначається одним із головних ризиків сучасної кібербезпеки. Серйозною проблемою є також недостатня регулярність оцінювання персоналу. У багатьох організаціях навчання проводиться формально або епізодично, без систематичного аналізу результатів та адаптації програм під сучасні загрози. Через це рівень обізнаності користувачів поступово знижується, а працівники перестають сприймати інформаційну безпеку як важливий елемент своєї професійної діяльності. Окремої уваги потребує проблема прихованого людського фактора. Навіть якщо користувач не став жертвою атаки безпосередньо, його дії можуть створювати додаткові ризики для організації. Використання слабких паролів, повторне застосування облікових даних, передача службової інформації через незахищені канали зв’язку або нехтування політиками безпеки значно підвищують імовірність успішної компрометації системи. У сучасних умовах для оцінювання стійкості персоналу дедалі активніше використовуються phishing simulation платформи. Подібні системи дозволяють моделювати реальні сценарії атак та аналізувати поведінку користувачів у контрольованому середовищі. Одним із найбільш відомих рішень є Gophish [16], який дозволяє створювати фішингові кампанії, відстежувати дії користувачів, збирати статистику та оцінювати рівень підготовки персоналу. Аналогічні функції реалізовані у KnowBe4 [21], яка спеціалізується на навчанні персоналу та тестуванні стійкості до соціальної інженерії. Важливим напрямом сучасного оцінювання є використання поведінкової аналітики та систем моніторингу активності користувачів. Для цього застосовуються рішення класу SIEM, XDR та UEBA, серед яких Splunk User Behavior Analytics [26], IBM QRadar [20], Microsoft Sentinel [23], Darktrace [19] та Wazuh [27]. Дані системи дозволяють аналізувати поведінку користувачів, виявляти аномальну активність та оцінювати потенційні ризики. Ще однією проблемою є баланс між контролем

та довірою до персоналу. Надмірний моніторинг користувачів може негативно впливати на психологічний клімат у колективі та створювати атмосферу недовіри. Саме тому сучасні підходи до оцінювання стійкості персоналу повинні поєднувати технічний контроль із навчанням, мотивацією та формуванням культури безпеки. Важливу роль у забезпеченні ефективності оцінювання відіграє створення системи постійного вдосконалення. Оцінювання стійкості персоналу не повинно бути одноразовою процедурою. Через постійний розвиток кіберзагроз організації повинні регулярно оновлювати сценарії тестувань, адаптувати навчальні матеріали та аналізувати поведінкові тенденції користувачів. Документ National Institute of Standards and Technology NIST SP 800-61 [2] також підкреслює необхідність створення механізмів реагування на інциденти, пов’язані з людським фактором. У сучасних умовах важливо не лише виявити факт помилки користувача, але й оперативно локалізувати наслідки інциденту, провести аналіз причин та впровадити додаткові заходи захисту. Таким чином, проблематика оцінювання стійкості персоналу є складною комплексною задачею, яка охоплює психологічні, поведінкові, організаційні та технічні аспекти інформаційної безпеки. Людський фактор залишається одним із головних джерел ризику для сучасних інформаційних систем, а тому ефективне оцінювання рівня підготовки користувачів є необхідною умовою забезпечення кібербезпеки організації. Сучасний підхід до оцінювання стійкості персоналу передбачає використання комплексних методів: регулярного навчання, phishing simulation кампаній, поведінкової аналітики, моніторингу активності користувачів та постійного вдосконалення програм інформаційної безпеки. Лише поєднання технічних засобів захисту з формуванням культури кібербезпеки дозволяє суттєво знизити ризики, пов’язані з людським фактором, та підвищити загальний рівень захищеності організації.

1.14 Висновки

У першому розділі було проведено комплексний аналіз проблематики соціальної інженерії як одного з найбільш небезпечних та актуальних напрямів сучасних кіберзагроз. У процесі дослідження встановлено, що стрімкий розвиток інформаційних технологій, цифровізація суспільства та широке використання мережевих сервісів суттєво підвищили залежність організацій і користувачів від інформаційних систем, що, у свою чергу, створило сприятливі умови для розвитку соціотехнічних атак. У ході аналізу предметної області визначено, що соціальна інженерія базується насамперед на використанні людського фактора як найуразливішого елемента системи інформаційної безпеки [6, 7]. На відміну від класичних технічних атак, соціальна інженерія орієнтується на психологічний вплив на людину, використовуючи довіру, страх, цікавість, авторитет, поспіх та інші поведінкові особливості користувачів [4, 5]. Було встановлено, що саме людські помилки, недостатній рівень обізнаності та порушення правил кібергігієни залишаються одними з головних причин успішної компрометації інформаційних систем. У розділі розглянуто сутність соціальної інженерії, її психологічні механізми впливу та причини високої ефективності подібних атак. Визначено, що сучасні кіберзлочинці активно використовують емоційний тиск, персоналізацію повідомлень, автоматизацію фішингових кампаній та новітні цифрові технології для підвищення рівня довіри користувачів і обходу технічних механізмів захисту [8, 9]. Особливу увагу приділено ролі людського фактора у системі інформаційної безпеки та проблематиці оцінювання стійкості персоналу до атак соціальної інженерії. У процесі дослідження проведено класифікацію основних типів атак соціальної інженерії, серед яких фішинг, spear phishing, vishing, smishing, baiting, pretexting та інші методи психологічного впливу. Встановлено, що саме фішинг сьогодні є основним інструментом реалізації соціотехнічних атак завдяки своїй універсальності, низькій вартості, масштабованості та високій ефективності [10, 11]. Окремо

проаналізовано канали реалізації та способи маскування фішингових атак, які дозволяють зловмисникам вводити користувачів в оману та обходити системи захисту. У роботі також було розглянуто сучасні підходи до протидії фішинговим атакам, які включають використання технічних засобів захисту, систем моніторингу та поведінкової аналітики, SIEM-, SOAR-, XDR- та UEBA-рішень [19, 20, 23], а також проведення навчання персоналу та phishing simulation кампаній [16, 21]. Проаналізовано роль міжнародних стандартів та нормативних документів, зокрема International Organization for Standardization ISO/IEC 27001:2015 [1] та рекомендацій National Institute of Standards and Technology NIST SP 800-50 [3] і NIST SP 800-61 [2], які підкреслюють необхідність комплексного підходу до забезпечення інформаційної безпеки з урахуванням людського фактора. На основі проведеного аналізу можна зробити висновок, що ефективний захист від соціальної інженерії неможливий виключно за рахунок технічних засобів безпеки. Сучасна система кіберзахисту повинна поєднувати технологічні механізми захисту з регулярним навчанням персоналу, формуванням культури інформаційної безпеки, моделюванням реальних сценаріїв атак та постійним удосконаленням процедур реагування на інциденти. Отримані результати теоретичного дослідження створюють основу для подальшого практичного аналізу методів реалізації phishing simulation, побудови тестового середовища для моделювання фішингових кампаній та оцінювання рівня стійкості користувачів до атак соціальної інженерії, що буде розглянуто у наступних розділах роботи.

РОЗДІЛ 2. ОБҐРУНТУВАННЯ ТА РОЗРОБЛЕННЯ ЛАБОРАТОРНОГО СТЕНДУ

2.1 Аналіз існуючих підходів до тестування персоналу

У сучасних умовах стрімкого зростання кількості кіберзагроз особливої актуальності набуває питання оцінювання готовності персоналу до протидії атакам соціальної інженерії. Незважаючи на значні інвестиції організацій у технічні засоби захисту, численні дослідження демонструють, що людський фактор продовжує залишатися одним із головних джерел ризику для інформаційної безпеки. Саме тому сучасні системи кіберзахисту все частіше включають не лише технічні механізми безпеки, але й процедури оцінювання рівня підготовки працівників. Відповідно до вимог ДСТУ ISO/IEC 27001:2015 [1], ефективна система управління інформаційною безпекою повинна передбачати постійний контроль ризиків, пов’язаних із людським фактором, а також впровадження заходів щодо підвищення обізнаності користувачів. Аналогічні положення містяться в рекомендаціях NIST SP 800-50 [3], де наголошується на необхідності створення комплексних програм навчання та регулярного оцінювання рівня знань працівників у сфері кібербезпеки. Одним із найстаріших та найпоширеніших підходів до оцінювання персоналу є проведення теоретичного тестування. Даний метод передбачає використання анкет, опитувальників, контрольних завдань та сертифікаційних тестів для перевірки знань працівників щодо політик безпеки, правил роботи з інформацією та основних типів кіберзагроз. Перевагою такого підходу є простота реалізації та можливість швидкого охоплення великої кількості співробітників. Організація може регулярно перевіряти рівень знань персоналу без необхідності розгортання додаткової інфраструктури. Проте практика показує, що результати теоретичних тестів не завжди відображають реальну поведінку користувачів під час виникнення інцидентів безпеки. Наступним підходом є проведення навчальних тренінгів та програм підвищення обізнаності. Подібні програми передбачають проведення лекцій,

вебінарів, практичних занять та демонстрацію реальних сценаріїв атак соціальної інженерії. Відповідно до рекомендацій NIST SP 800-50 [3], навчання має проводитися на постійній основі та адаптуватися до актуальних загроз. Важливим напрямом є використання платформ Security Awareness Training, які дозволяють автоматизувати процес навчання персоналу. Найбільш відомими рішеннями у даній сфері є KnowBe4 [21], Proofpoint [24] та інші подібні системи. Дані платформи забезпечують централізоване управління навчальними програмами, відстеження прогресу користувачів та формування статистичних звітів. Проте навіть найкращі навчальні програми не можуть повністю відобразити поведінку користувача в умовах реальної атаки. Саме тому найбільш ефективним методом оцінювання стійкості персоналу вважається проведення контрольованих симуляцій фішингових атак (phishing simulation). Phishing simulation являє собою процес моделювання реальної фішингової кампанії в контрольованому середовищі без створення загрози для інформаційної інфраструктури організації. Працівники отримують тестові повідомлення, які максимально наближені до реальних атак. У процесі проведення симуляції збирається інформація про відкриття листів, переходи за посиланнями, введення облікових даних та інші дії користувачів. Основною перевагою такого підходу є можливість оцінити фактичну поведінку працівників у реалістичних умовах. На відміну від звичайного тестування, користувач не знає про проведення перевірки, що дозволяє отримати об'єктивні результати. Згідно з даними звітів Verizon DBIR 2024 [8], Microsoft Digital Defense Report [12] та SANS Security Awareness Report 2024 [14], саме регулярне проведення phishing simulation демонструє найкращі результати щодо зниження кількості успішних атак соціальної інженерії. Для проведення подібних тестувань використовуються спеціалізовані платформи, серед яких найбільш поширеними є Gophish [16], KnowBe4 [21] та рішення корпоративного класу від великих постачальників засобів кібербезпеки. Проведений аналіз показує, що найбільш ефективним підходом до оцінювання стійкості персоналу є поєднання навчання користувачів, регулярного

тестування знань та практичного моделювання фішингових атак. Саме тому для реалізації дослідження доцільно використовувати спеціалізований стенд phishing simulation, який дозволить максимально наблизити умови тестування до реальних сценаріїв соціальної інженерії.

2.2 Опис технічного рішення

Для проведення дослідження було прийнято рішення створити спеціалізований лабораторний стенд для моделювання фішингових атак та збору статистичних даних щодо поведінки користувачів. Основною метою створення такого стенду є безпечне відтворення реальних сценаріїв соціальної інженерії без ризику для виробничої інфраструктури організації.

При виборі архітектури технічного рішення враховувалися такі вимоги:

- ізоляція тестового середовища від робочих систем;
- можливість створення реалістичних фішингових кампаній;
- збір статистики взаємодії користувачів із повідомленнями;
- гнучкість налаштування сценаріїв атак;
- можливість подальшого масштабування;
- використання безкоштовного або відкритого програмного забезпечення.

Для реалізації лабораторного середовища було обрано платформу віртуалізації VMware Workstation Pro [17]. Використання віртуалізації дозволяє створити ізольоване середовище, у якому можуть безпечно розгортатися сервери, клієнтські системи та допоміжні сервіси без впливу на основну операційну систему. Основним компонентом стенду виступає платформа Gophish [16]. Даний інструмент є одним із найпопулярніших відкритих рішень для проведення phishing simulation та широко використовується у сфері кібербезпеки для навчання персоналу та оцінювання рівня стійкості користувачів до атак соціальної інженерії.

Функціональні можливості Gophish дозволяють:

- створювати фішингові кампанії;
- формувати списки цільових користувачів;
- створювати шаблони електронних листів;
- створювати посадкові сторінки (landing pages);
- відстежувати переходи за посиланнями;
- фіксувати факти введення облікових даних;
- збирати статистичні показники;
- формувати аналітичні звіти.

Для розгортання серверної частини використовується операційна система Linux. Додатково для тестування та аналізу мережевої взаємодії можуть використовуватись інструменти середовища Kali Linux [15].

Архітектурно стенд складається з кількох основних компонентів:

- Сервер Gophish.
- Вебсервер для розміщення фішингових сторінок.
- Поштова підсистема для відправлення тестових повідомлень.
- Клієнтські віртуальні машини.
- Система збору та аналізу результатів.

У процесі роботи користувач отримує тестове повідомлення електронною поштою. Після відкриття листа та переходу за посиланням здійснюється перенаправлення на підготовлену вебсторінку, яка імітує реальний ресурс. Усі дії користувача автоматично фіксуються в системі Gophish [16] та використовуються для подальшого аналізу. Для забезпечення безпечності експерименту всі отримані дані використовуються виключно в межах

дослідження та не містять реальних облікових записів або конфіденційної інформації. Метою експерименту є оцінювання поведінкових реакцій користувачів, а не отримання доступу до реальних даних. Запропоноване технічне рішення забезпечує можливість проведення контрольованих phishing simulation кампаній, збору статистичних даних та подальшого аналізу ефективності навчання персоналу. Саме на основі даного стенду в наступних підрозділах буде виконано розгортання середовища, налаштування інфраструктури та проведення практичного експерименту з оцінювання стійкості користувачів до атак соціальної інженерії.

2.3 Аналіз принципів побудови сценаріїв соціальної інженерії

Ефективність будь-якої атаки соціальної інженерії значною мірою залежить не від використаних технічних засобів, а від правильності побудови сценарію взаємодії із потенційною жертвою. Саме сценарій визначає спосіб психологічного впливу, послідовність дій користувача та кінцевий результат атаки. У сучасній практиці кібербезпеки побудова сценаріїв соціальної інженерії розглядається як окремий напрям досліджень, що поєднує знання з психології, інформаційної безпеки, поведінкового аналізу та комунікаційних технологій. У працях Christopher Hadnagy та Kevin Mitnick [6, 7] зазначається, що успішний сценарій соціальної інженерії повинен бути максимально наближеним до реальної життєвої або робочої ситуації. Користувач не повинен відчувати ознак тестування або підозрювати наявність загрози. Саме тому сучасні сценарії будуються на основі повсякденних робочих процесів, корпоративних комунікацій та звичних для працівника дій. Першим етапом побудови сценарію є визначення цільової аудиторії. На цьому етапі аналізуються особливості користувачів, їхні посадові обов'язки, рівень доступу до інформаційних ресурсів, характер повсякденної діяльності та потенційні ризики. Працівники різних підрозділів можуть по-різному реагувати на однакові повідомлення. Наприклад, співробітники фінансового відділу більш схильні взаємодіяти з повідомленнями про рахунки, платежі та

фінансові документи, тоді як працівники кадрового відділу можуть частіше відкривати листи, пов'язані з резюме або кадровою документацією. Наступним етапом є визначення психологічного механізму впливу. Як було встановлено в першому розділі, більшість атак соціальної інженерії використовує певні людські емоції або поведінкові особливості. Найчастіше використовуються довіра, страх, цікавість, терміновість, бажання допомогти або прагнення отримати певну вигоду [4, 5]. Саме вибір психологічного механізму визначає зміст майбутнього повідомлення та загальну логіку сценарію. Важливим принципом побудови сценарію є реалістичність. Згідно з рекомендаціями National Institute of Standards and Technology NIST SP 800-50 [3], навчальні та тестові заходи повинні максимально відображати реальні загрози, з якими можуть зіткнутися працівники. Якщо сценарій виглядає неприродно або містить очевидні ознаки шахрайства, результати тестування не дозволяють об'єктивно оцінити реальний рівень стійкості персоналу. Особливе значення має використання контекстуальної інформації. У сучасних атаках соціальної інженерії активно застосовуються дані про організацію, внутрішні процеси, корпоративні сервіси або актуальні події. Подібний підхід дозволяє підвищити довіру до повідомлення та зменшити ймовірність виявлення атаки користувачем. Ще одним принципом є поступове залучення користувача до взаємодії. Ефективний сценарій рідко передбачає негайне отримання необхідної інформації. Натомість користувача послідовно підводять до виконання певної дії. Наприклад, спочатку він відкриває лист, потім переходить за посиланням, після чого взаємодіє із вебсторінкою та вводить необхідні дані. Подібна багаторівнева структура значно підвищує ефективність атаки. Важливим фактором є також використання елементів соціального підтвердження та авторитету. Користувачі значно частіше довіряють повідомленням, які нібито надходять від керівництва компанії, системних адміністраторів, служби підтримки або популярних цифрових сервісів. Саме тому більшість сучасних фішингових кампаній використовує імітацію відомих брендів, корпоративних порталів або державних установ.

Сучасні аналітичні звіти Verizon DBIR 2024 [8], ENISA Threat Landscape [10] та Microsoft Digital Defense Report [12] демонструють, що найбільш успішними залишаються саме ті сценарії, які максимально адаптовані під конкретну аудиторію та враховують особливості її поведінки. У контексті даного дослідження особливо важливим є те, що сценарії повинні не лише моделювати реальні загрози, але й забезпечувати можливість збору статистичних даних для подальшого аналізу. Саме тому під час їх розробки необхідно враховувати не лише психологічну складову, але й можливість відстеження дій користувача на кожному етапі взаємодії із системою. Проведений аналіз показує, що побудова сценаріїв соціальної інженерії є складним процесом, який вимагає врахування психологічних особливостей користувачів, специфіки діяльності організації та сучасних тенденцій розвитку кіберзагроз. На основі розглянутих принципів було сформовано набір сценаріїв, які використовуватимуться для проведення експериментального дослідження в межах даної роботи.

2.4 Розробка сценаріїв фішингових атак

На основі проведеного аналізу сучасних методів соціальної інженерії та принципів побудови поведінкових сценаріїв було виконано розробку набору фішингових кампаній для подальшого використання в тестовому середовищі. Основною метою створення сценаріїв є оцінювання рівня стійкості користувачів до різних видів психологічного впливу та визначення найбільш уразливих аспектів їхньої поведінки. Під час розробки сценаріїв враховувалися рекомендації стандарту International Organization for Standardization ISO/IEC 27001:2015 [1] щодо управління ризиками інформаційної безпеки, рекомендації National Institute of Standards and Technology NIST SP 800-50 [3] щодо навчання персоналу та результати сучасних досліджень у сфері соціальної інженерії [6, 7]. Для проведення експерименту було прийнято рішення використати декілька сценаріїв різного рівня складності та різної психологічної спрямованості. Такий підхід дозволяє отримати більш

об'єктивну оцінку поведінки користувачів та проаналізувати ефективність окремих механізмів впливу. Перший сценарій базується на використанні терміновості та страху. Користувач отримує повідомлення нібито від служби підтримки корпоративного сервісу із повідомленням про необхідність термінового підтвердження облікового запису. У листі міститься попередження про можливе блокування акаунта в разі невиконання зазначених дій. Основною метою даного сценарію є перевірка схильності користувачів до прийняття поспішних рішень під впливом емоційного тиску. Другий сценарій використовує авторитет та довіру до керівництва організації. Повідомлення імітує службове розпорядження або терміновий запит від керівника підрозділу. У листі міститься посилання на документ або внутрішній корпоративний ресурс. Даний сценарій дозволяє оцінити вплив авторитету на поведінку користувачів та їхню готовність перевіряти достовірність отриманої інформації. Третій сценарій побудований на використанні цікавості. Користувачу надсилається повідомлення із темою, яка потенційно може викликати інтерес, наприклад новий документ, результати перевірки або внутрішня інформація компанії. Основним завданням є визначення рівня обережності користувачів під час взаємодії з невідомими вкладеннями або посиланнями. Четвертий сценарій використовує прагнення до вигоди. Повідомлення містить інформацію про бонуси, додаткові виплати, спеціальні пропозиції або корпоративні привілеї. Подібний тип атак широко використовується в реальних фішингових кампаніях та дозволяє оцінити вплив матеріальної мотивації на поведінку користувачів. Для реалізації розроблених сценаріїв було використано платформу Gophish [16], яка забезпечує створення шаблонів повідомлень, налаштування цільових груп користувачів, розгортання посадкових сторінок та автоматичний збір статистичних даних. Кожен сценарій складається з трьох основних компонентів. Першим компонентом є фішинговий лист, який виступає початковою точкою взаємодії з користувачем. Другим компонентом є посадкова сторінка, що імітує легітимний вебресурс.

Третім компонентом є система моніторингу та збору статистики, яка фіксує всі дії користувача під час проходження сценарію.

Для оцінювання результатів передбачено збір таких показників:

- кількість доставлених повідомлень;
- кількість відкритих листів;
- кількість переходів за посиланнями;
- кількість введених облікових даних;
- час реакції користувачів;
- відсоток успішного виконання сценарію.

Отримані дані дозволяють визначити найбільш ефективні методи психологічного впливу, оцінити рівень підготовки персоналу та сформувати рекомендації щодо подальшого підвищення рівня інформаційної безпеки. Таким чином, розроблені сценарії фішингових атак відображають найбільш поширені та актуальні методи соціальної інженерії, що використовуються сучасними зловмисниками. Їх використання у створеному лабораторному середовищі дозволяє максимально наблизити умови експерименту до реальних кіберзагроз та забезпечити об'єктивне оцінювання стійкості користувачів до фішингових атак. Наступним етапом роботи є безпосереднє розгортання тестового середовища та реалізація створених сценаріїв у межах практичного експерименту.

2.5 Розробка моделі оцінювання стійкості персоналу

Одним із ключових завдань даного дослідження є створення моделі оцінювання стійкості персоналу до атак соціальної інженерії. Необхідність розробки такої моделі обумовлена тим, що традиційні методи оцінювання знань користувачів не дозволяють об'єктивно визначити їхню реальну готовність до протидії сучасним фішинговим кампаніям. Практика показує, що

навіть користувачі з високим рівнем теоретичної підготовки можуть ставати жертвами атак через психологічний тиск, втому, неуважність або недостатній рівень практичного досвіду. Відповідно до положень ДСТУ ISO/IEC 27001:2015 [1] система управління інформаційною безпекою повинна включати механізми оцінювання ризиків, пов’язаних із людським фактором. Аналогічно рекомендації NIST SP 800-50 [3] наголошують на необхідності регулярного вимірювання ефективності програм підвищення обізнаності персоналу. Таким чином, оцінювання стійкості користувачів повинно ґрунтуватися не лише на перевірці знань, а й на аналізі фактичної поведінки працівників у реалістичних умовах. Основною метою розробленої моделі є отримання кількісної оцінки рівня стійкості користувачів до фішингових атак та визначення найбільш уразливих аспектів їхньої поведінки. Для досягнення цієї мети модель базується на аналізі результатів phishing simulation кампаній та передбачає оцінювання декількох ключових показників. Першим показником є факт відкриття фішингового повідомлення. Даний параметр дозволяє оцінити рівень зацікавленості користувача та ефективність тематики повідомлення. Відкриття листа саме по собі не свідчить про компрометацію користувача, однак є початковим етапом взаємодії із фішинговою кампанією. Другим показником виступає перехід за вбудованим посиланням. Саме ця дія демонструє готовність користувача довіряти отриманому повідомленню та взаємодіяти з потенційно небезпечними ресурсами. У більшості реальних атак саме перехід за посиланням стає точкою входу для подальшої компрометації системи. Третім показником є введення облікових даних на підробленій вебсторінці. Даний критерій вважається одним із найбільш важливих, оскільки безпосередньо відображає успішність атаки соціальної інженерії. Передача логіна або пароля фактично означає компрометацію користувача та створення загрози для інформаційної системи. Четвертим показником є швидкість реакції користувача. Даний параметр дозволяє оцінити ступінь імпульсивності прийняття рішень. Чим швидше користувач взаємодіє з фішинговим повідомленням, тим менше часу він витрачає на аналіз його достовірності.

П’ятим показником є здатність користувача виявляти підозрілу активність та повідомляти про неї відповідальним особам. З точки зору сучасної кібербезпеки саме повідомлення про підозрілий лист є однією з найбільш бажаних моделей поведінки. На основі зазначених параметрів формується інтегральний показник стійкості користувача. Результати оцінювання дозволяють розподілити користувачів на кілька рівнів готовності до протидії атакам соціальної інженерії. До високого рівня стійкості відносяться користувачі, які не взаємодіяли з фішинговим повідомленням або своєчасно ідентифікували його як підозріле. Подібні користувачі демонструють високий рівень цифрової грамотності та дотримання правил інформаційної безпеки. Середній рівень стійкості характеризує користувачів, які взаємодіяли з повідомленням або відкрили його, але не здійснили критичних дій, пов’язаних із передачею конфіденційної інформації. Низький рівень стійкості визначається у випадках, коли користувач перейшов за посиланням, ввів облікові дані або виконав інші дії, які можуть призвести до компрометації інформаційної системи. Особливістю запропонованої моделі є можливість її адаптації до різних сценаріїв тестування та різних категорій користувачів. Це дозволяє використовувати модель не лише в межах даного дослідження, але й під час проведення внутрішніх аудитів безпеки або регулярних перевірок персоналу в організаціях. Важливим аспектом є також використання статистичних даних для подальшого вдосконалення програм навчання. Аналіз результатів оцінювання дозволяє визначати найбільш проблемні напрямки підготовки користувачів та формувати цільові програми підвищення обізнаності. Таким чином, розроблена модель оцінювання стійкості персоналу забезпечує комплексний підхід до аналізу поведінки користувачів та дозволяє отримати кількісні показники ефективності захисту від соціальної інженерії. Для практичного застосування моделі необхідно визначити порядок проведення тестування, умови реалізації фішингових кампаній та процедури збору результатів, що розглядається в наступному підрозділі.

2.6 Методика проведення тестування

Для забезпечення об'єктивності результатів дослідження та коректного оцінювання рівня стійкості персоналу була розроблена методика проведення тестування, яка базується на використанні контрольованих phishing simulation кампаній. Методика враховує рекомендації стандарту ДСТУ ISO/IEC 27001:2015 [1], рекомендації NIST SP 800-50 [3] щодо навчання користувачів та NIST SP 800-61 [2] щодо реагування на інциденти інформаційної безпеки. Основною метою тестування є визначення рівня готовності користувачів до протидії атакам соціальної інженерії шляхом моделювання реалістичних сценаріїв фішингових атак у контрольованому середовищі. На першому етапі здійснюється підготовка тестового середовища. Для реалізації експерименту використовується віртуальна інфраструктура на базі VMware Workstation Pro [17] та платформа Gophish [16]. Подібний підхід дозволяє забезпечити ізоляцію тестової інфраструктури від виробничих систем та виключити ризик впливу на реальні корпоративні ресурси. Другий етап передбачає формування цільової групи користувачів та підготовку сценаріїв фішингових атак. Для проведення тестування використовуються сценарії, розроблені у попередньому підрозділі, які моделюють найбільш поширені типи соціотехнічних атак: використання терміновості, авторитету, цікавості та матеріальної вигоди. На третьому етапі здійснюється створення шаблонів електронних повідомлень та посадкових сторінок. При розробці шаблонів враховуються сучасні тенденції розвитку фішингових кампаній, описані у звітах Verizon DBIR 2024 [8], CrowdStrike Global Threat Report [9] та Microsoft Digital Defense Report [12]. Основною вимогою є максимальна реалістичність повідомлень та їхня відповідність реальним сценаріям атак. Наступним етапом є безпосереднє проведення фішингової кампанії. Платформа Gophish [16] виконує автоматизовану розсилку підготовлених повідомлень користувачам та здійснює моніторинг їхньої взаємодії із вмістом листів.

Під час проведення тестування система автоматично реєструє такі події:

- факт доставки повідомлення;
- факт відкриття листа;
- факт переходу за посиланням;
- факт відвідування посадкової сторінки;
- факт введення облікових даних;
- час виконання кожної дії;
- загальну послідовність взаємодії користувача зі сценарієм.

Отримані дані накопичуються в централізованій базі результатів та використовуються для подальшого аналізу. Особливу увагу приділено питанням етичності проведення дослідження. Тестування здійснюється виключно в межах навчального або дослідницького середовища. У процесі експерименту не використовуються реальні паролі, фінансові реквізити або інша конфіденційна інформація користувачів. Усі отримані дані застосовуються лише для оцінювання поведінкових характеристик та аналізу ефективності навчання. Після завершення кампанії виконується обробка результатів. Для кожного користувача визначається рівень стійкості відповідно до розробленої моделі оцінювання. Додатково проводиться аналіз ефективності окремих сценаріїв та психологічних механізмів впливу. Наступним етапом є формування аналітичного звіту. У звіті відображаються загальні показники кампанії, відсоток відкритих повідомлень, кількість переходів за посиланнями, випадки введення облікових даних та інтегральні показники стійкості користувачів. Отримані результати використовуються для визначення рівня готовності персоналу до сучасних кіберзагроз та формування рекомендацій щодо подальшого вдосконалення програм навчання. Подібний підхід відповідає рекомендаціям сучасних платформ підвищення обізнаності, зокрема KnowBe4 [21], та дозволяє забезпечити безперервний процес покращення культури інформаційної безпеки в організації. Таким чином,

розроблена методика забезпечує системний підхід до проведення тестування персоналу, дозволяє отримати об'єктивні результати оцінювання та створює основу для подальшого аналізу ефективності фішингових сценаріїв у межах практичної частини дослідження. Наступним етапом роботи є безпосередня реалізація лабораторного стенду та проведення експериментального тестування з використанням розроблених сценаріїв соціальної інженерії.

2.7 Розробка лабораторного стенду

Після проведення аналізу сучасних підходів до тестування персоналу, розробки сценаріїв соціальної інженерії та формування методики оцінювання стійкості користувачів виникає необхідність створення спеціалізованого лабораторного стенду, який дозволить реалізувати експериментальне дослідження у контрольованому середовищі. Основним призначенням такого стенду є безпечне відтворення реальних сценаріїв фішингових атак, збір статистичних даних про поведінку користувачів та оцінювання рівня їхньої готовності до протидії соціотехнічним загрозам. Необхідність створення лабораторного середовища обумовлена тим, що проведення подібних досліджень у виробничій інфраструктурі організації може створювати додаткові ризики для інформаційної безпеки. Використання тестового середовища дозволяє моделювати реальні сценарії атак без загрози для корпоративних ресурсів, користувацьких даних та критично важливих інформаційних систем. Відповідно до рекомендацій ДСТУ ISO/IEC 27001:2015 [1] та NIST SP 800-61 [2] під час проведення тестувань інформаційної безпеки необхідно забезпечувати контрольованість процесів, можливість моніторингу подій та мінімізацію ризиків для основної інфраструктури. Саме тому лабораторний стенд будується як окреме ізольоване середовище, яке функціонує незалежно від виробничих ресурсів. При розробці лабораторного стенду були визначені основні вимоги до майбутньої системи. Насамперед середовище повинно забезпечувати можливість проведення фішингових кампаній різного рівня складності. Крім

того, необхідною умовою є можливість створення та редагування шаблонів електронних повідомлень, розгортання фішингових вебсторінок, моніторингу дій користувачів та накопичення статистичних даних для подальшого аналізу. Особлива увага приділялася масштабованості рішення. Лабораторний стенд повинен дозволяти розширення функціональності без необхідності повної перебудови архітектури. Це забезпечує можливість використання стенду не лише для проведення окремого дослідження, але й для подальшого навчання користувачів, моделювання нових сценаріїв соціальної інженерії та тестування додаткових механізмів захисту. Для реалізації середовища було прийнято рішення використовувати платформу віртуалізації VMware Workstation Pro [17]. Використання технологій віртуалізації дозволяє створити декілька ізольованих віртуальних машин, що імітують окремі елементи інформаційної інфраструктури. На рисунку 2.1 представлено загальну структуру розробленого лабораторного стенду.

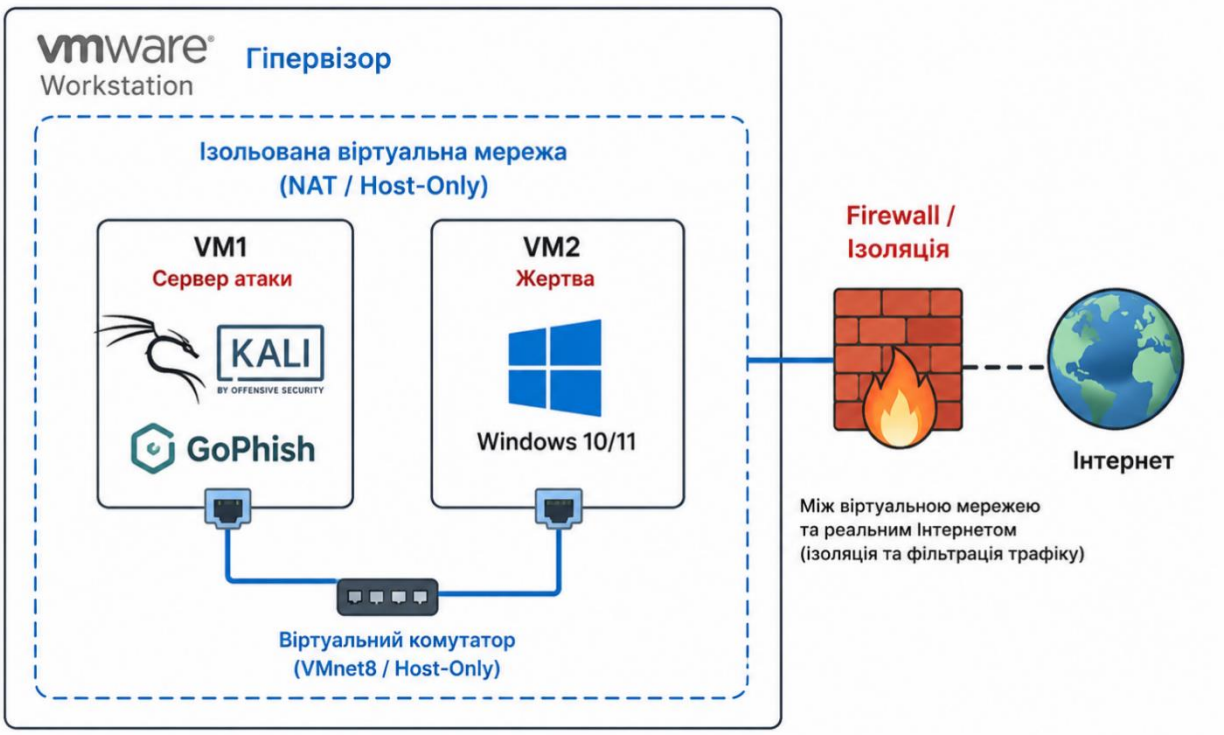

Рисунок 2.1 – Загальна структура лабораторного стенду для моделювання фішингових атак

Основою середовища виступає платформа VMware Workstation, у межах якої створено ізольовану віртуальну мережу. У середовищі функціонують дві віртуальні машини: сервер атаки на базі Kali Linux із встановленою платформою Gophish та клієнтська система під керуванням Windows 10/11, яка виконує роль потенційної жертви фішингової атаки. Взаємодія між вузлами здійснюється через віртуальний комутатор, а доступ до зовнішніх мереж контролюється механізмами ізоляції та фільтрації трафіку. Такий підхід значно спрощує процес налаштування середовища, забезпечує безпечність експериментів та дозволяє швидко відновлювати систему після проведення тестувань. Як основний інструмент моделювання фішингових кампаній було обрано Gophish [16]. Дана платформа є одним із найбільш поширених відкритих рішень для проведення phishing simulation та широко використовується як у навчальних цілях, так і під час проведення внутрішніх аудитів безпеки. Вибір Gophish [16] пояснюється його функціональними можливостями, серед яких створення шаблонів електронних листів, налаштування посадкових сторінок, автоматизація розсилок, збір статистики та формування аналітичних звітів. Важливою перевагою платформи є наявність вебінтерфейсу, що значно спрощує процес адміністрування та керування кампаніями. Для забезпечення максимальної наближеності до реальних умов у лабораторному середовищі передбачено використання окремого вебсервера, який виконує функції розміщення фішингових сторінок. Також реалізовано тестову поштову інфраструктуру, яка використовується для розсилання повідомлень учасникам експерименту. Окрему роль у структурі лабораторного стенду відіграють клієнтські системи, які імітують робочі станції користувачів. Саме через взаємодію з цими системами здійснюється моделювання поведінки користувачів під час отримання фішингових повідомлень та переходу на підроблені вебресурси. У процесі розробки лабораторного стенду особлива увага приділялася питанням безпеки. Всі компоненти середовища працюють виключно в межах ізольованої мережі. Жоден із елементів стенду не має доступу до реальних корпоративних ресурсів

або персональних даних користувачів. Подібний підхід дозволяє повністю виключити можливість негативного впливу дослідження на зовнішні системи. Таким чином, створений лабораторний стенд забезпечує необхідні умови для проведення комплексного дослідження ефективності фішингових атак та оцінювання стійкості персоналу до методів соціальної інженерії. Для детального розуміння принципів функціонування створеного середовища необхідно розглянути його архітектуру та структуру.

2.8 Архітектура та структура лабораторного стенду

Архітектура лабораторного стенду була спроєктована з урахуванням вимог до безпечності, масштабованості, ізоляції та можливості збору статистичних даних під час проведення експериментів. Основною задачею архітектури є забезпечення взаємодії між компонентами системи таким чином, щоб максимально точно моделювати реальну фішингову кампанію та водночас гарантувати повний контроль над усіма процесами. Структурно лабораторний стенд складається з декількох взаємопов’язаних підсистем, кожна з яких виконує окремі функції в межах експерименту.

Таблиця 2.1 – Основні компоненти лабораторного стенду

Компонент	**Призначення**
VMware Workstation Pro	Створення та керування віртуальними машинами
Kali Linux	Платформа для розгортання інструментів тестування безпеки

Продовження таблиц таблиця 2.1.

Gophish	Створення та проведення фішингових кампаній
Web Server	Розміщення посадкових (landing) сторінок
Windows 10/11 Client VM	Імітація робочої станції користувача
Virtual Network (Host-Only)	Організація ізольованого мережевого середовища
Virtual Switch (VMnet)	Забезпечення мережевої взаємодії між вузлами
Firewall / Network Isolation	Контроль мережевого доступу та ізоляція стенду

Першим компонентом архітектури є система віртуалізації на базі VMware Workstation Pro [17]. Вона виступає основою всього лабораторного середовища та забезпечує створення окремих ізольованих віртуальних машин. Завдяки цьому кожен компонент системи функціонує незалежно та може бути налаштований відповідно до поставлених завдань. Другим компонентом виступає сервер управління фішинговими кампаніями, реалізований на базі Gophish [16]. Саме цей сервер відповідає за створення сценаріїв атак, формування шаблонів повідомлень, керування кампаніями та збір результатів тестування. У структурі сервера Gophish виділяються декілька функціональних модулів. Перший модуль забезпечує створення та редагування шаблонів електронних повідомлень. Другий відповідає за налаштування

цільових груп користувачів. Третій виконує функції моніторингу та збору статистики. Четвертий забезпечує формування аналітичних звітів за результатами проведених кампаній. Наступним елементом архітектури є вебсервер, який використовується для розміщення посадкових сторінок. Його основною функцією є імітація реальних вебресурсів, на які перенаправляються користувачі після переходу за посиланням із фішингового повідомлення. Дані сторінки можуть відтворювати інтерфейси популярних сервісів, корпоративних порталів або інших інформаційних ресурсів. Важливим компонентом системи є тестова поштова інфраструктура. Вона забезпечує доставку повідомлень користувачам та імітує роботу реальних поштових сервісів. Саме через даний компонент здійснюється початкова взаємодія користувача із фішинговою кампанією. Наступним елементом архітектури є клієнтські віртуальні машини. Вони моделюють робочі станції співробітників організації та використовуються для відтворення поведінки реальних користувачів під час виконання тестування. На цих системах встановлюються типові програмні засоби, які використовуються в повсякденній роботі, зокрема веббраузери та поштові клієнти. Окрему роль відіграє підсистема збору та аналізу даних. Під час проведення тестування система автоматично фіксує всі ключові події, включаючи відкриття повідомлень, переходи за посиланнями, взаємодію з посадковими сторінками та введення тестових облікових даних. Отримана інформація накопичується в централізованому сховищі та використовується для подальшого аналізу. Архітектура стенду також передбачає можливість інтеграції із сучасними системами моніторингу інформаційної безпеки. У перспективі результати можуть аналізуватися за допомогою рішень класу SIEM та XDR, таких як IBM QRadar [20], Microsoft Sentinel [23], Wazuh [27] або Splunk Enterprise Security [25]. Це дозволяє наблизити дослідницьке середовище до сучасних корпоративних систем кібербезпеки. З функціональної точки зору робота стенду реалізується за наступною схемою. Сервер Gophish формує фішингову кампанію та надсилає підготовлені повідомлення користувачам. Після отримання листа користувач

відкриває повідомлення та взаємодіє з його вмістом. У разі переходу за посиланням здійснюється перенаправлення на посадкову сторінку, де система фіксує подальші дії користувача. Уся інформація автоматично передається до модуля збору статистики та використовується для розрахунку показників стійкості персоналу. Таким чином, розроблена архітектура лабораторного стенду забезпечує повний цикл моделювання фішингових атак - від створення сценарію до збору та аналізу результатів. Структура системи дозволяє безпечно проводити експерименти, отримувати достовірні статистичні дані та використовувати їх для подальшого оцінювання рівня підготовки користувачів до сучасних загроз соціальної інженерії. Наступним етапом роботи є практична реалізація розробленої архітектури та налаштування всіх компонентів лабораторного стенду. Ось текст підрозділів 2.9, 2.10 та 2.11 із правильно розставленими посиланнями на літературу у квадратних дужках відповідно до академічних вимог та наданого вами списку джерел:

2.9 Вибір програмного забезпечення та платформ

Одним із найважливіших етапів розробки лабораторного стенду для моделювання фішингових атак є вибір програмного забезпечення та технологічних платформ, які забезпечать реалізацію поставлених завдань. Від правильності вибору програмних компонентів залежить не лише функціональність створеного середовища, але й можливість проведення об’єктивного дослідження, збору статистичних даних та подальшого аналізу отриманих результатів. Під час вибору програмного забезпечення враховувалися вимоги, сформовані на попередніх етапах дослідження. Насамперед необхідно було забезпечити можливість створення реалістичних фішингових кампаній, розгортання підроблених вебресурсів, автоматизованого збору статистики, моделювання поведінки користувачів та функціонування середовища в ізольованій інфраструктурі. Важливими критеріями також були доступність програмного забезпечення, наявність документації, підтримка спільнотою та можливість масштабування рішення.

Таблиця 2.2 – Порівняння програмних рішень, використаних під час створення лабораторного стенду

Програмне забезпечення	Основне призначення	Причина вибору
VMware Workstation Pro	Створення та керування віртуальними машинами	Простота налаштування, підтримка ізольованих мереж
Kali Linux	Середовище для тестування безпеки	Наявність великої кількості інструментів кібербезпеки
Gophish	Проведення фішингових кампаній	Відкритий код, зручний вебінтерфейс, збір статистики
Windows 10/11	Імітація робочої станції користувача	Найбільш поширена клієнтська ОС
Apache/Nginx	Розміщення посадкових сторінок	Простота розгортання та налаштування
Virtual-Network (VMnet8/Host-Only)	Організація ізольованої мережі	Безпечне проведення тестування

Як видно з таблиці 2.2, під час вибору програмного забезпечення перевага надавалася рішенням з відкритим вихідним кодом або продуктам, які широко використовуються в професійному середовищі кібербезпеки. Такий підхід забезпечує можливість відтворення результатів дослідження, спрощує налаштування лабораторного стенду та дозволяє використовувати актуальні

інструменти, що застосовуються під час проведення сучасних досліджень у сфері інформаційної безпеки. Основою лабораторного середовища було обрано платформу віртуалізації VMware Workstation Pro [17]. Використання віртуалізації дозволяє створити декілька незалежних віртуальних машин, що імітують різні компоненти інформаційної системи. Віртуалізація забезпечує ізоляцію середовища, спрощує процес налаштування та дозволяє швидко відновлювати систему після проведення експериментів. Крім того, VMware Workstation Pro [17] підтримує створення локальних віртуальних мереж, що є важливою умовою для безпечного тестування фішингових сценаріїв. Для реалізації фішингових кампаній було обрано платформу Gophish [16]. На сьогодні Gophish є одним із найбільш популярних інструментів для проведення phishing simulation та широко використовується у сфері кібербезпеки для навчання персоналу та оцінювання рівня стійкості користувачів до соціальної інженерії. Важливою перевагою даного рішення є відкритий вихідний код, простота налаштування та наявність широкого набору функцій для створення та управління фішинговими кампаніями. Серед функціональних можливостей Gophish [16] слід виділити створення шаблонів електронних листів, налаштування посадкових сторінок, формування груп користувачів, автоматизоване відстеження подій та побудову статистичних звітів. Використання даного програмного забезпечення дозволяє отримувати достовірні дані про поведінку користувачів у процесі проходження тестування. Для серверної частини лабораторного стенду використовується операційна система Linux. Вибір Linux пояснюється її стабільністю, високим рівнем безпеки, низькими вимогами до апаратних ресурсів та широкими можливостями адміністрування. Крім того, більшість сучасних інструментів для тестування безпеки розробляються саме для Linux-середовищ. Для проведення додаткових досліджень та аналізу мережевої взаємодії використовується Kali Linux [15]. Даний дистрибутив містить велику кількість інструментів для аналізу мережевого трафіку, тестування захищеності систем та проведення дослідницьких робіт у сфері інформаційної безпеки. При

розгляді перспектив розвитку лабораторного стенду також було проаналізовано можливість інтеграції із сучасними системами моніторингу безпеки. До таких рішень належать Microsoft Sentinel [23], IBM QRadar [20], Splunk Enterprise Security [25], Wazuh [27] та CrowdStrike Falcon [18]. Хоча в межах даного дослідження повноцінна інтеграція з цими системами не виконується, можливість їхнього використання була врахована під час проєктування архітектури стенду. Таким чином, обраний набір програмного забезпечення забезпечує повну реалізацію поставлених завдань та створює необхідні умови для проведення дослідження стійкості персоналу до фішингових атак.

2.10 Розгортання та налаштування стенду

Після завершення етапу проєктування архітектури та вибору програмного забезпечення було виконано розгортання лабораторного стенду для моделювання фішингових атак. Основною метою даного етапу стало створення працездатного середовища, яке дозволяє реалізувати розроблені сценарії соціальної інженерії та забезпечити збір статистичних даних про поведінку користувачів. Першим етапом розгортання стало створення віртуальної інфраструктури на базі VMware Workstation Pro [17]. У межах середовища було сформовано набір віртуальних машин, які виконують функції серверних та клієнтських компонентів системи. Для забезпечення безпеки всі віртуальні машини були розміщені в окремому сегменті мережі з обмеженим доступом до зовнішніх ресурсів. Наступним кроком стало встановлення серверної операційної системи Linux та виконання її базового налаштування. На даному етапі були налаштовані мережеві параметри, створені необхідні користувацькі облікові записи та реалізовані базові механізми захисту серверної інфраструктури. Після підготовки серверного середовища було встановлено платформу Gophish [16]. Процес налаштування включав конфігурацію вебінтерфейсу адміністратора, створення тестових кампаній, формування груп користувачів та налаштування механізмів збору

статистичних даних. Наступним етапом стало створення шаблонів фішингових повідомлень та посадкових сторінок відповідно до сценаріїв, розроблених у попередніх підрозділах. Особлива увага приділялася забезпеченню реалістичності повідомлень та максимальній відповідності сучасним методам соціальної інженерії, описаним у звітах Verizon DBIR [8], Microsoft Digital Defense Report [12] та ENISA Threat Landscape [10]. Для моделювання поведінки користувачів було створено окремі клієнтські віртуальні машини. На них встановлено типове програмне забезпечення, що використовується під час роботи з електронною поштою та вебресурсами. Це дозволило максимально наблизити умови тестування до реального робочого середовища. Окремим завданням стало налаштування механізмів збору статистики. Платформа Gophish [16] автоматично реєструє відкриття листів, переходи за посиланнями, взаємодію з посадковими сторінками та введення тестових облікових даних. Усі події накопичуються в централізованій базі даних і використовуються для подальшого оцінювання рівня стійкості користувачів. Після завершення налаштування було виконано серію тестових запусків системи. Перевірялися працездатність усіх компонентів архітектури, коректність взаємодії між сервером Gophish [16], вебсервером та клієнтськими системами, а також точність фіксації подій у журналі активності. Результати перевірки підтвердили готовність лабораторного стенду до проведення експериментального дослідження. Створене середовище забезпечує реалізацію повного циклу phishing simulation - від формування сценарію атаки до збору та аналізу результатів взаємодії користувачів із фішинговими повідомленнями. Таким чином, виконане розгортання та налаштування лабораторного стенду створює необхідну технічну основу для проведення практичного етапу дослідження, який буде присвячений реалізації фішингових кампаній, збору статистичних даних та аналізу отриманих результатів.

2.11 Висновки до розділу 2

У другому розділі було виконано комплексне проєктування системи тестування стійкості персоналу до атак соціальної інженерії та розроблено лабораторний стенд для проведення практичного дослідження. На основі аналізу сучасних підходів до оцінювання рівня підготовки користувачів встановлено, що найбільш ефективним методом перевірки готовності персоналу до протидії соціотехнічним загрозам є використання контрольованих phishing simulation кампаній [14, 16], які дозволяють оцінювати реальну поведінку користувачів у максимально наближених до реальності умовах. У процесі виконання роботи було досліджено принципи побудови сценаріїв соціальної інженерії та визначено основні психологічні механізми впливу, які використовуються сучасними зловмисниками [4, 6, 7]. На основі проведеного аналізу розроблено набір сценаріїв фішингових атак, спрямованих на використання таких факторів, як терміновість, авторитет, цікавість та прагнення до отримання вигоди. Створені сценарії дозволяють моделювати найбільш поширені види сучасних фішингових кампаній та забезпечують можливість об’єктивного оцінювання поведінки користувачів. У межах дослідження було розроблено модель оцінювання стійкості персоналу, яка базується на аналізі фактичних дій користувачів під час взаємодії з фішинговими повідомленнями. Модель передбачає оцінювання таких показників, як відкриття електронних листів, переходи за посиланнями, введення облікових даних та здатність користувачів розпізнавати потенційні загрози. На основі цих параметрів формується інтегральний показник стійкості, що дозволяє кількісно оцінювати рівень підготовки персоналу. Також було розроблено методику проведення тестування, яка визначає порядок підготовки середовища, реалізації сценаріїв атак, збору статистичних даних та аналізу результатів [1, 2]. Запропонована методика забезпечує об’єктивність дослідження та дозволяє отримувати достовірні результати щодо рівня готовності користувачів до сучасних кіберзагроз. Особливу увагу приділено

створенню лабораторного стенду та розробці його архітектури. Було сформовано структуру середовища, яка включає платформу віртуалізації, сервер керування фішинговими кампаніями, тестову поштову інфраструктуру, вебсервер для розміщення посадкових сторінок та клієнтські системи. Така архітектура забезпечує безпечне проведення експериментів та дозволяє реалізувати повний цикл моделювання фішингових атак. На основі проведеного аналізу виконано вибір програмного забезпечення та платформ для реалізації лабораторного стенду. Як основні компоненти були використані VMware Workstation Pro [17] для побудови віртуальної інфраструктури та Gophish [16] для створення і проведення phishing simulation кампаній. Обрані рішення забезпечують необхідну функціональність, гнучкість налаштування та можливість подальшого розвитку створеного середовища. Завершальним етапом другого розділу стало розгортання та налаштування лабораторного стенду. У результаті було створено повністю працездатне тестове середовище, готове до проведення експериментальних досліджень. Реалізована інфраструктура забезпечує можливість моделювання реалістичних фішингових атак, збору статистичних даних та подальшого аналізу рівня стійкості персоналу до методів соціальної інженерії. Отримані результати створюють необхідну основу для переходу до практичної частини дослідження. У наступному розділі буде розглянуто процес реалізації лабораторного стенду, проведення фішингових кампаній, аналіз отриманих результатів та оцінювання ефективності запропонованої моделі визначення стійкості персоналу до атак соціальної інженерії.

РОЗДІЛ 3. РЕАЛІЗАЦІЯ ТА АНАЛІЗ РЕЗУЛЬТАТІВ

3.1 Реалізація сценаріїв у середовищі стенду

Після завершення проєктування лабораторного стенду та налаштування його компонентів було виконано практичну реалізацію розроблених сценаріїв соціальної інженерії. Основною метою даного етапу стало відтворення реальних фішингових кампаній у контрольованому середовищі та отримання статистичних даних щодо поведінки користувачів під час взаємодії з потенційно небезпечними повідомленнями. Реалізація сценаріїв здійснювалася на базі платформи Gophish [16], яка була розгорнута у створеному лабораторному середовищі. Дана платформа дозволила створити необхідні шаблони електронних листів, налаштувати групи користувачів, сформувати посадкові сторінки та забезпечити автоматизований збір статистики. Під час створення сценаріїв особлива увага приділялася максимальній реалістичності повідомлень. Як показують дослідження, наведені у звітах Verizon DBIR 2024 [8], Microsoft Digital Defense Report [12] та ENISA Threat Landscape [10], успішність сучасних фішингових кампаній значною мірою залежить від того, наскільки правдоподібно виглядає повідомлення для потенційної жертви. У межах дослідження було реалізовано чотири окремі сценарії фішингових атак. Перший сценарій імітував повідомлення про необхідність термінової зміни пароля в сервісі Microsoft 365. Основою даного сценарію став психологічний фактор терміновості, який змушує користувача діяти швидко та не витрачати час на перевірку достовірності інформації. У повідомленні зазначалося, що обліковий запис користувача буде заблоковано у випадку невиконання запропонованих дій протягом визначеного часу.

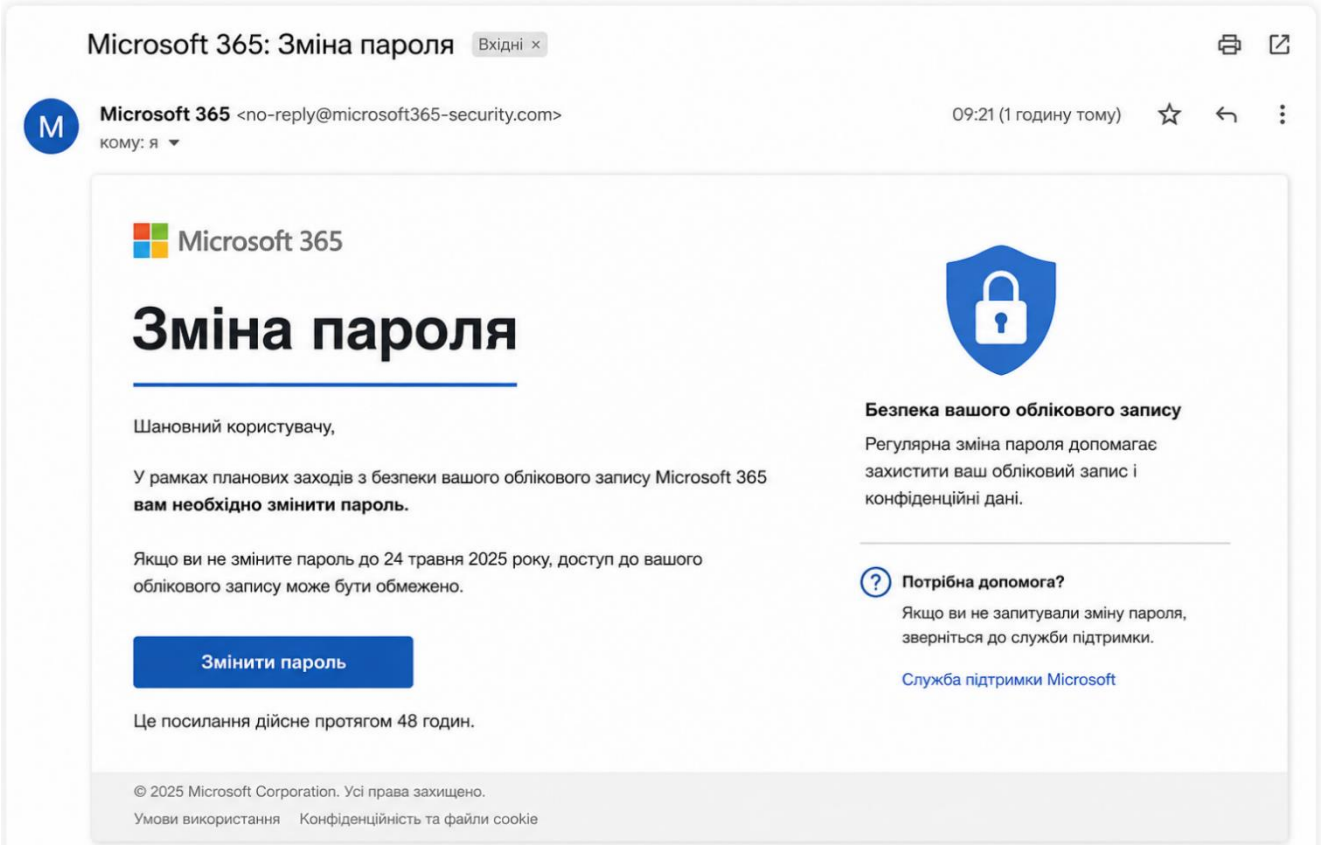

Рисунок 3.1 – Фішинговий лист, що імітує повідомлення Microsoft 365

Представлений на рисунку 3.1 лист містить типові ознаки сучасної фішингової атаки, зокрема використання корпоративної символіки, повідомлення про загрозу блокування облікового запису та посилання на підроблену сторінку авторизації. Подібні сценарії активно використовуються зловмисниками для викрадення облікових даних користувачів. Другий сценарій моделював повідомлення від служби інформаційної безпеки організації про виявлення підозрілої активності в обліковому записі користувача. Основною метою даного сценарію було створення відчуття небезпеки та необхідності негайного реагування.

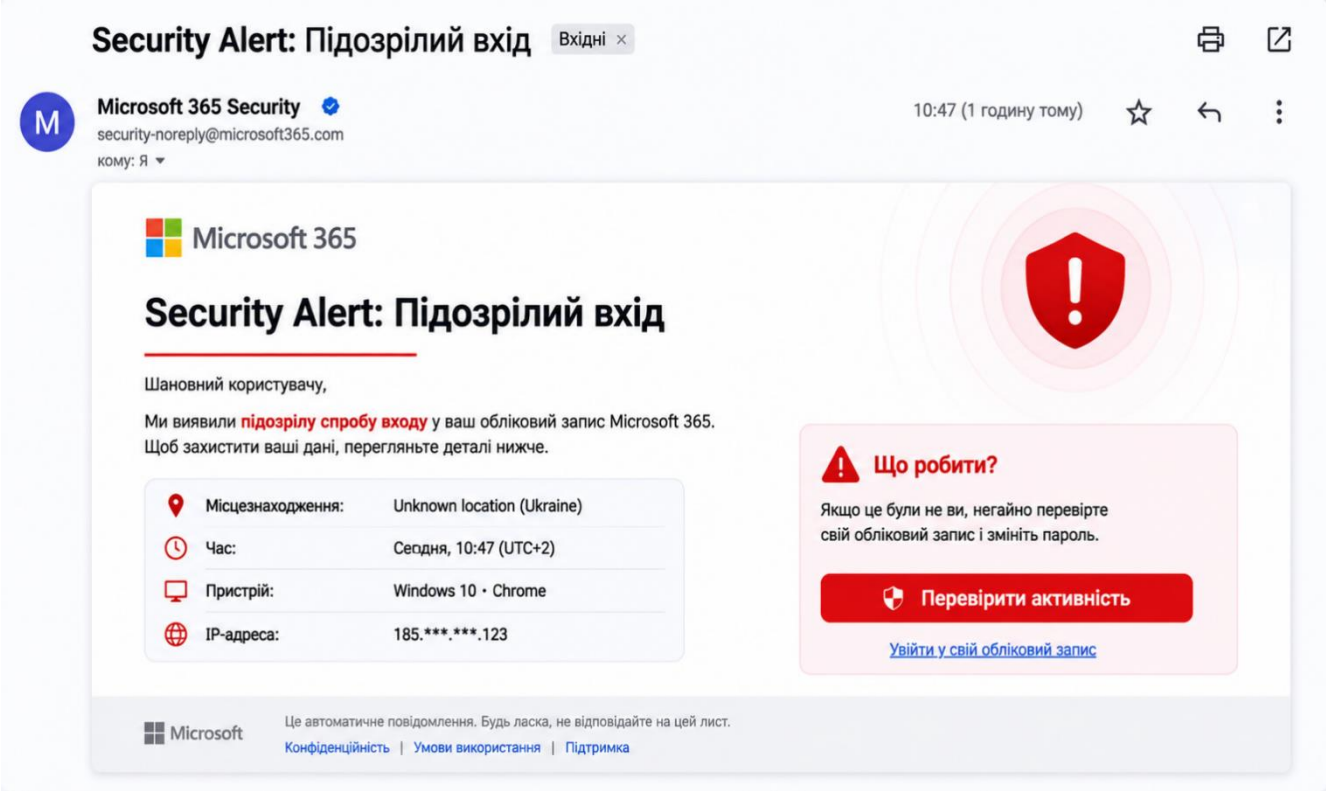

Рисунок 3.2 – Фішинговий лист від служби безпеки

На рисунку 3.2 наведено приклад повідомлення, яке імітує офіційне звернення служби безпеки. Для підвищення достовірності використовувалися елементи корпоративного стилю, службова термінологія та попередження про можливу компрометацію облікового запису. Третій сценарій був орієнтований на використання фінансової тематики та передбачав надсилання повідомлення про необхідність перевірки рахунку або підтвердження фінансової операції. Подібні повідомлення широко використовуються під час атак на бухгалтерські та фінансові підрозділи організацій.

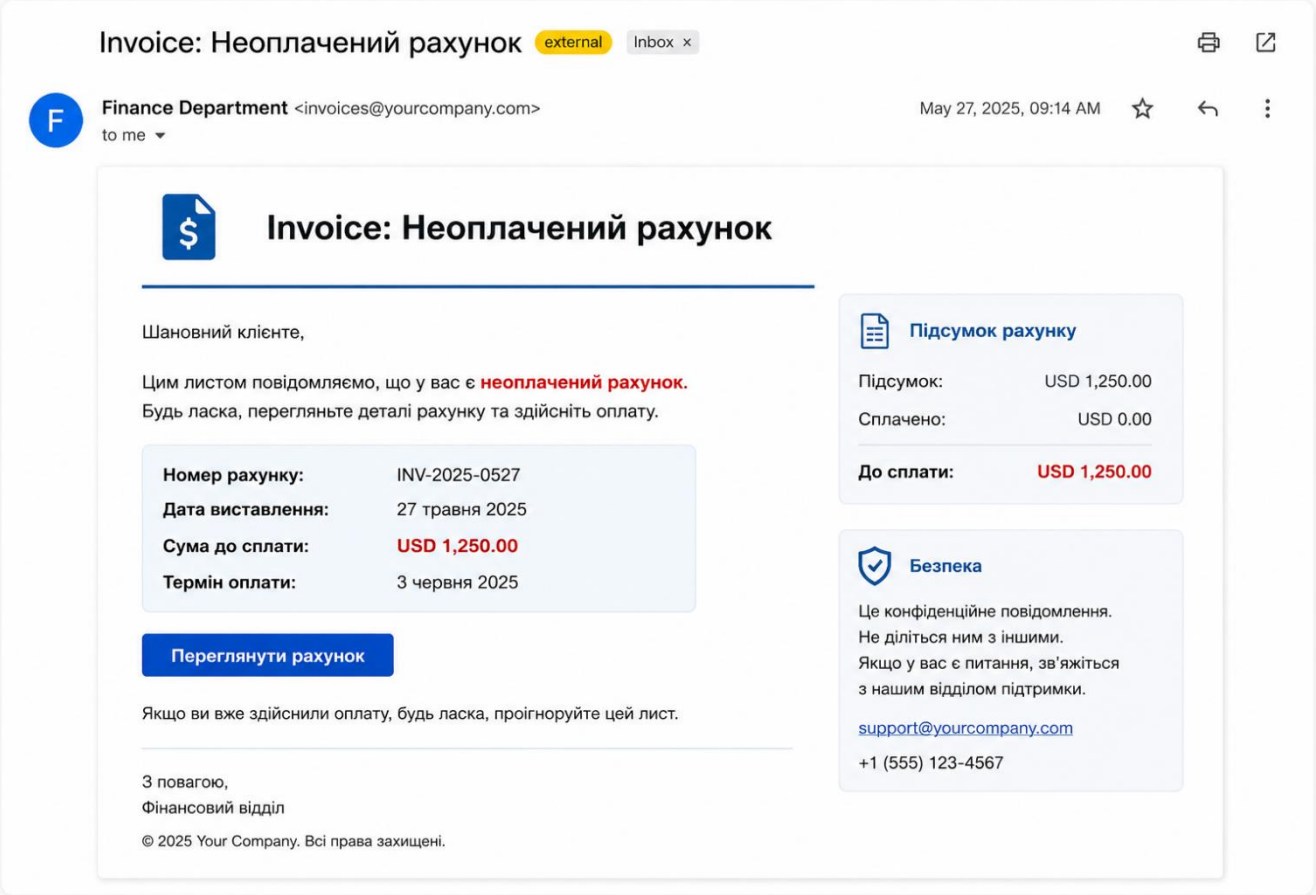

Рисунок 3.3 – Фішинговий лист із фінансовим запитом

Як показано на рисунку 3.3, повідомлення містить вкладення або посилання на ресурс із нібито фінансовими документами. Основний психологічний механізм впливу полягає у використанні цікавості користувача та його прагнення своєчасно виконати службові обов'язки. Четвертий сценарій був спрямований на моделювання атаки типу Business Email Compromise (BEC), також відомої як CEO Fraud. Даний тип атак належить до найбільш небезпечних різновидів соціальної інженерії, оскільки використовує авторитет керівництва організації для впливу на співробітників. Основною метою сценарію було перевірити готовність користувачів виконувати термінові запити, отримані нібито від керівника компанії.

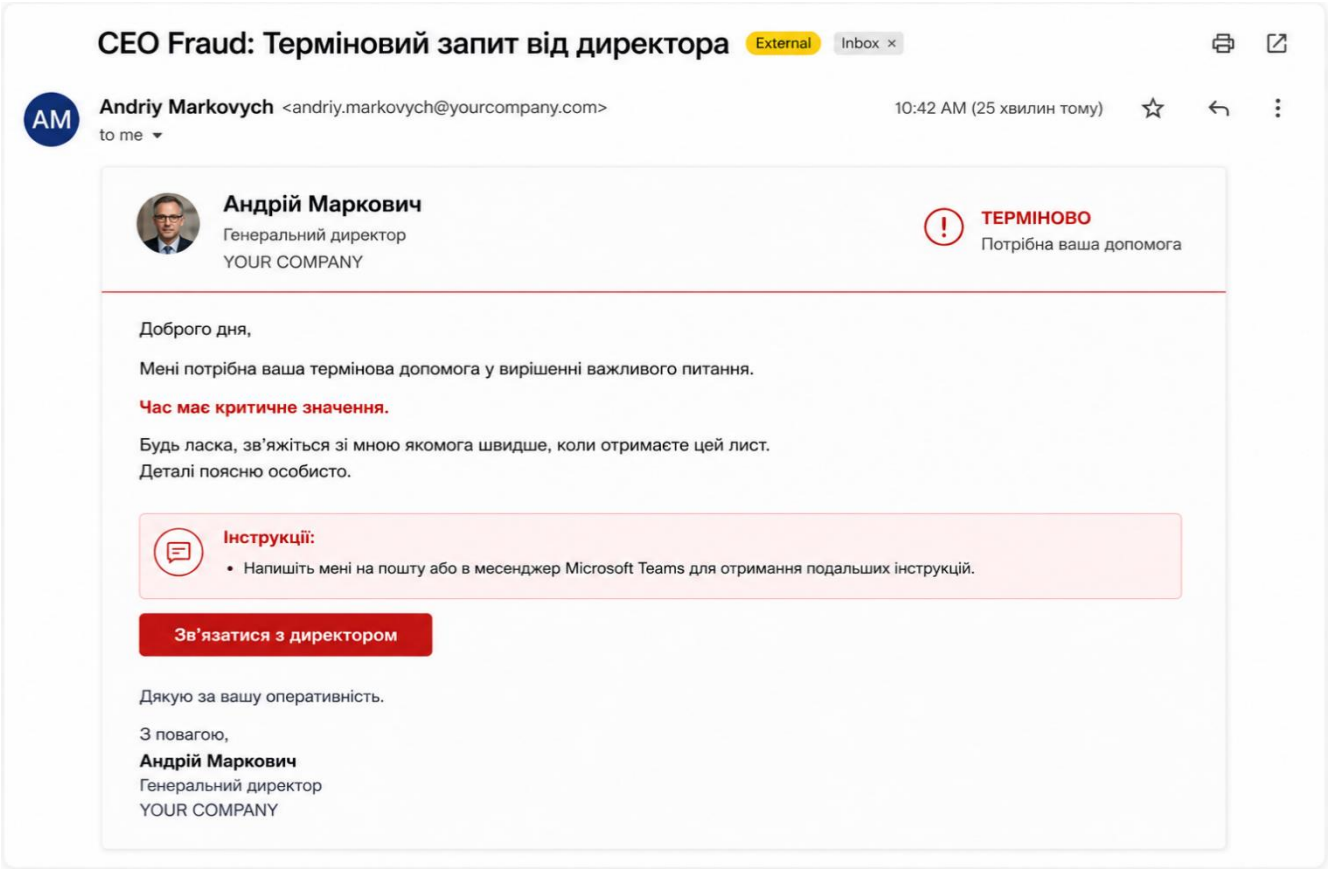

Рисунок 3.4 – Фішинговий лист із використанням сценарію CEO Fraud

Як показано на рисунку 3.4, повідомлення містить характерні ознаки атак типу CEO Fraud. Насамперед використовується апеляція до авторитету керівника та наголос на критичній важливості завдання. Крім того, у листі відсутні деталі запиту, а користувачу пропонується зв'язатися з відправником для отримання подальших інструкцій. Подібний підхід часто використовується зловмисниками для обходу автоматичних систем захисту електронної пошти, оскільки такі повідомлення не містять шкідливих вкладень або підозрілих посилань. Для кожного сценарію були створені окремі шаблони повідомлень та посадкові сторінки, які відтворювали зовнішній вигляд реальних корпоративних сервісів. Це дозволило забезпечити високий рівень достовірності експерименту та максимально наблизити його до умов реальної атаки. Після завершення налаштування всі сценарії були інтегровані до єдиної системи тестування. Платформа Gophish [16] забезпечувала автоматичну доставку повідомлень, контроль переходів за посиланнями та фіксацію всіх дій

користувачів у централізованій базі даних. Таким чином, у лабораторному середовищі було реалізовано комплекс сценаріїв соціальної інженерії, що відображають найбільш поширені методи сучасних фішингових атак та дозволяють оцінити поведінку користувачів у реалістичних умовах.

3.2. Проведення тестування персоналу

Після реалізації сценаріїв було проведено практичне тестування персоналу з використанням створеного лабораторного стенду. Метою експерименту стало визначення рівня стійкості користувачів до атак соціальної інженерії та перевірка ефективності розробленої моделі оцінювання. Тестування проводилося відповідно до методики, розробленої у другому розділі роботи. У дослідженні брали участь 50 користувачів, для яких були підготовлені фішингові повідомлення різних типів. Учасники не були попереджені про проведення тестування, що дозволило отримати максимально об'єктивні результати та виключити вплив зовнішніх факторів на їхню поведінку. Процес тестування складався з кількох послідовних етапів. На першому етапі здійснювалася автоматизована розсилка підготовлених повідомлень. Після доставки листів система розпочинала моніторинг взаємодії користувачів із вмістом повідомлень. Платформа Gophish [16] автоматично реєструвала відкриття листів, переходи за посиланнями, відвідування посадкових сторінок та спроби введення тестових облікових даних. Важливим аспектом проведення тестування було суворе дотримання етичних норм та принципів інформаційної безпеки. У налаштуваннях платформи Gophish функція перехоплення паролів (capture_passwords) була примусово вимкнена. Система фіксувала виключно сам факт взаємодії користувача з формою авторизації, не зберігаючи реальні облікові дані в базі. Це дозволило унеможливити витік конфіденційної інформації та уникнути зайвого психологічного тиску на персонал. Особлива увага приділялася не лише фіксації дій користувачів, але й аналізу їхньої здатності розпізнавати

потенційні загрози. Для цього додатково враховувалися випадки повідомлення служби безпеки про отримання підозрілих листів.

Отримані результати дозволили сформувати повну картину поведінки користувачів під час взаємодії з фішинговими повідомленнями та визначити найбільш уразливі етапи прийняття рішень. Проведене тестування підтвердило доцільність використання phishing simulation як інструменту оцінювання рівня підготовки персоналу та дозволило отримати необхідні дані для подальшого аналізу ефективності сценаріїв соціальної інженерії. Таким чином, проведене тестування стало основою для практичної перевірки розробленого лабораторного стенду та створило необхідний масив даних для оцінювання рівня стійкості користувачів до сучасних кіберзагроз.

3.3 Реалізація та практичне застосування лабораторного стенду

Практичне застосування створеного лабораторного стенду стало завершальним етапом дослідження та дозволило перевірити працездатність усіх компонентів системи в умовах проведення реальної phishing simulation кампанії. Для проведення тестування використовувалася платформа Gophish, яка забезпечує централізоване керування всіма етапами фішингової кампанії. Загальний вигляд інтерфейсу системи під час проведення експерименту наведено на рисунку 3.5.

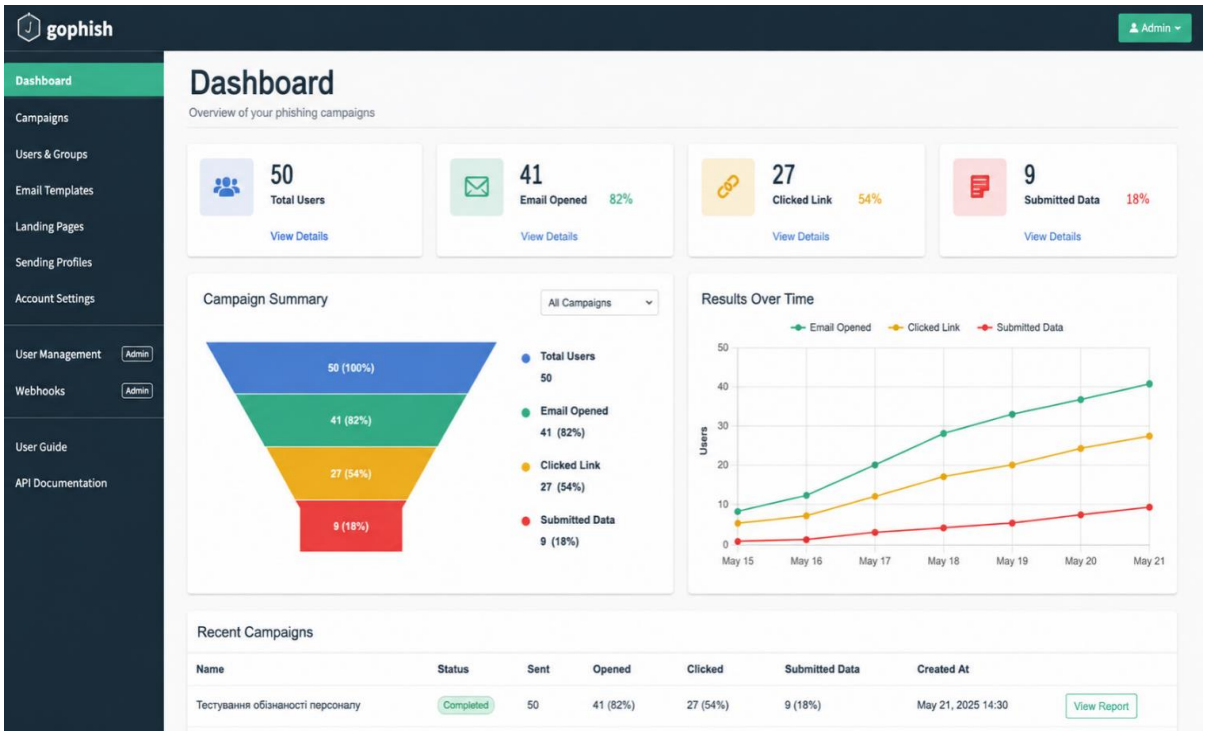

Рисунок 3.5 – Інтерфейс Gophish під час проведення кампанії

Як видно з рисунка 3.5, платформа забезпечує моніторинг процесу розсилання повідомлень, відображення статистики взаємодії користувачів та централізоване керування всіма компонентами кампанії. Під час експерименту лабораторний стенд забезпечив повний цикл моделювання фішингової атаки: від створення сценарію та розсилання повідомлень до збору статистичних даних та формування підсумкових аналітичних звітів. Перед запуском кампанії було сформовано цільову групу користувачів, яка використовувалася для оцінювання рівня стійкості персоналу до фішингових атак. Процес створення групи наведено на рисунку 3.6.

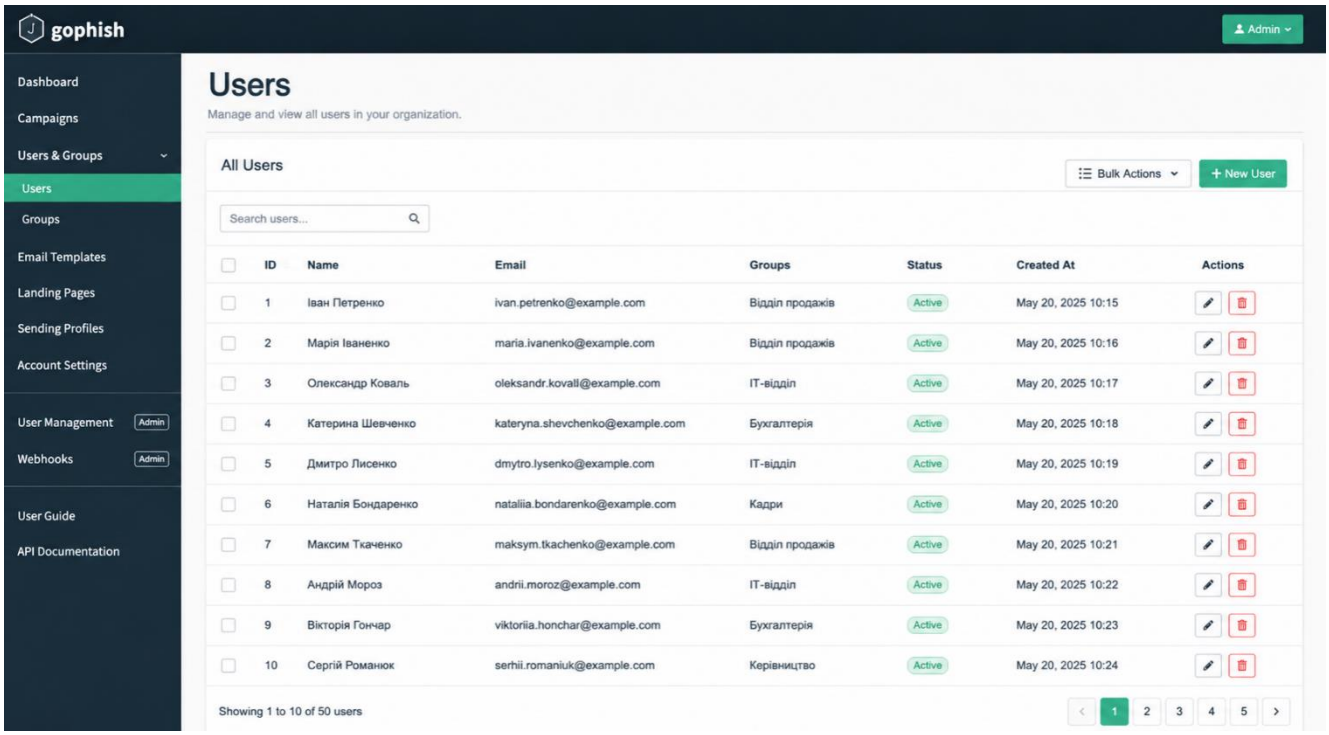

Рисунок 3.6 – Створення цільової групи користувачів

Формування груп користувачів дозволяє проводити тестування різних категорій персоналу та здійснювати подальший аналіз отриманих результатів залежно від ролі користувача в організації. Після підготовки сценаріїв та груп отримувачів було виконано налаштування параметрів фішингової кампанії. Основні параметри запуску кампанії наведено на рисунку 3.7.

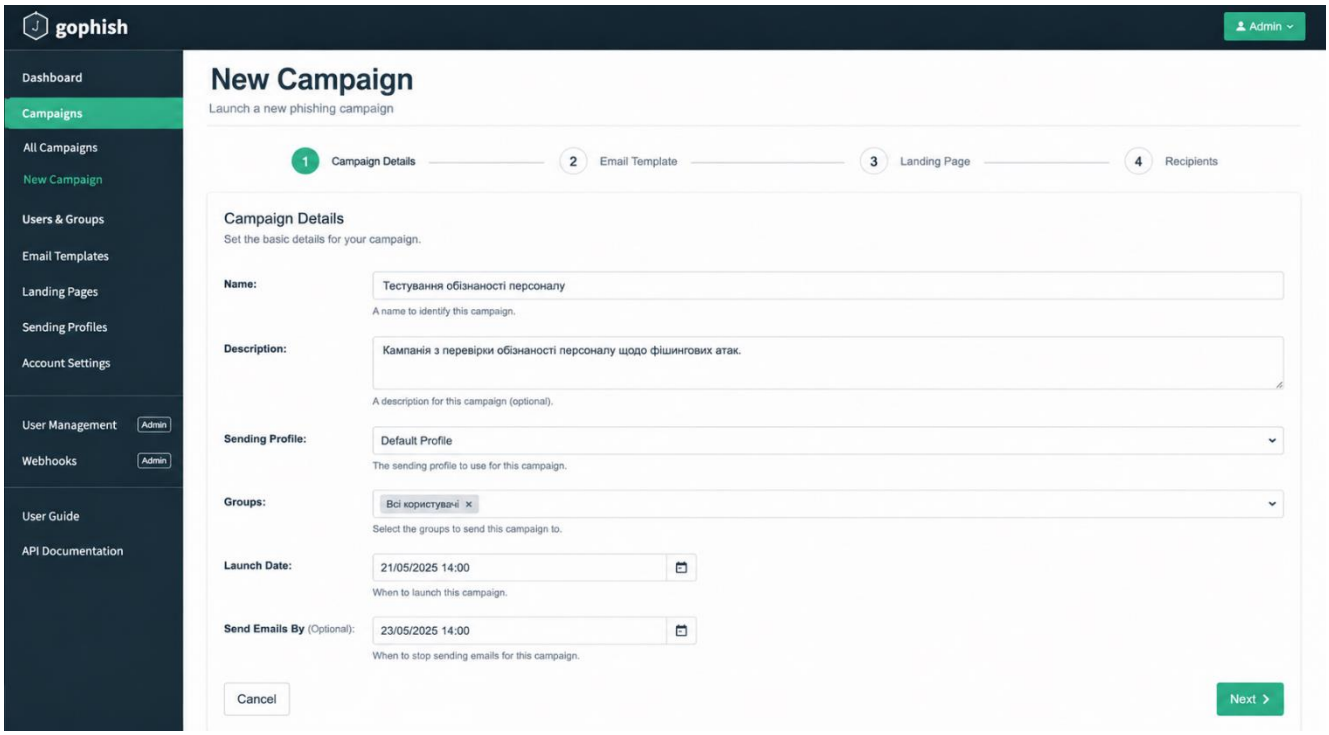

Рисунок 3.7 – Налаштування фішингової кампанії

Під час налаштування кампанії визначалися шаблон повідомлення, посадкова сторінка, група отримувачів та параметри відправлення. Після запуску система автоматично виконувала розсилання повідомлень та збір статистики щодо дій користувачів. За результатами проведеного тестування було встановлено, що із 50 користувачів 41 особа відкрила отримані повідомлення, що становить 82% від загальної кількості учасників експерименту. За посиланнями перейшли 27 користувачів або 54% учасників. Найбільш критичним показником стало введення облікових даних на підготовлених посадкових сторінках - таку дію виконали 9 користувачів, що становить 18% від загальної кількості учасників дослідження. Окрему увагу було приділено аналізу показника повідомлення про інцидент (Report Rate). Результати показали, що лише 22% користувачів повідомили про отримання підозрілого листа. Це свідчить про недостатній рівень сформованої культури інформаційної безпеки та низьку готовність персоналу до участі в процесах виявлення кіберінцидентів. Проведений аналіз також показав, що найбільшу ефективність продемонстрували сценарії, які використовували фактор терміновості та імітацію популярних корпоративних сервісів.

Найуспішнішими виявилися повідомлення, пов'язані з Microsoft 365 та питаннями безпеки облікових записів, що повністю узгоджується з тенденціями, описаними у сучасних звітах Verizon DBIR [8], ENISA [10] та Microsoft Digital Defense Report [12]. Практична експлуатація лабораторного стенду підтвердила його придатність для проведення досліджень у сфері соціальної інженерії та оцінювання рівня кіберобізнаності персоналу. Створене середовище дозволяє проводити як одноразові перевірки, так і регулярні кампанії з навчання користувачів, накопичувати статистику та аналізувати динаміку змін рівня стійкості персоналу в часі [21]. Отримані результати демонструють, що навіть за наявності сучасних технічних засобів захисту людський фактор продовжує залишатися одним із головних джерел ризику для інформаційної безпеки організації. Саме тому використання лабораторних стендів та регулярних phishing simulation кампаній може розглядатися як ефективний інструмент підвищення рівня кібербезпеки та формування культури безпечної поведінки користувачів [1, 3].

3.4 Аналіз отриманих результатів

Після завершення експериментального тестування та збору статистичних даних було проведено комплексний аналіз отриманих результатів з метою визначення рівня стійкості персоналу до фішингових атак та оцінювання ефективності реалізованих сценаріїв соціальної інженерії. Для оцінювання ефективності проведеної phishing simulation кампанії було виконано аналіз статистичних даних, отриманих засобами платформи Gophish. Основними показниками оцінювання стали кількість відкритих повідомлень, переходів за фішинговими посиланнями, випадків введення облікових даних та повідомлень про підозрілі листи. Узагальнені результати тестування наведено в таблиці 3.1.

Таблиця 3.1 – Результати тестування персоналу

Показник	Значення
Кількість учасників	50
Відкрили лист	41
Перейшли за посиланням	27
Ввели облікові дані	9
Повідомили про підозрілий лист	11

Дані, наведені в таблиці 3.1, свідчать про високий рівень взаємодії користувачів із фішинговими повідомленнями. У ході експерименту фішингові повідомлення були доставлені 50 користувачам. Аналіз журналів активності показав, що 41 користувач відкрив отримане повідомлення, що становить 82% від загальної кількості учасників тестування. Даний показник свідчить про високий рівень довіри користувачів до електронних повідомлень та підтверджує, що електронна пошта залишається одним із найбільш ефективних каналів реалізації атак соціальної інженерії. Подальший аналіз показав, що 27 користувачів перейшли за вбудованими фішинговими посиланнями, що становить 54% від загальної кількості учасників дослідження. Цей результат демонструє, що більше половини користувачів не здійснили достатньої перевірки отриманих повідомлень перед виконанням потенційно небезпечної дії. Найбільш критичним показником стало введення облікових даних на підготовлених посадкових сторінках. Подібну дію виконали 9 користувачів, що відповідає 18% від загальної кількості учасників експерименту. Незважаючи на те, що абсолютне значення показника може здаватися відносно невеликим, у реальних умовах навіть компрометація одного облікового запису може призвести до серйозних наслідків для інформаційної безпеки організації, включаючи несанкціонований доступ до корпоративних ресурсів та витік конфіденційної інформації. Окрему увагу привертає показник повідомлення про підозрілі повідомлення. Лише 11

користувачів, або 22% від загальної кількості учасників, повідомили про потенційний інцидент інформаційної безпеки. Незважаючи на позитивний характер даного показника, його значення залишається недостатнім та свідчить про необхідність подальшого розвитку культури інформаційної безпеки, підвищення рівня кіберобізнаності персоналу та вдосконалення механізмів реагування на потенційні кіберінциденти. Отримані результати підтверджують висновки, наведені у звітах Verizon DBIR 2024 [8], Microsoft Digital Defense Report [12] та ENISA Threat Landscape [10], згідно з якими людський фактор продовжує залишатися одним із головних джерел ризику в сучасних інформаційних системах. Навіть за наявності сучасних технічних засобів захисту значна частина успішних кібератак починається саме з компрометації користувача шляхом використання методів соціальної інженерії.

3.5 Статистичний аналіз та оцінка ефективності сценаріїв

Для більш детального дослідження результатів та об'єктивного оцінювання рівня стійкості персоналу було проведено статистичний аналіз ефективності реалізованих сценаріїв соціальної інженерії з використанням стандартизованих метрик кібербезпеки.

Основними розрахунковими параметрами для оцінки фішингових кампаній виступали:

1. Click Rate (CR) - показник клікабельності. Відображає відсоток користувачів, які перейшли за шкідливим посиланням у листі від загальної кількості тих, хто отримав повідомлення. Розраховується за формулою:

CR = (Кількість переходів / Загальна кількість доставлених листів) × 100%

2. Credential Submission Rate (CSR) - показник компрометації облікових даних. Визначає відсоток користувачів, які ввели свої дані на підробленій сторінці авторизації. Розраховується за формулою:

CSR = (Кількість уведених даних / Загальна кількість доставлених листів) × 100%

3. Report Rate (RR) - показник обізнаності. Відображає відсоток співробітників, які розпізнали загрозу та повідомили про неї службу інформаційної безпеки (SOC/IT-відділ). Розраховується за формулою:

RR = (Кількість повідомлень про інцидент / Загальна кількість доставлених листів) × 100%

Побудована воронка взаємодії користувачів із фішинговими повідомленнями показала поступове зменшення кількості учасників на кожному етапі атаки. Із 50 доставлених повідомлень було відкрито 41 лист. Із числа користувачів, які відкрили повідомлення, 27 осіб перейшли за посиланнями (CR = 54%). Завершальним етапом компрометації стало введення облікових даних дев’ятьма користувачами (CSR = 18%). При цьому показник повідомлення про інцидент виявився критично низьким (RR = 22%). Подібна структура повністю відповідає моделі поведінки користувачів, яка спостерігається під час реальних фішингових кампаній. Кожен наступний етап вимагає від користувача більшого рівня довіри до повідомлення, тому кількість потенційних жертв поступово зменшується. Найбільш результативними виявилися сценарії, пов'язані з використанням сервісів Microsoft 365 та повідомленнями від служби безпеки. Як було зазначено у презентаційних матеріалах дослідження, саме сценарії, які використовували фактор терміновості та необхідність негайної реакції користувача, демонстрували найвищі показники переходів за посиланнями та введення облікових даних. Отримані результати узгоджуються з роботами Крістофера Хеднегі та Кевіна Мітніка [6, 7], які зазначають, що найефективнішими механізмами впливу залишаються страх, терміновість та авторитет. Саме ці фактори дозволяють тимчасово знижувати рівень критичного мислення користувачів та підвищують ймовірність успішної реалізації атаки. Статистичний аналіз також показав, що значна частина користувачів не перевіряла достовірність

повідомлень перед виконанням дій. Це свідчить про недостатній рівень практичної підготовки персоналу та необхідність регулярного проведення навчальних заходів і контрольованих симуляцій. Таким чином, результати експерименту підтвердили високу ефективність використаних сценаріїв та дозволили кількісно оцінити найвразливіші аспекти поведінки користувачів за допомогою метрик CR, CSR та RR.

3.6 Аналіз вразливостей **персоналу**

На основі результатів тестування було виконано аналіз основних вразливостей персоналу, які стали причиною успішного проходження окремих етапів фішингових сценаріїв. Першою та найбільш поширеною вразливістю виявилася надмірна довіра до електронних повідомлень. Високий відсоток відкриття листів свідчить про те, що більшість користувачів сприймає електронну пошту як безпечний канал комунікації та не проводить попередню оцінку достовірності повідомлення. Другою вразливістю стала недостатня перевірка джерела інформації. Значна частина користувачів переходила за посиланнями без аналізу адреси відправника, структури доменного імені або інших ознак потенційного шахрайства. Третьою проблемою є схильність до прийняття рішень під впливом емоційного тиску. Найвищу ефективність продемонстрували сценарії, які використовували фактор терміновості та загрозу блокування облікового запису. Це підтверджує, що користувачі часто приймають рішення імпульсивно, не витрачаючи достатньо часу на аналіз ситуації. Четвертою вразливістю є недостатній рівень обізнаності щодо сучасних методів соціальної інженерії. Незважаючи на активний розвиток програм навчання персоналу, багато користувачів усе ще не можуть своєчасно розпізнати добре підготовлені фішингові повідомлення. Окремою проблемою є низький рівень взаємодії зі службами інформаційної безпеки. Показник Report Rate на рівні 22% свідчить про те, що більшість співробітників не сприймає повідомлення про інциденти як власну відповідальність. Подібна ситуація значно ускладнює своєчасне виявлення атак та реагування на них.

Проведений аналіз дозволяє зробити висновок, що основними факторами ризику залишаються психологічні особливості користувачів, недостатня практика протидії фішинговим атакам та відсутність сталої культури інформаційної безпеки [3, 4, 5]. Саме ці аспекти повинні стати основними напрямами подальшого вдосконалення системи підготовки персоналу та підвищення рівня кіберзахисту організації.

3.7 Рекомендації щодо підвищення рівня безпеки

Проведене дослідження показало, що навіть за наявності сучасних технічних засобів захисту персонал залишається одним із найбільш уразливих елементів системи інформаційної безпеки.

Рисунок 3.1 – Результати тестування персоналу

Результати експериментального тестування продемонстрували високий рівень взаємодії користувачів із фішинговими повідомленнями: 82% учасників

відкрили отримані листи, 54% перейшли за посиланнями, а 18% ввели облікові дані на підготовлених посадкових сторінках. Крім того, лише 22% користувачів повідомили про підозрілий лист, що свідчить про недостатній рівень сформованої культури кібербезпеки та низьку залученість персоналу до процесів виявлення кіберзагроз. Отримані результати підтверджують висновки, наведені в ДСТУ ISO/IEC 27001:2015 [1], рекомендаціях NIST SP 800-50 [3] та сучасних аналітичних звітах Verizon DBIR [8], ENISA Threat Landscape [10], Microsoft Digital Defense Report [12] і SANS Security Awareness Report [14]. Згідно з ними, ефективний захист від соціальної інженерії можливий лише за умови поєднання технічних засобів захисту, організаційних заходів та постійного навчання персоналу. Одним із ключових напрямів підвищення рівня безпеки є формування культури інформаційної безпеки в організації. Працівники повинні усвідомлювати власну роль у забезпеченні захисту інформаційних ресурсів та розуміти, що кібербезпека є не лише відповідальністю ІТ-відділу чи служби інформаційної безпеки, а спільним завданням усіх співробітників. Для цього необхідно регулярно проводити навчальні заходи, інформувати персонал про актуальні кіберзагрози та демонструвати реальні приклади атак соціальної інженерії. Важливим елементом підвищення рівня безпеки є впровадження програм безперервного навчання користувачів. Відповідно до рекомендацій NIST SP 800-50 [3] навчання не повинно обмежуватися одноразовими тренінгами або інструктажами. Натомість необхідно створити систему постійного підвищення обізнаності, яка включатиме регулярні курси, вебінари, тематичні розсилки та практичні заняття. Особливу увагу слід приділяти новим методам соціальної інженерії, які активно розвиваються разом із сучасними цифровими технологіями. Значну роль у підвищенні стійкості персоналу відіграє регулярне проведення phishing simulation кампаній. Проведене дослідження підтвердило ефективність такого підходу, оскільки він дозволяє оцінювати не теоретичні знання користувачів, а їхню реальну поведінку в умовах, максимально наближених до справжніх атак. Використання платформ на

кшталт Gophish [16] або KnowBe4 [21] дозволяє автоматизувати процес тестування та відстежувати зміни рівня підготовки персоналу в динаміці. Наступним важливим напрямом є вдосконалення процедур повідомлення про інциденти. Отримані результати показали, що більшість користувачів не повідомляє про отримання підозрілих повідомлень, навіть якщо не взаємодіє з ними. Для виправлення цієї ситуації необхідно створити простий та зрозумілий механізм інформування служби безпеки про потенційні загрози. Працівники повинні чітко розуміти порядок своїх дій у разі виявлення підозрілого листа або іншої ознаки можливої атаки [2, 3]. Окрему увагу необхідно приділяти впровадженню сучасних технічних засобів захисту електронної пошти. Ефективним рішенням є використання багаторівневої системи фільтрації повідомлень, яка поєднує класичні антивірусні механізми з технологіями поведінкового аналізу та машинного навчання. Подібні функції реалізовані у рішеннях класу XDR та SIEM, таких як Microsoft Defender XDR [22], Microsoft Sentinel [23], IBM QRadar [20], Wazuh [27] та CrowdStrike Falcon [18]. Не менш важливим є використання багатофакторної автентифікації. Навіть у випадку успішного отримання облікових даних зловмисник не зможе отримати доступ до системи без проходження додаткового етапу перевірки. У сучасних умовах багатофакторна автентифікація розглядається як один із найбільш ефективних механізмів протидії наслідкам фішингових атак. Для підвищення рівня захищеності також доцільно впроваджувати принцип мінімальних привілеїв. Доступ користувачів до інформаційних ресурсів повинен надаватися виключно в обсязі, необхідному для виконання посадових обов'язків. Такий підхід дозволяє мінімізувати потенційні наслідки компрометації окремого облікового запису. Таким чином, результати проведеного дослідження свідчать, що підвищення рівня безпеки повинно базуватися на комплексному підході, який поєднує організаційні, освітні та технічні заходи. Лише системне вдосконалення всіх складових системи інформаційної безпеки дозволить суттєво знизити ризики, пов'язані з людським фактором та атаками соціальної інженерії.

3.8 Розробка рекомендацій з кібербезпеки для персоналу

На основі проведеного аналізу результатів тестування, виявлених вразливостей та сучасних рекомендацій у сфері кібербезпеки було сформовано комплекс практичних рекомендацій для персоналу, спрямованих на підвищення рівня захищеності від фішингових атак та інших методів соціальної інженерії. Першочерговою рекомендацією є формування звички критичного аналізу будь-яких електронних повідомлень, незалежно від того, хто зазначений відправником. Працівники повинні розуміти, що сучасні фішингові кампанії здатні успішно імітувати корпоративні сервіси, державні установи, фінансові організації та навіть внутрішню переписку компанії. Перед виконанням будь-яких дій необхідно перевіряти адресу відправника, уважно аналізувати зміст повідомлення та звертати увагу на ознаки потенційного шахрайства. Важливим правилом є перевірка вебпосилань перед переходом за ними. Користувач повинен аналізувати доменне ім'я ресурсу, звертати увагу на наявність помилок у написанні адреси та перевіряти використання захищеного з'єднання. Особливу обережність необхідно проявляти у випадках, коли повідомлення містить вимоги терміново перейти за посиланням або виконати певну дію. Працівникам рекомендується ніколи не вводити облікові дані після переходу за посиланням із електронного листа без попередньої перевірки справжності вебресурсу. Якщо виникають сумніви щодо легітимності повідомлення, необхідно самостійно перейти на офіційний сайт організації через браузер або звернутися до відповідальної особи. Окрему увагу слід приділяти повідомленням, які створюють атмосферу терміновості або психологічного тиску. Як показало проведене дослідження, саме такі сценарії продемонстрували найвищу ефективність. Зловмисники часто використовують загрози блокування облікового запису, повідомлення про фінансові операції або термінові запити від керівництва для примушення користувача до необдуманих дій. У подібних ситуаціях необхідно зберігати спокій та виконувати додаткову перевірку отриманої інформації [6, 7].

Працівникам рекомендується використовувати складні унікальні паролі для кожного сервісу та уникати повторного використання однакових облікових даних. Додатково необхідно застосовувати багатофакторну автентифікацію всюди, де це можливо. Навіть у випадку компрометації пароля це значно ускладнює несанкціонований доступ до системи. Важливим елементом кібергігієни є своєчасне оновлення програмного забезпечення та операційних систем. Багато сучасних атак поєднують соціальну інженерію з експлуатацією технічних вразливостей, тому актуальний стан програмного забезпечення суттєво знижує ризик успішної компрометації. Працівники повинні негайно повідомляти службу інформаційної безпеки про будь-які підозрілі повідомлення, вебресурси або інші потенційні ознаки кібератак [2]. Як показали результати проведеного експерименту, саме недостатній рівень повідомлення про інциденти є однією з головних проблем сучасних організацій. Своєчасне інформування дозволяє швидко локалізувати загрозу та запобігти її поширенню серед інших користувачів. Окрему роль відіграє регулярна участь персоналу в навчальних заходах та тренуваннях з кібербезпеки. Практика показує, що знання, які не підкріплюються регулярними вправами та тестуваннями, поступово втрачаються [3]. Саме тому рекомендується періодично проводити контрольовані phishing simulation кампанії та аналізувати результати для подальшого вдосконалення навичок користувачів [16, 21]. Таким чином, розроблені рекомендації спрямовані на формування у персоналу стійких навичок безпечної поведінки в цифровому середовищі. Їх впровадження дозволить підвищити рівень кіберобізнаності користувачів, знизити ймовірність успішної реалізації атак соціальної інженерії та зміцнити загальну систему інформаційної безпеки організації. Наступним етапом роботи є формування підсумкових висновків до третього розділу та узагальнення результатів проведеного дослідження. Ось текст підрозділу 3.9 із розставленими посиланнями на літературу у квадратних дужках відповідно до академічних вимог та наданого вами списку джерел:

3.9 Перспективи розвитку методів протидії фішингу

Стрімкий розвиток цифрових технологій, глобальна цифровізація бізнес-процесів та постійне вдосконалення методів соціальної інженерії зумовлюють необхідність безперервного розвитку засобів протидії фішинговим атакам. Результати проведеного дослідження підтвердили, що навіть за наявності сучасних технічних механізмів захисту людський фактор продовжує залишатися одним із найбільш уразливих елементів системи інформаційної безпеки. Отримані під час експерименту показники відкриття фішингових повідомлень, переходів за посиланнями та введення облікових даних свідчать про те, що традиційні підходи до навчання персоналу вже не забезпечують достатнього рівня захисту від сучасних соціотехнічних загроз. Саме тому подальший розвиток методів протидії фішингу повинен базуватися на комплексному поєднанні технічних, організаційних та поведінкових механізмів безпеки [4, 5]. Одним із найперспективніших напрямів розвитку є використання технологій штучного інтелекту та машинного навчання для автоматичного виявлення фішингових атак. Якщо традиційні системи захисту здебільшого базуються на сигнатурному аналізі або перевірці відомих шаблонів загроз, то сучасні алгоритми штучного інтелекту здатні аналізувати поведінку користувачів, структуру повідомлень, особливості мережевого трафіку та виявляти потенційні загрози навіть у випадках, коли вони раніше не зустрічалися в базах даних. Подібні підходи активно реалізуються в сучасних рішеннях класу XDR та SIEM, зокрема в системах Microsoft Defender XDR [22], CrowdStrike Falcon [18], Darktrace [19] та Microsoft Sentinel [23]. Важливим напрямом розвитку є впровадження поведінкової аналітики користувачів. Сучасні системи кібербезпеки дедалі частіше використовують концепцію User and Entity Behavior Analytics (UEBA), яка передбачає постійний моніторинг активності користувачів та автоматичне виявлення аномалій. Якщо користувач раптово починає виконувати нетипові дії, система може автоматично згенерувати попередження або обмежити доступ до

критично важливих ресурсів. Такий підхід реалізується в рішеннях Splunk User Behavior Analytics [26] та IBM QRadar [20]. Особливого значення набуває розвиток концепції Zero Trust Security. Традиційна модель захисту передбачає довіру до користувача після успішної автентифікації. Натомість концепція Zero Trust базується на принципі «ніколи не довіряй, завжди перевіряй». У межах такого підходу кожна дія користувача проходить додаткову перевірку незалежно від його місцезнаходження або попереднього рівня довіри. Саме ця концепція розглядається багатьма експертами як один із ключових напрямів розвитку кібербезпеки в найближчі роки. Окремим перспективним напрямом є вдосконалення механізмів багатофакторної автентифікації. Сучасні фішингові кампанії дедалі частіше спрямовані на викрадення облікових даних користувачів. Використання додаткових факторів автентифікації значно ускладнює реалізацію подібних атак навіть у випадку успішної компрометації пароля. У майбутньому очікується більш широке впровадження біометричних методів автентифікації, апаратних токенів безпеки та безпарольних технологій доступу. Значний потенціал мають технології автоматизованого реагування на інциденти. Сучасні рішення класу SOAR дозволяють не лише виявляти потенційні загрози, але й автоматично виконувати дії з локалізації інциденту. Наприклад, система може самостійно заблокувати підозрілий обліковий запис, ізолювати робочу станцію від мережі або заборонити доступ до потенційно небезпечного вебресурсу. Подібний підхід дозволяє суттєво скоротити час реагування на атаки та мінімізувати можливі наслідки компрометації. Перспективним напрямом розвитку залишається використання постійних програм підвищення обізнаності персоналу. Результати проведеного дослідження показали, що значна частина користувачів залишається вразливою до методів соціальної інженерії. У зв'язку з цим сучасні організації все частіше переходять від одноразових навчальних курсів до концепції безперервного навчання. Відповідно до рекомендацій NIST SP 800-50 [3] та сучасних підходів, реалізованих у платформах на кшталт KnowBe4 [21], процес навчання повинен бути інтегрований у повсякденну діяльність

працівників та супроводжуватися регулярними практичними тренуваннями. Окремої уваги заслуговує розвиток технологій моделювання фішингових атак. Створений у межах даної роботи лабораторний стенд демонструє ефективність використання phishing simulation для оцінювання рівня підготовки персоналу. У майбутньому подібні системи можуть бути інтегровані з корпоративними платформами навчання, автоматично адаптувати сценарії під конкретних користувачів та використовувати результати попередніх тестувань для формування індивідуальних програм підготовки [16]. Водночас розвиток технологій штучного інтелекту створює нові виклики для систем захисту. Сучасні зловмисники вже починають використовувати генеративні моделі для створення високоякісних фішингових повідомлень, автоматизованого збору інформації про потенційних жертв та генерації персоналізованих сценаріїв атак. Крім того, поширення технологій Deepfake створює додаткові ризики використання підроблених голосових або відеоповідомлень для реалізації складних схем соціальної інженерії. У зв'язку з цим системи протидії фішингу повинні розвиватися випереджальними темпами та використовувати аналогічні технології штучного інтелекту для виявлення нових типів загроз [10]. Подальший розвиток методів протидії фішингу також пов'язаний із поглибленням інтеграції між різними компонентами систем кібербезпеки. У майбутньому очікується активне використання єдиних платформ, які поєднуватимуть функції моніторингу, аналізу поведінки користувачів, виявлення загроз, автоматизованого реагування та навчання персоналу [1]. Такий підхід дозволить створити багаторівневу систему захисту, здатну ефективно протистояти як технічним, так і соціотехнічним атакам. Таким чином, перспективи розвитку методів протидії фішингу пов'язані з переходом від реактивної моделі захисту до проактивного управління ризиками. Майбутні системи інформаційної безпеки будуть поєднувати штучний інтелект, поведінкову аналітику, автоматизоване реагування, багатофакторну автентифікацію та безперервне навчання персоналу. Проведене дослідження підтвердило, що саме комплексний підхід до забезпечення інформаційної

безпеки є найбільш ефективним способом зниження ризиків, пов'язаних із фішинговими атаками та соціальною інженерією, а створений лабораторний стенд може слугувати основою для подальших досліджень та вдосконалення методів оцінювання стійкості персоналу до сучасних кіберзагроз.

3.10 Висновки до розділу 3

У третьому розділі було виконано практичну реалізацію розробленого лабораторного стенду та проведено експериментальне дослідження стійкості персоналу до фішингових атак. На основі сформованих у попередніх розділах теоретичних положень, моделі оцінювання та методики тестування було реалізовано комплекс сценаріїв соціальної інженерії, які відтворюють найбільш поширені сучасні способи проведення фішингових кампаній [16]. Створене середовище дозволило максимально наблизити умови тестування до реальних атак та забезпечити об'єктивний збір статистичних даних щодо поведінки користувачів. У межах практичної частини дослідження було проведено тестування групи користувачів із використанням розроблених сценаріїв. Отримані результати підтвердили актуальність проблеми людського фактора в системі інформаційної безпеки. Аналіз дій користувачів показав високий рівень взаємодії з фішинговими повідомленнями, що свідчить про наявність суттєвих ризиків компрометації облікових записів та інформаційних ресурсів організації [8, 12]. Значна частина учасників відкривала повідомлення, переходила за посиланнями та виконувала дії, які в реальних умовах могли б призвести до витоку конфіденційної інформації або несанкціонованого доступу до корпоративних систем. Проведений аналіз результатів дозволив виявити основні причини успішності фішингових атак. Найбільший вплив на користувачів мали сценарії, що використовували психологічні механізми терміновості, авторитету та страху втрати доступу до корпоративних ресурсів [6, 7]. Отримані результати підтвердили висновки сучасних досліджень у сфері соціальної інженерії та продемонстрували, що навіть за наявності технічних засобів захисту саме поведінка користувача

часто стає вирішальним фактором успішності атаки. У процесі дослідження було виконано статистичний аналіз отриманих даних та проведено оцінювання ефективності розроблених сценаріїв. Результати показали, що найбільшу небезпеку становлять добре підготовлені повідомлення, які імітують роботу популярних корпоративних сервісів та використовують актуальні для користувачів теми. Водночас було встановлено недостатній рівень повідомлення про підозрілі інциденти, що свідчить про потребу подальшого розвитку культури інформаційної безпеки в організаціях [2, 14]. На основі отриманих результатів було проведено аналіз вразливостей персоналу та визначено ключові проблеми, які впливають на рівень стійкості користувачів до соціальної інженерії. До таких проблем належать недостатня увага до перевірки джерел інформації, надмірна довіра до електронних повідомлень, схильність до прийняття рішень під психологічним тиском та недостатня обізнаність щодо сучасних кіберзагроз [4, 5, 10]. Виявлені особливості поведінки користувачів дозволили сформувати практичні рекомендації щодо підвищення рівня захищеності персоналу. У межах розділу також було розроблено комплекс рекомендацій з кібербезпеки, спрямованих на вдосконалення системи навчання персоналу, розвиток культури інформаційної безпеки, впровадження регулярних тренувань із використанням phishing simulation кампаній та застосування сучасних технічних засобів захисту [1, 3, 21]. Запропоновані заходи дозволяють суттєво знизити ймовірність успішної реалізації атак соціальної інженерії та підвищити загальний рівень захищеності організації. Окрему увагу було приділено аналізу перспектив розвитку методів протидії фішингу. Встановлено, що подальше підвищення ефективності захисту буде пов'язане з активним використанням технологій штучного інтелекту, поведінкової аналітики, концепції Zero Trust, багатофакторної автентифікації та автоматизованих систем реагування на інциденти [18, 19, 20, 23, 26]. Також важливим напрямом розвитку залишається вдосконалення методів навчання користувачів та створення адаптивних систем оцінювання рівня їхньої кіберобізнаності. Таким чином, результати

практичного дослідження підтвердили досягнення поставленої мети роботи та довели ефективність розробленого лабораторного стенду як інструменту оцінювання стійкості персоналу до фішингових атак. Створене середовище забезпечує можливість моделювання реалістичних сценаріїв соціальної інженерії, збору статистичних даних та формування обґрунтованих рекомендацій щодо підвищення рівня інформаційної безпеки. Отримані результати можуть бути використані як основа для впровадження програм підвищення кіберобізнаності персоналу, удосконалення систем управління інформаційною безпекою та подальших наукових досліджень у сфері протидії фішинговим атакам і соціальній інженерії [1, 3].

ВИСНОВКИ

У процесі виконання дипломної роботи було досліджено сучасний стан проблеми протидії фішинговим атакам та соціальній інженерії, які залишаються одними з найбільш актуальних загроз інформаційній безпеці організацій. Проведений аналіз наукових праць та розроблена модель безпосередньо забезпечує досягнення ключових програмних результатів навчання (ПРН-3, ПРН-7, ПРН-9, ПРН-11, ПРН-14) Стандарту спеціальності 125 «Кібербезпека» та міжнародних стандартів та аналітичних звітів провідних компаній у сфері кібербезпеки підтвердив, що людський фактор продовжує залишатися одним із найуразливіших елементів систем захисту інформації. Незважаючи на постійний розвиток технічних засобів захисту, значна кількість успішних кіберінцидентів пов'язана саме з використанням методів соціальної інженерії та фішингових атак. У першому розділі роботи було розглянуто теоретичні аспекти соціальної інженерії, психологічні механізми впливу на користувачів, причини ефективності соціотехнічних атак, класифікацію фішингових загроз та сучасні методи протидії їм. Особливу увагу приділено ролі людського фактора в системі інформаційної безпеки та проблематиці оцінювання рівня стійкості персоналу до сучасних кіберзагроз. Проведений аналіз показав, що традиційні технічні засоби захисту не забезпечують повного усунення ризиків, пов'язаних із помилками користувачів, а тому необхідним є впровадження практичних методів перевірки рівня кіберобізнаності персоналу. У другому розділі було виконано проєктування лабораторного стенду для моделювання фішингових атак та оцінювання стійкості користувачів до методів соціальної інженерії. Проведено аналіз існуючих підходів до тестування персоналу, розроблено модель оцінювання стійкості користувачів, сформовано методику проведення тестування та спроєктовано архітектуру лабораторного середовища. Для реалізації поставлених завдань було обрано платформу VMware Workstation Pro, операційну систему Kali Linux та платформу Gophish, що забезпечили

можливість створення контрольованого середовища для проведення експериментів і збору статистичних даних. У третьому розділі здійснено практичну реалізацію розробленого лабораторного стенду та проведено експериментальне дослідження стійкості персоналу до фішингових атак. У межах роботи було реалізовано декілька сценаріїв соціальної інженерії, які моделювали сучасні фішингові кампанії. За результатами тестування встановлено, що з 50 учасників експерименту 41 користувач відкрив отримані повідомлення, 27 перейшли за фішинговими посиланнями, а 9 осіб ввели свої облікові дані на підготовлених посадкових сторінках. Водночас лише 11 користувачів повідомили про підозрілу активність. Отримані результати підтвердили високий рівень впливу людського фактора на загальний рівень інформаційної безпеки організації та продемонстрували необхідність систематичного навчання персоналу. На основі проведеного дослідження було виконано аналіз ефективності використаних сценаріїв, визначено основні вразливості користувачів та розроблено комплекс рекомендацій щодо підвищення рівня кібербезпеки. Запропоновані рекомендації охоплюють організаційні, технічні та освітні заходи, включаючи регулярне проведення phishing simulation кампаній, впровадження багатофакторної автентифікації, розвиток культури інформаційної безпеки та використання сучасних засобів моніторингу кіберзагроз. Мета дипломної роботи - розробка та практична реалізація лабораторного стенду для моделювання фішингових атак з метою оцінювання рівня стійкості персоналу до методів соціальної інженерії - була повністю досягнута. Усі поставлені завдання виконані в повному обсязі. Створений лабораторний стенд забезпечує можливість проведення контрольованих фішингових кампаній, збору статистичних даних, оцінювання рівня кіберобізнаності персоналу та формування обґрунтованих рекомендацій щодо підвищення рівня захищеності організації. Практична значущість роботи полягає у можливості використання розробленого стенду як навчального та дослідницького інструменту для оцінювання стійкості персоналу до соціотехнічних загроз. Результати дослідження можуть бути використані під

час організації програм підвищення кіберобізнаності, проведення внутрішніх аудитів безпеки та вдосконалення систем управління інформаційною безпекою. Подальший розвиток дослідження може бути пов'язаний із розширенням функціональних можливостей лабораторного стенду, інтеграцією систем поведінкової аналітики, використанням технологій штучного інтелекту для автоматичного створення сценаріїв соціальної інженерії та впровадженням засобів автоматизованого аналізу результатів тестування. Це дозволить підвищити точність оцінювання рівня підготовки користувачів та забезпечити більш ефективну протидію сучасним кіберзагрозам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. Київ : ДП «УкрНДНЦ», 2016. 34 с.

2 NIST Special Publication 800-61 Revision 2. Computer Security Incident Handling Guide. Gaithersburg : National Institute of Standards and Technology, 2012. 147 p.

3 NIST Special Publication 800-50. Building an Information Technology Security Awareness and Training Program. Gaithersburg : National Institute of Standards and Technology, 2003. 68 p.

4 Конахович Г. Ф., Пацай Б. П. Захист інформації в комп'ютерних системах і мережах. Київ : ВВ ПВП «Задруга», 2006. 715 с.

5 Хорошко В. А., Чекатков А. А. Методи та засоби захисту інформації. Київ : Юніор, 2003. 504 с.

6 Hadnagy C. Social Engineering: The Science of Human Hacking. 2nd ed. Indianapolis : John Wiley & Sons, 2018. 320 p.

7 Mitnick K. D., Simon W. L. The Art of Deception: Controlling the Human Element of Security. Indianapolis : John Wiley & Sons, 2002. 352 p.

8 2024 Data Breach Investigations Report (DBIR) / Verizon. 2024. URL: https://www.verizon.com/business/resources/reports/dbir/ (дата звернення: 05.06.2026).

9 CrowdStrike 2024 Global Threat Report / CrowdStrike. 2024. URL: https://www.crowdstrike.com/global-threat-report/ (дата звернення: 05.06.2026).

10 ENISA Threat Landscape 2023 / European Union Agency for Cybersecurity. 2023. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (дата звернення: 05.06.2026).

11 X-Force Threat Intelligence Index 2024 / IBM Security. 2024. URL: https://www.ibm.com/reports/threat-intelligence (дата звернення: 05.06.2026).

12 Microsoft Digital Defense Report 2023 / Microsoft Security. 2023. URL: https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report (дата звернення: 05.06.2026).

13 OWASP Top 10:2021. The Ten Most Critical Web Application Security Risks / OWASP Foundation. 2021. URL: https://owasp.org/Top10/ (дата звернення: 05.06.2026).

14 SANS 2024 Security Awareness Report / SANS Institute. 2024. URL: https://www.sans.org/white-papers/2024-security-awareness-report/ (дата звернення: 05.06.2026).

15 Kali Linux Official Documentation / Kali Linux. URL: https://www.kali.org/docs/ (дата звернення: 05.06.2026).

16 Gophish Open-Source Phishing Framework / Gophish. URL: https://getgophish.com/documentation/ (дата звернення: 05.06.2026).

17 VMware Workstation Pro Documentation / VMware. URL: https://docs.vmware.com/en/VMware-Workstation-Pro/ (дата звернення: 05.06.2026).

18 CrowdStrike Falcon Platform / CrowdStrike. URL: https://www.crowdstrike.com/falcon-platform/ (дата звернення: 05.06.2026).

19 Darktrace Cyber AI Platform / Darktrace. URL: https://darktrace.com/ (дата звернення: 05.06.2026).

20 IBM QRadar SIEM Documentation / IBM. URL: https://www.ibm.com/products/qradar-siem (дата звернення: 05.06.2026).

21 Security Awareness Training and Simulated Phishing Platform / KnowBe4. URL: https://www.knowbe4.com/ (дата звернення: 05.06.2026).

22 Microsoft Defender XDR Documentation / Microsoft Learn. URL: https://learn.microsoft.com/en-us/defender-xdr/ (дата звернення: 05.06.2026).

23 Microsoft Sentinel Documentation / Microsoft Learn. URL: https://learn.microsoft.com/en-us/azure/sentinel/ (дата звернення: 05.06.2026).

24 Cybersecurity and Compliance Solutions / Proofpoint. URL: https://www.proofpoint.com/ (дата звернення: 05.06.2026).

25 Splunk Enterprise Security Product Documentation / Splunk. URL: https://docs.splunk.com/Documentation/ES (дата звернення: 05.06.2026).

26 Splunk User Behavior Analytics (UBA) / Splunk. URL: https://docs.splunk.com/Documentation/UBA (дата звернення: 05.06.2026).

27 Wazuh Open Source XDR and SIEM Documentation / Wazuh. URL: https://documentation.wazuh.com/ (дата звернення: 05.06.2026).

28 Cisco Secure Products and Solutions / Cisco. URL: https://www.cisco.com/c/en/us/products/security/index.html (дата звернення: 05.06.2026).

ДОДАТКИ

ДОДАТОК А

Шаблони фішингових повідомлень, розроблені для тестування персоналу

У даному додатку наведено приклади шаблонів фішингових повідомлень, які використовувалися під час проведення експериментального тестування персоналу в межах дослідження.

Сценарій 1: Імітація системного повідомлення про зміну пароля (Microsoft 365)

Відправник: Відділ технічної підтримки support@secure-company365-alert.com

Тема: Термінове оновлення корпоративного пароля

Текст повідомлення:

Шановний користувачу!

Система безпеки зафіксувала підозрілу активність у вашому корпоративному обліковому записі. Відповідно до політики безпеки, ваш поточний пароль буде деактивовано через 15 хвилин.

Для збереження доступу до сервісів Microsoft 365 та уникнення блокування, будь ласка, терміново підтвердьте свої облікові дані за посиланням нижче:

[Підтвердити обліковий запис] *(посилання веде на фішингову сторінку авторизації)*

Якщо ви не виконаєте цю дію, ваш обліковий запис буде автоматично заблоковано до з'ясування обставин.

З повагою,

Відділ технічної підтримки

Сценарій 2: Сповіщення від служби безпеки (Security Alert)

Відправник: Security Operations Center soc-alerts@company-secure-verification.net

Тема: Security Alert: Підозрілий вхід у систему

Текст повідомлення:

Увага!

Система інформаційної безпеки виявила спробу несанкціонованого входу до вашого корпоративного акаунта з нового пристрою (IP: 192.168.x.x, локація: закордон).

Якщо це були не ви, вам необхідно негайно пройти перевірку безпеки та відхилити запит на авторизацію:

[Перейти до порталу безпеки] *(посилання веде на лендінг GoPhish)*

У разі відсутності підтвердження протягом 1 години, доступ до корпоративної мережі буде обмежено.

Сценарій 3: Фінансовий фішинг (Invoice phishing)

Відправник: Фінансовий департамент accounting@finance-secure-docs.com

Тема: Invoice #4721 - потребує підтвердження

Текст повідомлення:

Доброго дня.

У додатку надсилаємо оновлений рахунок (Invoice #4721) для підтвердження та подальшої обробки платежу.

Документ завантажено у захищене корпоративне сховище. Переглянути деталі можна за посиланням:

[Переглянути Invoice_4721.pdf] *(посилання веде на сторінку перехоплення сесії)*

Просимо перевірити реквізити та підтвердити оплату до 16:00 поточного робочого дня.

З повагою,

Фінансовий відділ

ДОДАТОК Б

Структурна та мережева схема лабораторного стенда

Опис схеми:

1. **Host-система (Фізичний комп'ютер):** Забезпечує роботу гіпервізора (VMware Workstation).
2. **Virtual Network (VMnet - Host-Only / NAT):** Ізольована віртуальна мережа (підмережа 192.168.50.0/24), яка обмежує вихід фішингового трафіку у реальну мережу Інтернет.
3. **VM 1: Сервер Атаки (Kali Linux):**
    - IP-адреса: 192.168.50.10
    - Розгорнуті сервіси: GoPhish (порт 3333 для адміністрування, порт 80/443 для фішингових лендінгів), локальний DNS-сервер (для резолвінгу підроблених доменів).
4. **VM 2: Робоча станція жертви (Windows 10/11):**
    - IP-адреса: 192.168.50.20
    - Встановлене ПЗ: MS Outlook / браузер Chrome, підключення до локального поштового сервера.

ДОДАТОК В

Приклад конфігурації фішингової кампанії у платформі GoPhish (JSON)

У цьому додатку наведено фрагмент JSON-конфігурації, який використовувався для автоматизованого запуску сценарію "Повідомлення про зміну пароля" через API платформи GoPhish.

JSON

{

"name": "Password Reset Campaign - IT Dept",

"template": {

"name": "O365 Password Expiration",

"subject": "Термінове оновлення корпоративного пароля",

"text": "",

"html": "<html><body> Шановний користувачу! Ваш пароль буде деактивовано через 15 хвилин. Підтвердити обліковий запис </body></html>"

},

"url": "http://secure-company365-support.com",

"page": {

"name": "Microsoft 365 Fake Login",

<html>...[фрагмент навчальної посадкової сторінки]...</html>
"capture_credentials": true,

"capture_passwords": false,

"redirect_url": "https://office.com"

},

"smtp": {

"name": "Internal SMTP Relay",

```
    "host": "192.168.50.10:25",
    "from_address": "IT Support <support@secure-company365-alert.com>"
  },
  "groups": [
    {"name": "Office Personnel"}
  ]
}
```


(Примітка: параметр capture_passwords встановлено у false з метою дотримання етичних норм та безпечності тестування, фіксується лише факт спроби введення даних).