

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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

**«Технологія виявлення атак соціальної інженерії для користувачів в
корпоративній системі організації»**

зі спеціальності

125 Кібербезпека та захист інформації

(код, найменування спеціальності)

освітньо-професійної програми

Інформаційна та кібернетична безпека

(назва програми)

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

Асія ПРОЦЕНКО

(підпис)

Виконала: здобувачка вищої освіти групи **БСДМ-61**

ПРОЦЕНКО Асія

(прізвище, ім'я)

Керівник

д.т.н., професор ГАЙДУР Галина

(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент

(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ
ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ**

Кафедра Систем та технологій кібербезпеки

Ступінь вищої освіти Магістр

Спеціальність 125 Кібербезпека та захист інформації

Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ

Завідувач кафедри

Систем та технологій
кібербезпеки

_____ Галина ГАЙДУР
“ ____ ” _____ 2026 року

**З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ**

ЧАБАН Анастасії Іванівни

(прізвище, ім'я)

1. Тема кваліфікаційної роботи: «Технологія виявлення атак соціальної
для користувачів в корпоративній системі організації»

керівник кваліфікаційної роботи Гайдур Галина Іванівна, д.т.н., професор
(прізвище, ім'я, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних
технологій від « ____ » _____ 2026 року № ____.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 12.01.2026 р.

3. Вихідні дані до кваліфікаційної роботи _____

інформаційні ресурси організації;

наукова та технічна література, експлуатаційна документація, нормативні
документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно
розробити)

1. Дослідження проблеми соціально-інженерних атак у корпоративних
середовищах та аналіз причин їх успішності серед користувачів

2. Аналіз інструментів моделювання фішингових атак: можливості Gophish та
Evilginx у побудові сценаріїв соціальної інженерії

3. Розроблення методології моделювання соціально-інженерної атаки в

корпоративній системі з використанням Gophish та Evilginx.

4. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 01.10.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми успішності соціально-інженерних атак у корпоративних системах	30.12.2025 р.	
2.	Аналіз наукової та технічної літератури з питань соціально-інженерних атак	30.12.2025 р.	
3.	Аналіз методів і засобів моделювання фішингових атак за допомогою інструментів Gophish та Evilginx	31.12.2025 р.	
4.	Розробка методології моделювання фішингових атак в корпоративному середовищі	01.01.2026 р.	
5.	Розроблення рекомендацій щодо проведення та захисту від фішингових атак корпоративному середовищі	01.01.2026 р.	
6.	Оформлення результатів дослідження.	01.01.2026 р.	
7.	Підготовка доповіді до захисту.	01.01.2026 р.	

Здобувачка вищої освіти

(підпис)

Асія ПРОЦЕНКО

(ім'я, прізвище)

Керівник кваліфікаційної роботи

(підпис)

Галина ГАЙДУР

(ім'я, прізвище)

ВІДГУК РЕЦЕНЗЕНТА на кваліфікаційну роботу

здобувачки ЧАБАН Анастасії

на тему: «Технологія виявлення атак соціальної інженерії для користувачів в корпоративній системі організації»

Актуальність: Атаки на основі соціальної інженерії залишаються однією з найпоширеніших загроз для корпоративних систем, оскільки зловмисники експлуатують психологічні фактори та недостатню обізнаність користувачів. Незважаючи на наявність технічних засобів захисту, саме поведінка співробітників часто стає слабкою ланкою безпеки, що робить дослідження причин успішності таких атак надзвичайно важливим.

Особливо актуальним є використання інструментів моделювання фішингових атак, таких як Gophish та Evilginx, для створення контрольованих сценаріїв соціальної інженерії. Розроблення методології моделювання таких атак дозволяє оцінити вразливість користувачів, підвищити їхню обізнаність і зміцнити безпеку корпоративної системи, що робить тему роботи своєчасною та значущою.

Позитивні сторони:

1. На основі проведеного аналізу встановлено актуальність проблеми соціально-інженерних атак у корпоративних системах та визначено мету і завдання дослідження, а також ключові етапи моделювання атак.
2. Досліджено проблеми соціально-інженерних атак у корпоративних системах та проаналізовано причини їх успішності серед користувачів.
3. Досліджено можливості інструментів Gophish та Evilginx для побудови сценаріїв соціальної інженерії та оцінки вразливості користувачів.
4. Розроблено методологію моделювання соціально-інженерної атаки в корпоративній системі та надано рекомендації щодо її застосування та підвищення обізнаності персоналу.
5. Робота викладена логічно та послідовно, висновки сформульовані чітко, графічні матеріали оформлені якісно. Використаний список літератури свідчить про вміння користуватися науковими джерелами за темою кваліфікаційної роботи.

Недоліки:

1. Було б доцільно провести аналіз ефективності моделювання атак на прикладі конкретної організації для більшої практичної значущості.
2. Запропоновану методологію моделювання соціально-інженерних атак бажано було б ілюструвати конкретними прикладами тестових кампаній у корпоративному середовищі.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **“відмінно”**, а здобувачка **ПРОЦЕНКО Асія** – присвоєння кваліфікації магістр з кібербезпеки за освітньою програмою інформаційна та кібернетична безпека.

Рецензент:

*(науковий ступінь,
вчене звання)*

(підпис)

(ім'я, прізвище)

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

**ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ**

Направляється здобувач ПРОЦЕНКО Асія до захисту кваліфікаційної роботи
(прізвище, ім'я)
спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Технологія виявлення атак соціальної інженерії для користувачів в
корпоративній системі організації».
Кваліфікаційна робота і рецензія додаються.

Директор інституту

(підпис)

Євгенія ІВАНЧЕНКО

(ім'я, прізвище)

Висновок керівника кваліфікаційної роботи

Здобувачка **ПРОЦЕНКО Асія** обрала тему роботи, метою якої було дослідити проблему соціально-інженерних атак у корпоративних системах та проаналізувати причини їхньої успішності серед користувачів; провести аналіз інструментів моделювання фішингових атак, зокрема можливостей Gophish та Evilginx для побудови реалістичних сценаріїв соціальної інженерії; а також розробити методологію моделювання соціально-інженерної атаки в корпоративній системі із застосуванням цих платформ. Перелік використаних джерел свідчить про вміння здобувачки оперувати сучасними науковими підходами до моделювання соціальної інженерії та успішно застосовувати їх у практичних дослідженнях. Під час виконання кваліфікаційної роботи **ПРОЦЕНКО Асія** показала добру теоретичну та практичну підготовку, вміння самостійно вирішувати поставлені завдання й робити обґрунтовані висновки. Роботу виконувала сумлінно, акуратно та вчасно відповідно до затвердженого плану.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувачки **ПРОЦЕНКО Асії** на оцінку “**відмінно**” та присвоїти їй кваліфікацію магістр з кібербезпеки за освітньою програмою інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи

(підпис)

Галина ГАЙДУР

(ім'я, прізвище)

“ ”

2026 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувачка **ПРОЦЕНКО Асія** допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Систем та технологій кібербезпеки

(назва)

(підпис)

Галина ГАЙДУР

(ім'я, прізвище)

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: _ сторінки, _ рисунків, _ таблиця, _ джерел.

Об'єкт дослідження – користувачі корпоративної системи та їх взаємодія з інформаційними ресурсами організації.

Предмет дослідження – технологія моделювання соціально-інженерних атак із використанням інструментів Gophish та Evilginx.

Мета роботи – розробити методологію моделювання соціально-інженерних атак у корпоративній системі та надати рекомендації щодо підвищення обізнаності користувачів і зниження ризику успішних атак.

Методи дослідження – опрацювання наукової та спеціалізованої літератури, аналіз інструментів Gophish та Evilginx, підходів до моделювання соціальної інженерії та дослідження практичних сценаріїв.

Інструменти Gophish та Evilginx забезпечують можливість моделювання соціально-інженерних атак у корпоративних системах, дозволяючи створювати контрольовані та реалістичні сценарії фішингових кампаній. Gophish – це платформа для автоматизованого розсилання електронних листів із піддробленими посиланнями, збору взаємодії користувачів із фішинговими повідомленнями та формування звітів для аналізу поведінки персоналу. Evilginx, у свою чергу, дозволяє проводити більш складні атаки, зокрема перехоплення облікових даних через проксування веб-трафіку, що дозволяє моделювати реалістичні сценарії маніпуляцій.

У роботі проаналізовано проблему атак на основі соціальної інженерії, визначено ключові фактори їхньої успішності серед користувачів та проведено аналіз можливостей Gophish та Evilginx у корпоративному середовищі. На основі досліджень розроблено методологію моделювання атак та рекомендації для підвищення обізнаності користувачів і зниження ризику успішних атак.

Галузь використання – кібербезпека інформаційних ресурсів організації.

СОЦІАЛЬНА ІНЖЕНЕРІЯ, ФІШИНГ, КОРПОРАТИВНА БЕЗПЕКА,
GOPHISH, EVILGINX, МОДЕЛЮВАННЯ АТАК

ABSTRACT

Text part of the qualification work: _ pages, _ figures, _ table, _ sources.

Object of research – corporate system users and their interaction with the organization's information resources.

Subject of research – the technology of modeling social engineering attacks using Gophish and Evilginx tools.

Objective of the work – to develop a methodology for modeling social engineering attacks in a corporate system and provide recommendations for increasing user awareness and reducing the risk of successful attacks.

Research methods – review of scientific and specialized literature, analysis of Gophish and Evilginx tools, approaches to modeling social engineering, and study of practical scenarios.

Gophish and Evilginx tools provide the ability to model social engineering attacks in corporate systems, allowing for the creation of controlled and realistic phishing campaign scenarios. Gophish is a platform for automated sending of emails with fake links, collecting user interactions with phishing messages, and generating reports for analyzing employee behavior. Evilginx, in turn, enables more advanced attacks, including credential interception through web traffic proxying, allowing the modeling of realistic manipulation scenarios.

The work analyzes the problem of social engineering attacks, identifies key factors for their success among users, and examines the capabilities of Gophish and Evilginx in a corporate environment. Based on the research, a methodology for modeling attacks and recommendations for increasing user awareness and reducing the risk of successful attacks have been developed.

Field of application – cybersecurity of the organization's information resources.

SOCIAL ENGINEERING, PHISHING, CORPORATE SECURITY, GOPHISH, EVILGINX, ATTACK MODELING

ЗМІСТ

	Стор.
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ	10
ВСТУП	11
1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ СОЦІАЛЬНО-ІНЖЕНЕРНИХ АТАК У КОРПОРАТИВНИХ СЕРЕДОВИЩАХ ТА АНАЛІЗ ПРИЧИН ЇХ УСПІШНОСТІ СЕРЕД КОРИСТУВАЧІВ	13
1.1 Актуальність дослідження на основі аналізу реальних інцидентів та причин їх успішності.....	13
1.2 Аналіз основних видів соціально-інженерних атак та визначення найбільш поширених у корпоративних середовищах.....	26
1.3 Аналіз підходів для моделювання фішингових атак.....	35
2 АНАЛІЗ ІНСТРУМЕНТІВ МОДЕЛЮВАННЯ ФІШИНГОВИХ АТАК: МОЖЛИВОСТІ GORNISH ТА EVILGINX У ПОБУДОВІ СЦЕНАРІЇВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ.....	43
2.1 Архітектура компонентів інфраструктури для проведення соціально-інженерних атак у корпоративних середовищах.....	43
2.2 Особливості побудови реалістичних сценаріїв соціально-інженерних атак у корпоративному контексті.....	50
2.3 Методика оцінювання рівня обізнаності користувачів та аналіз їх поведінкових реакцій під час тестових кампаній.....	56
3 ТЕХНОЛОГІЯ МОДЕЛЮВАННЯ СОЦІАЛЬНО-ІНЖЕНЕРНОЇ АТАКИ В КОРПОРАТИВНІЙ СИСТЕМІ З ВИКОРИСТАННЯМ GORNISH ТА EVILGINX.....	63
3.1 Технологія проведення моделювання соціально-інженерних атак та збору результатів.....	63
3.2 Рекомендації щодо підвищення рівня захисту корпоративного середовища від соціально-інженерних атак.....	70
ВИСНОВКИ	74
ПЕРЕЛІК ПОСИЛАНЬ	76

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)	78
---	-----------

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

BEC	– Business Email Compromise
AiTM	– Adversary in The Middle
MFA	– Multi-Factor Authentication

ВСТУП

Актуальність дослідження. Сучасні корпоративні інформаційні системи функціонують в умовах постійного зростання цифрових загроз, зумовлених розвитком хмарних технологій, віддаленого формату роботи, мобільності користувачів та активного використання зовнішніх сервісів. За таких умов традиційні підходи до забезпечення інформаційної безпеки, орієнтовані переважно на захист мережевого периметра та технічних компонентів інфраструктури, поступово втрачають свою ефективність. Зловмисники дедалі рідше використовують складні технічні вразливості, натомість фокусуються на людині як найбільш уразливому елементі системи безпеки.

Соціальна інженерія є одним із найпоширеніших і найрезультативніших векторів сучасних кібератак. Вона ґрунтується на психологічному впливі на користувачів з метою отримання конфіденційної інформації, облікових даних або ініціювання дій, що призводять до компрометації корпоративних ресурсів. Аналіз реальних інцидентів останніх років свідчить, що значна частина порушень інформаційної безпеки розпочинається саме з фішингових повідомлень або інших соціально-інженерних технік, успішність яких обумовлена недостатнім рівнем обізнаності користувачів та недосконалістю організаційних і технічних заходів захисту.

Особливої актуальності проблема соціальної інженерії набуває в корпоративних середовищах, де один скомпрометований обліковий запис може стати точкою входу для подальшої ескалації привілеїв, горизонтального переміщення мережею та отримання доступу до критично важливих даних.

Вищевикладене визначає актуальність теми даної кваліфікаційної роботи, присвяченої дослідженню технологій виявлення атак соціальної інженерії для користувачів у корпоративній системі організації, а також аналізу причин їх успішності та шляхів підвищення рівня захищеності корпоративного середовища.

Об'єкт дослідження – користувачі корпоративної системи та їх взаємодія з інформаційними ресурсами організації.

Предмет дослідження – технологія моделювання соціально-інженерних атак із використанням інструментів Gophish та Evilginx.

Мета роботи – розробити методологію моделювання соціально-інженерних атак у корпоративній системі та надати рекомендації щодо підвищення обізнаності користувачів і зниження ризику успішних атак.

Наукові завдання:

дослідити сутність проблеми успішності соціально-інженерних атак серед працівників організації;

проаналізувати підходи до проведення фішингових атак у корпоративному середовищі;

проаналізувати існуючі рішення захисту для забезпечення безпеки користувачів від фішингових атак;

проаналізувати методи та засоби моделювання фішингових атак на базі Gophish та Evilginx;

розкрити порядок реалізації технології проведення соціально-інженерних атак у корпоративному середовищі.

Методи дослідження – опрацювання наукової та спеціалізованої літератури, аналіз інструментів Gophish та Evilginx, підходів до моделювання соціальної інженерії та дослідження практичних сценаріїв.

Практичне значення одержаних результатів: визначено ключові фактори успішності соціальної інженерії серед користувачів та проведено аналіз можливостей Gophish та Evilginx у корпоративному середовищі, а також, розроблено методологію моделювання атак та рекомендації для підвищення обізнаності користувачів і зниження ризику успішних атак.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2023 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ СОЦІАЛЬНО-ІНЖЕНЕРНИХ АТАК У КОРПОРАТИВНИХ СЕРЕДОВИЩАХ ТА АНАЛІЗ ПРИЧИН ЇХ УСПІШНОСТІ СЕРЕД КОРИСТУВАЧІВ

1.1 Актуальність дослідження на основі аналізу реальних інцидентів та причин їх успішності

У сучасних умовах розвитку цифрових технологій корпоративні інформаційні системи зазнають суттєвих змін під впливом глобальних трансформацій, що пов'язані з переходом до хмарних сервісів, гібридним та віддаленим режимом роботи, а також зростанням ролі сторонніх сервісів і партнерів у бізнес-процесах. Ці тенденції створюють нові можливості для оптимізації діяльності організацій, проте одночасно підвищують складність захисту інформаційних активів. Класична модель інформаційної безпеки, яка спиралась на ізольований мережевий периметр та захисні засоби точкової дії (наприклад, брандмауери, антивірусні продукти або системи запобігання вторгнень), у сучасному середовищі вже не здатна забезпечити необхідний рівень безпеки. Це пов'язано з тим, що периметр мережі фактично розпався, а основний вектор загроз змістився від чисто технічних експлойтів до маніпуляцій із людською поведінкою. Саме людський фактор, як показують численні дослідження, стає провідним шляхом проникнення в корпоративні системи через використання методів соціальної інженерії.

Соціальна інженерія — це методика психологічного впливу на людину з метою обману, маніпуляцій та отримання неправомірного доступу до конфіденційних даних або виконання дій, які можуть спричинити шкоду організації (наприклад, передача облікових даних, ініціювання фінансових транзакцій або інсталяція шкідливого програмного забезпечення). Такий підхід не потребує обов'язкового використання технічних вразливостей, оскільки він експлуатує поведінкові та когнітивні слабкості користувачів, зокрема схильність

довіряти авторитетним джерелам, реагувати на емоційні тригери або виконувати дії під тиском часу.

Провідні аналітичні звіти відображають величезну роль соціальної інженерії в сучасному ландшафті кіберзагроз. За даними Verizon Data Breach Investigations Report 2025 (DBIR), близько 60 % усіх інцидентів порушення безпеки пов'язані з «людським елементом», що охоплює як випадкові помилки користувачів, так і цілеспрямовані атаки через фішинг і суміжні техніки [1]. Ця частка залишається незмінною з року в рік, що підкреслює вразливість користувачів, що зберігається, до обману і когнітивного перевантаження в цифровому середовищі. Це свідчить про те, що люди залишаються ключовим чинником у більшості компрометацій сучасних ІТ-середовищ, незалежно від рівня технічного захисту організації. Оцінки, засновані на моделюванні, показують, що, незважаючи на безперервну підготовку щодо підвищення обізнаності, медіана імітація фішингу Коефіцієнт клікабельності стабілізувався на рівні приблизно 1,5%, що вказує на поведінковий мінімум, нижче якого подальше зниження показників статистично та оперативно скрутне. Цей ризик, що зберігається, обумовлений людським фактором, таким як відволікання уваги, розумове навантаження або вкрай переконливі фішингові повідомлення.

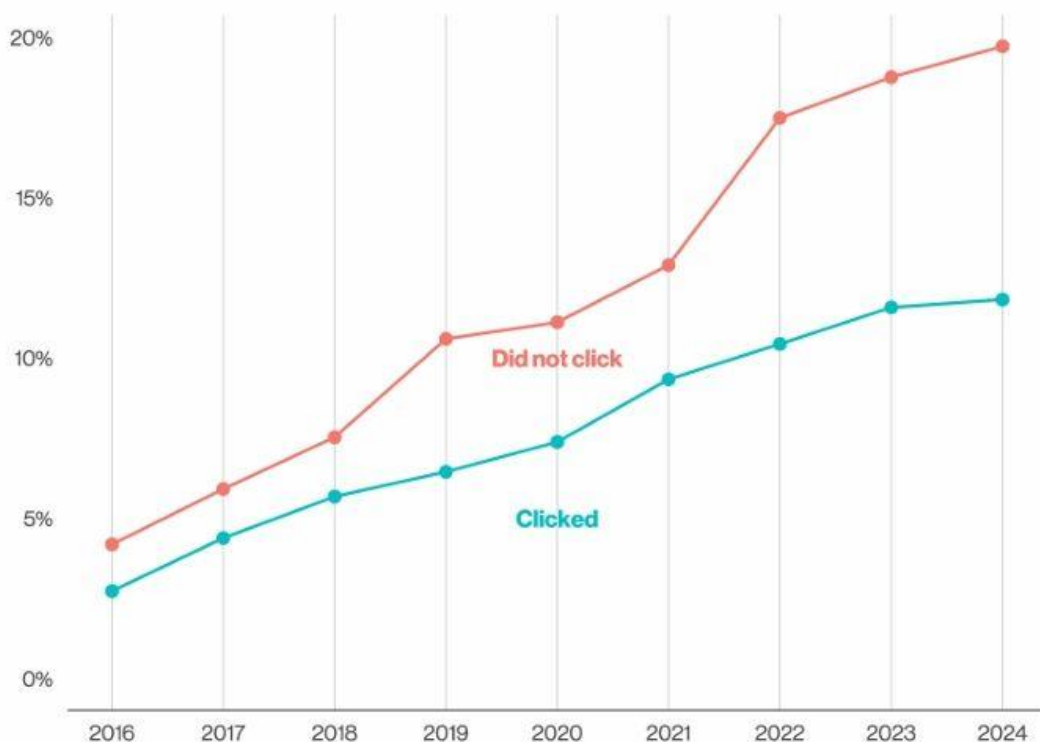


Рис.1.1 – Показник ефективності фішингових симуляційних кампаній залежно від статусу кліка [2]

Проблема стає ще більш очевидною при розгляді масштабів фішингових атак — щодня зловмисники розсилають мільярди таких повідомлень, і значна їх частина імітує легітимні бренди або бізнес-процеси, що ускладнює розпізнавання загрози користувачем та автоматичними системами захисту.

Для обґрунтування практичної значущості соціальної інженерії як одного з ключових векторів сучасних кібератак доцільно звернутися до аналізу реальних інцидентів, що мали місце у 2020–2025 роках. Розгляд таких випадків дозволяє не лише продемонструвати різноманіття технік фішингу та соціального впливу, але й виявити спільні закономірності, які зумовлюють їхню ефективність, а також оцінити масштаби наслідків для організацій різних секторів.

Цілеспрямовані атаки «payroll pirate» на університети США (2025 рік). Microsoft Threat Intelligence зафіксував активність загрози, яку вони класифікують як Storm-2657, що спеціалізується на отриманні несанкціонованого доступу до облікових записів співробітників із метою перенаправлення заробітної плати на рахунки, контрольовані зловмисниками. У професійній літературі такі інциденти

отримали назву «payroll pirate», що вказує на їхню фінансову спрямованість. Основними цілями атак Storm-2657 є організації, розташовані на території США, зокрема працівники освітніх закладів вищої освіти.

У кампанії, зафіксованій у першій половині 2025 року, аналітики визначили, що зловмисники цілеспрямовано націлювалися на облікові записи користувачів у Workday. Водночас важливо зазначити, що аналогічні методи можуть бути застосовані до будь-яких SaaS-систем, які зберігають інформацію про персонал, заробітну плату або банківські реквізити, оскільки атаки спрямовані не на вразливість платформи як такої, а на соціальну інженерію та відсутність або недостатню налаштованість багатофакторної автентифікації. Зловмисники застосовували високорозвинуті техніки маніпуляції користувачами, використовуючи методи фішингу з посередником (Adversary-in-the-Middle, AiTM), що дозволило їм отримувати одноразові коди MFA та обійти стандартні заходи безпеки. Відсутність MFA або використання не фішинг-резистентної MFA унеможливило ефективний захист користувацьких акаунтів, що робить соціальну інженерію ключовим інструментом загрози.

Після отримання первинного доступу через підроблені фішингові листи, Storm-2657 здобував контроль над обліковими записами Exchange Online жертв, що дозволяло не лише переглядати кореспонденцію, а й створювати правила вхідної пошти для видалення сповіщень від Workday. Це дозволило приховувати будь-які зміни в облікових записах HR. Наступним етапом атаки була модифікація налаштувань виплати заробітної плати, що призводило до переказу коштів на рахунки, контрольовані зловмисниками. Така зміна фінансової інформації завдавала безпосередньої матеріальної шкоди співробітникам та могла суттєво порушити фінансову діяльність організації.

Одним із прикладів соціально-інженерного підходу є використання Storm-2657 тем фішингових повідомлень, пов'язаних із здоров'ям, наприклад, імітація звітів про хвороби або спалахи інфекцій на кампусі університетів. Листи містили посилання на документи Google Docs, які перенаправляли користувачів на сайти зловмисників. Використання таких тем дозволяло підвищити ймовірність того, що

користувачі натиснуть на посилання, через природну тривогу за власне здоров'я або безпеку оточуючих. Іншим методом було надання вигляду офіційних повідомлень від адміністрації університету або від імені HR-відділу, де містилися деталі компенсацій або посилання на документи, нібито важливі для працівника. Така персоналізація імітувала легітимність повідомлень і значно підвищувала шанси успішного фішингу.

Критичним етапом атаки була ескалація захоплених облікових записів для забезпечення стійкого доступу (persistence). Зловмисники реєстрували власні номери телефонів для MFA у профілях жертв, що дозволяло обійти додаткові перевірки при наступних входах і забезпечувало безперервний контроль над обліковими записами без виявлення [3]. Така практика демонструє поєднання соціальної інженерії із технічними методами обходу стандартних заходів безпеки.

Фінансові та операційні наслідки такої атаки були значними. Зловмисники отримали прямий доступ до виплат співробітників, що призвело до фінансових втрат, необхідності відновлення облікових записів, додаткових перевірок і аудиту транзакцій, а також створило ризик втрати довіри працівників та порушення внутрішньої безпеки організацій. Системна експлуатація SaaS-платформ без ефективного багатофакторного захисту стала прямим каналом для крадіжки коштів та конфіденційних даних, що підкреслює важливість інтегрованих методів захисту, моніторингу та навчання персоналу.

Фішингова кампанія NOBELIUM із використанням компрометованого сервісу розсилки (2021). Microsoft Threat Intelligence Center (MSTIC) у 2021 році виявив та задокументував масштабну шкідливу email-кампанію, організовану угрупованням NOBELIUM, який раніше стояв за однією з найрезонансніших кібератак сучасності, а саме компрометацією платформи SolarWinds Orion та розповсюдженням бекдору SUNBURST, а також використанням шкідливих компонентів TEARDROP, GoldMax та інших допоміжних інструментів. Виявлена кампанія демонструвала високий рівень складності, поетапну еволюцію тактик та значну адаптивність до механізмів виявлення й захисту.

Починаючи з січня 2021 року, кампанія розвивалася хвилеподібно, що

свідчить про цілеспрямоване експериментування з різними методами доставки шкідливого навантаження, збору розвідувальної інформації та обходу захисних механізмів. Кульмінацією кампанії стала подія 25 травня 2021 року, коли NOBELIUM використало легітимний сервіс масових розсилок Constant Contact для маскуванню під американську урядову організацію та поширення шкідливих URL-адрес серед широкого кола цільових організацій. Використання довіреної сторонньої платформи як інфраструктурного посередника стало критично важливим елементом атаки, оскільки значно підвищило рівень довіри з боку отримувачів листів та ускладнило автоматичне виявлення загрози.

Історично NOBELIUM зосереджувалося на атаках проти державних органів, неурядових організацій, аналітичних центрів, військових структур, постачальників ІТ-послуг, телекомунікаційних компаній, а також організацій у сфері охорони здоров'я та наукових досліджень. У межах цієї кампанії зловмисники намагалися скомпрометувати приблизно 3000 окремих облікових записів у більш ніж 150 організаціях.

Особливістю операції стало використання унікальної інфраструктури та інструментарію для кожної цілі або невеликої групи цілей. Такий підхід значно знижував ефективність сигнатурних засобів захисту та ускладнював кореляцію інцидентів між різними жертвами, що дозволяло зловмисникам тривалий час залишатися непоміченими.

На ранньому етапі кампанії, зафіксованому наприкінці січня 2021 року, зловмисники застосовували підхід, характерний для класичних операцій соціальної інженерії, — без негайної доставки шкідливого коду. Фішингові листи містили лише посилання на ресурси, розміщені на платформі Google Firebase, метою яких був збір інформації про користувачів, що перейшли за посиланням. Таким чином, NOBELIUM здійснювало попередню розвідку, ідентифікуючи зацікавлених або менш обережних користувачів без ризику негайного викриття. Такий підхід демонструє високий рівень розуміння людського фактору: жертва не піддається миттєвій атаці, а поступово залучається у взаємодію, не усвідомлюючи потенційної небезпеки.

У наступних хвилях кампанії NOBELIUM почало використовувати HTML-вкладення у spear-phishing листах. Після відкриття такого файлу у браузері або локально, вбудований JavaScript створював ISO-образ на диску та спонукав користувача відкрити його. ISO-файл, у свою чергу, монтувався як знімний носій і містив ярлик (LNK), що запускав DLL-файл із шкідливим кодом.

Ключовим елементом соціальної інженерії на цьому етапі було формування у користувача відчуття легітимності дій: відкриття файлу виглядало як стандартна операція перегляду документів, а присутність приманкового PDF-документа відволікала увагу від фонові компрометації системи.

Найбільш небезпечна фаза кампанії розпочалася 25 травня 2021 року, коли NOBELIUM використало сервіс Constant Contact для масового розсилання листів, замаскованих під повідомлення від USAID. Листи містили коректні технічні заголовки, справжні домени сервісу розсилок та переконливі адреси відповіді, що значно знижувало підозру з боку отримувачів.

Перехід за посиланням спочатку вів на легітимний домен Constant Contact, після чого відбувалося перенаправлення на інфраструктуру, контрольовану зловмисниками, де користувачу пропонувався до завантаження шкідливий ISO-файл. У середині ISO знаходилися ярлик для запуску шкідливого коду, приманковий документ та прихований DLL-файл, який завантажував Cobalt Strike Beacon. [4]

Проаналізована кампанія NOBELIUM є яскравим прикладом сучасної кібероперації, у якій соціальна інженерія виступає не допоміжним, а центральним елементом атаки. Зловмисники системно експлуатували довіру користувачів до відомих організацій, звичних форматів документів і легітимних онлайн-сервісів, поєднуючи це з поетапною технічною ескалацією.

Інцидент підтверджує, що навіть найрозвиненіші технічні засоби захисту можуть бути обійдені за умови успішного маніпулювання людською поведінкою. Відтак протидія подібним загрозам потребує комплексного підходу, який включає не лише технологічні рішення, але й системну роботу з персоналом, моделювання атак соціальної інженерії та постійний аналіз змін у тактиках державних

кіберугруповань.

Серія соціально-інженерних атак угруповання LAPSUS\$ (2022). Однією з найхарактерніших особливостей Lapsus\$ було систематичне використання соціальної інженерії як основного механізму первинного доступу. Група демонструвала високий рівень психологічного впливу на співробітників організацій-жертв, поєднуючи технічні прийоми з маніпуляцією людською поведінкою. До основних методів належали фішингові та spear-phishing кампанії, спрямовані на конкретні організації або окремих співробітників. Особливу увагу зловмисники приділяли мобільним пристроям, зокрема телефонам із встановленими додатками для багатофакторної автентифікації. Поширеною практикою було SIM-swapping, що дозволяло перехоплювати SMS-коди підтвердження.

SIM-swap (підміна SIM-карти) — це кібератака, при якій шахраї обманом переконують оператора зв'язку перенести ваш номер телефону на нову SIM-карту, яку вони контролюють, отримуючи доступ до ваших дзвінків, SMS, а значить, до банківських рахунків, соцмереж та інших акаунтів через одноразові паролі. Це досягається за допомогою соціальної інженерії (видаючи себе за жертву) або корупції співробітника оператора, відкриваючи шлях до крадіжки особи та фінансів.

Окрім цього, Lapsus\$ активно застосовувало техніку MFA-fatigue — багаторазове надсилання запитів на підтвердження входу з метою психологічного виснаження користувача та спонукання його до автоматичного схвалення запиту, часто у нічний час або в незручний момент. Додатково використовувалося видавання себе за співробітників служби підтримки з метою переконати жертву підтвердити MFA або перейти на шкідливі ресурси.

Особливо небезпечним елементом соціальної інженерії було вербування інсайдерів. За грошову винагороду співробітників організацій схиляли до надання облікових даних, схвалення MFA-запитів або виконання дій, що сприяли компрометації внутрішніх систем.

Після проникнення в інфраструктуру жертви Lapsus\$ використовувало

широкий набір інструментів для ескалації привілеїв, горизонтального переміщення мережею та закріплення у середовищі. Значну роль відігравало використання неправильно збережених облікових даних, зокрема паролів у відкритому вигляді. Зловмисники активно застосовували легітимні інструменти віддаленого доступу, що ускладнювало виявлення їхньої діяльності та дозволяло маскуватися під звичайних користувачів. Також використовувалися вразливості у поширених корпоративних системах, зокрема Active Directory, Microsoft Exchange, Confluence, Jira та GitLab.

Основним наслідком атак Lapsus\$ став масовий витік конфіденційної інформації, включно з вихідним кодом, внутрішньою документацією та корпоративними обліковими даними. Такі інциденти мали не лише фінансові, а й довгострокові репутаційні наслідки для постраждалих організацій. Група активно застосовувала модель подвійного вимагання, поєднуючи крадіжку даних із погрозами публічного розголошення. Крім того, діяльність Lapsus\$ призводила до збоїв у роботі сервісів, зупинки бізнес-процесів та необхідності проведення масштабних відновлювальних заходів. Окремо слід відзначити психологічний тиск і переслідування, яких зазнавали фахівці з кібербезпеки та дослідники, що брали участь у розслідуванні інцидентів. Публікація персональних даних та загрози фізичної безпеки використовувалися як інструмент залякування.

Основною мотивацією Lapsus\$ був фінансовий зиск. Група спеціалізувалася на атаках проти великих корпорацій та державних установ із метою викрадення конфіденційних даних для подальшого продажу, вимагання або використання як інструменту тиску на жертву. Серед найбільш відомих цілей Lapsus\$ фігурують Microsoft, NVIDIA, Samsung, Vodafone, Okta, Ubisoft та T-Mobile.[5]

Діяльність угруповання LAPSUS\$ у 2022 році стала яскравим прикладом того, як соціальна інженерія може бути використана як основний інструмент атак навіть проти найбільших технологічних корпорацій. На відміну від класичних APT-кампаній, орієнтованих на складні технічні експлойти, LAPSUS\$ робило ставку на маніпуляцію людьми, зокрема співробітниками технічної підтримки та користувачами з розширеними правами доступу.

Аналітичний аналіз цих інцидентів свідчить про системну проблему надмірних привілеїв та слабого контролю за ролями користувачів. Соціальна інженерія в цьому контексті виступає прискорювачем, який дозволяє швидко перетворити локальну помилку окремого співробітника на масштабний витік інформації. Значущість кейсу LAPSUS\$ полягає також у демонстрації того, що навіть добре захищені технічні системи можуть бути обійдені без використання складних експлойтів, якщо організація недооцінює людський фактор та не інвестує достатньо ресурсів у навчання персоналу і аудит доступів.

Інцидент Twilio та кампанія SMS-фішингу (2022). У серпні 2022 року компанія Twilio підтвердила факт несанкціонованого доступу до даних клієнтів унаслідок успішної фішингової атаки, спрямованої на співробітників компанії. Зловмисникам вдалося отримати облікові дані корпоративного доступу, використовуючи SMS-фішинг (smishing), що імітував внутрішні повідомлення від IT-відділу Twilio.

Атака базувалася на класичних прийомах соціальної інженерії. Співробітникам надсилалися текстові повідомлення з інформацією про нібито закінчення терміну дії пароля або зміну робочого графіка. Повідомлення містили посилання на підроблені вебсторінки, контрольовані зловмисниками, де жертви вводили свої облікові дані. Для підвищення довіри в повідомленнях навмисно використовувалися терміни, пов'язані з корпоративною автентифікацією, зокрема «Okta» та «SSO».

У результаті атаки зловмисники отримали доступ до внутрішніх систем Twilio та даних 125 клієнтів. Хоча точний перелік скомпрометованої інформації офіційно не був повністю розкритий, політика конфіденційності компанії вказує, що такі дані можуть включати адреси, платіжну інформацію, IP-адреси та, в окремих випадках, документи для підтвердження особи. Інцидент є особливо значущим з огляду на масштаби діяльності Twilio та наявність понад 150 тисяч корпоративних клієнтів, серед яких великі технологічні компанії.

Попри оперативні дії з боку Twilio, зокрема блокування шкідливих доменів, співпрацю з мобільними операторами та хостинг-провайдерами, зловмисники

продовжували кампанію, змінюючи інфраструктуру. Це дозволило компанії дійти висновку, що атака була організована добре скоординованою та технічно підготовленою групою.[6]

З аналітичної точки зору даний інцидент демонструє, що навіть організації з розвиненою інфраструктурою безпеки залишаються вразливими до атак, у яких ключовою ланкою є людський фактор. Компрометація стала можливою не через технічні вразливості систем, а через успішне маніпулювання довірою співробітників, що підкреслює критичну роль соціальної інженерії у сучасних кібератаках.

Розповсюдження phishing-as-a-service платформи та масове викрадення облікових даних (2024). У вересні 2024 року корпорація Microsoft повідомила про вилучення майже 340 доменів, пов'язаних із сервісом Raccoon0365 — phishing-as-a-service платформою, що діяла під керівництвом операторів, імовірно базованих у Нігерії. Відповідне рішення було ухвалене Окружним судом США в Манхеттені та реалізоване силами підрозділу Microsoft Digital Crimes Unit.

Raccoon0365 надавав підписникам інструменти для масового проведення фішингових кампаній, зокрема можливість імітації довірених брендів Microsoft та створення підроблених сторінок входу для збору облікових даних користувачів. Сервіс функціонував через закритий Telegram-канал із понад 850 учасниками та дозволяв розсилати тисячі фішингових листів одночасно. За даними Microsoft, у результаті діяльності платформи було викрадено щонайменше 5 000 облікових даних користувачів Microsoft.

Особливо активною була кампанія у лютому, під час якої зловмисники застосовували податкову тематику для підвищення переконливості повідомлень. Зафіксовано атаки проти понад 2 300 організацій, переважно на території США. Окрему стурбованість викликали атаки на медичний сектор: щонайменше п'ять організацій охорони здоров'я зазнали успішного викрадення облікових даних.

З фінансової точки зору діяльність Raccoon0365 була ефективною: з моменту запуску в липні 2024 року оператори сервісу отримали щонайменше 100 000 доларів США у криптовалюти. Для маскуванню інфраструктури використовувалися

послуги Cloudflare, яка згодом спільно з Microsoft та Секретною службою США долучилася до припинення діяльності платформи. [7]

Аналітично даний інцидент демонструє небезпечну тенденцію демократизації кіберзлочинності. Використання готових фішингових сервісів суттєво знижує поріг входу для зловмисників і переносить основний вектор атак у площину соціальної інженерії, де компрометація відбувається не через технічні вразливості, а через маніпуляцію довірою користувачів. Це підкреслює критичну необхідність поєднання технічних засобів захисту з постійним навчанням персоналу та контролем аномальної автентифікаційної поведінки.

Аналіз наведених інцидентів дозволяє виділити низку спільних закономірностей. По-перше, вирішальну роль відіграє довіра до джерела повідомлень, особливо у випадках компрометації легітимних сервісів або використання відомих брендів. По-друге, значні ризики створює компрометація третіх сторін і постачальників, що розширює поверхню атаки. По-третє, людський фактор залишається ключовим елементом успіху соціальної інженерії, особливо в умовах терміновості та інформаційної невизначеності. Нарешті, використання нестійких до фішингу методів багатофакторної аутентифікації та надмірні привілеї користувачів суттєво підвищують потенційний збиток від компрометації.

Економічні наслідки від таких атак також є вражаючими. Business Email Compromise (BEC) — це клас соціально-інженерних атак, коли зловмисники шляхом обману змушують співробітників організації виконувати фінансові операції або передавати конфіденційні дані. За даними Федерального бюро розслідувань США (FBI IC3) лише в 2024 році збитки від BEC становили приблизно \$2,77 мільярда у зафіксованих випадках. [8] Ще гірші локальні оцінки свідчать про глобальні втрати, що вимірюються десятками мільярдів доларів на рік, особливо коли враховуються непрямі витрати на реагування, відновлення, репутаційні втрати та операційні ризики.

Соціальна інженерія не обмежується лише електронною поштою. Станом на 2025 рік фіксується також стрімке зростання інших форм маніпуляцій, включно з vishing (голосові фішингові дзвінки), smishing (SMS-фішингом) та

deepfake-атаками, що використовують штучний інтелект для створення переконливих автентичних аудіо- і відеоматеріалів. Дані показують, що голосові атаки можуть зростати на сотні відсотків щороку, а deepfake-схеми вже призводили до багатомільйонних шахрайських операцій, як у випадку з британською інженерною компанією Arup, де один з фінансових службовців після відеодзвінка з AI-імітацією керівництва відправив зловмисникам понад \$25 млн. [9] Крім того, сучасні інструменти штучного інтелекту дозволяють автоматизувати створення фішингового контенту, роблячи його більш персоналізованим і важчим для розпізнавання, що значно підвищує ймовірність успішної атаки.

Такі тенденції викликають серйозне занепокоєння серед практиків і дослідників: за деякими оцінками, до 26 % усіх соціально-інженерних атак у 2025 році включали deepfake-аудіо чи відео, що ускладнює процес ідентифікації шахрайства та змушує переглядати підходи до навчання персоналу та виявлення загроз.

Успішність соціально-інженерних атак пояснюється не лише еволюцією інструментів та тактик зловмисників, але й властивостями людської психології. Атаки зазвичай спираються на відомі тригери: почуття терміновості та страху (наприклад, «Ваш обліковий запис буде заблоковано!»), довіру до авторитетних або знайомих осіб (імпульс діяти на прохання «керівника»), бажання отримати вигоду або полегшення (безкоштовний бонус, «унікальна можливість»). Ці психологічні механізми зумовлюють так званий «розрив між обізнаністю та поведінкою» — навіть обізнані користувачі можуть виконувати ризикові дії під впливом емоційного чи ситуаційного тиску.

Це підтверджують не лише загальні статистичні дані але й конкретні випадки великих інцидентів.

Отже, з урахуванням широти та глибини соціальної інженерії як загрози, а також її значного впливу на ефективність кібербезпеки організацій, стає очевидним, що актуальність дослідження методів виявлення та моделювання соціально-інженерних атак є надзвичайно високою. Необхідно не лише з'ясувати, які саме техніки використовують зловмисники, а й розробити ефективні

інструменти, які б дозволяли раннє виявлення, аналіз та запобігання таким атакам. Такий підхід має включати поєднання технічних засобів аналізу мережевих та поведінкових сигналів, організаційних процедур повідомлення та блокування підозрілих подій, а також адаптованих моделей навчання користувачів для підвищення їхньої обізнаності та резистентності до маніпулятивних впливів.

1.2 Аналіз основних видів соціально-інженерних атак та визначення найбільш поширених у корпоративних середовищах

Соціально-інженерна атака є різновидом кібератаки, що ґрунтується на психологічному маніпулюванні поведінкою людини з метою отримання конфіденційної інформації, компрометації облікових даних, надання несанкціонованого доступу до цифрових ресурсів або порушення цілісності інформаційної безпеки. На відміну від суто технічних методів злому, соціальна інженерія експлуатує людські емоції, довіру, страх, співчуття та відчуття терміновості, що робить її особливо ефективною в умовах сучасних корпоративних середовищ.

Соціально-інженерні атаки становлять одну з найбільших загроз кібербезпеці, оскільки значна частина кібератак починається саме з персональної взаємодії зі співробітниками організацій. Такі атаки здебільшого спираються на людську помилку як початковий етап ланцюга компрометації. Використовуючи психологічний тиск та маніпулятивні сценарії, зловмисники отримують доступ до особистої інформації користувачів або безпосередньо до кінцевих пристроїв. У разі, якщо скомпрометований пристрій підключений до корпоративної мережі або містить облікові дані для доступу до внутрішніх систем, це створює передумови для подальших атак на рівні підприємства.

З огляду на постійне вдосконалення методів соціальної інженерії та зростання їх складності, організації змушені адаптувати підходи до захисту та підвищувати рівень обізнаності персоналу. У сучасній практиці виділяють низку основних типів соціально-інженерних атак, які найбільш часто використовуються

зловмисниками та мають суттєвий вплив на безпеку корпоративних інформаційних систем.

Фішинг. Фішинг є найбільш масовим і водночас універсальним видом соціально-інженерних атак. Його сутність полягає у використанні електронної пошти, месенджерів, соціальних мереж або інших каналів комунікації для введення користувача в оману та спонукання до виконання небезпечних дій. У корпоративному середовищі фішингові повідомлення часто імітують офіційні звернення від внутрішніх підрозділів, партнерів або відомих сервісів. Основною метою таких атак є отримання облікових даних, встановлення шкідливого програмного забезпечення або перенаправлення жертви на підроблені вебресурси. Висока ефективність фішингу пояснюється його масштабованістю та здатністю адаптуватися до актуальних подій, зокрема фінансових звітних періодів, кризових ситуацій або внутрішніх організаційних змін.

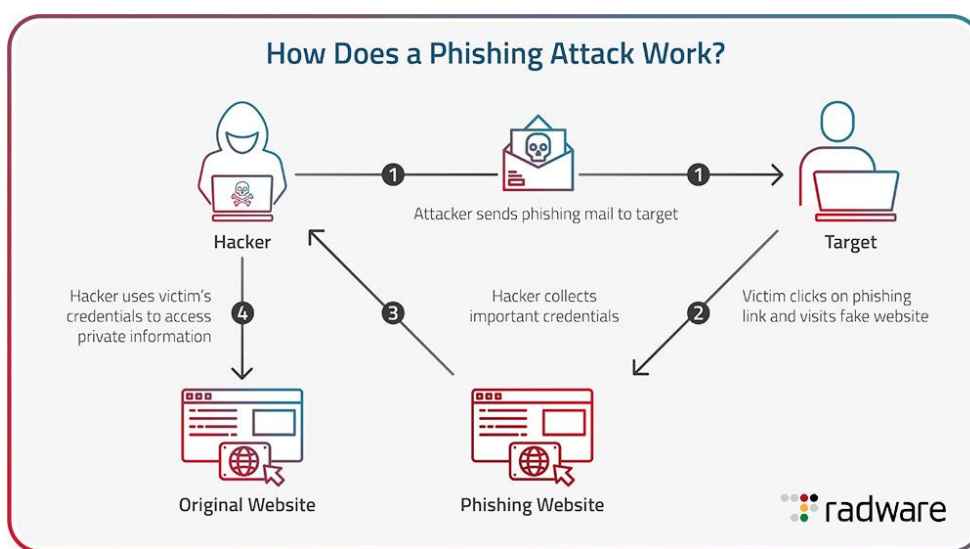


Рис.1.2 – Схема роботи фішингу через пошту [10]

Whaling. Whaling є різновидом фішингових атак, орієнтованим на осіб, які займають керівні або стратегічно важливі посади в організації. На відміну від масового фішингу, такі атаки характеризуються високим рівнем персоналізації та потребують попереднього збору інформації про жертву. Зловмисники аналізують публічну активність керівників, їхні професійні зв'язки, стиль комунікації та роль у прийнятті рішень. Компрометація облікових записів або пристроїв топменеджменту часто має серйозні наслідки, оскільки ці особи володіють

доступом до фінансових ресурсів, конфіденційної інформації та стратегічних систем управління.

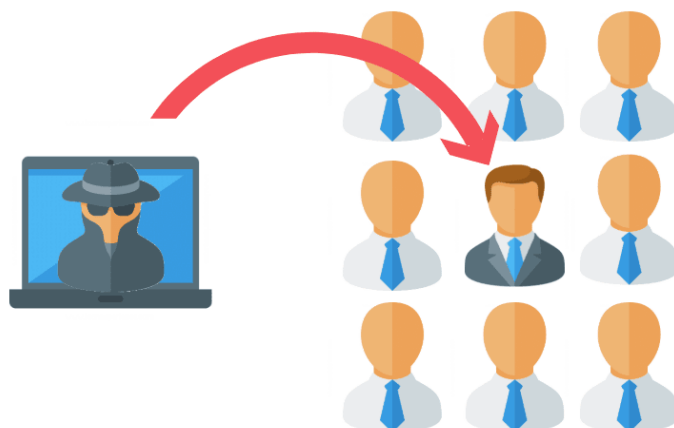


Рис.1.3 – Схема роботи Whaling-атаки [11]

Baiting. Baiting-атаки базуються на використанні привабливих пропозицій або обіцянок вигоди з метою спонукання користувачів до небезпечної поведінки. У корпоративному середовищі baiting може проявлятися у вигляді фальшивих рекламних пропозицій, безкоштовного програмного забезпечення або нібито службових матеріалів. Окрему небезпеку становлять фізичні baiting-атаки, коли заражені носії інформації навмисно залишаються в місцях загального доступу. Використання таких носіїв співробітниками може призвести до зараження внутрішніх систем та подальшого поширення шкідливого коду мережею організації.



Рис.1.4 – Різновиди застосування Baiting-атаки [12]

Vishing (voice phishing). Vishing є різновидом фішингових атак, у межах яких зловмисники використовують голосові канали зв'язку, найчастіше телефонні дзвінки, для отримання конфіденційної інформації від жертви. Основною особливістю цього типу атаки є активна експлуатація міжособистісної комунікації, що дозволяє нападникам здійснювати безпосередній психологічний вплив на співрозмовника. Під час vishing-атак зловмисники, як правило, видають себе за представників авторитетних або довірених організацій, зокрема банківських установ, державних органів, служб безпеки або технічної підтримки, що суттєво підвищує рівень довіри з боку жертви.

Ефективність vishing-атак значною мірою зумовлена тим, що голосова взаємодія сприймається як більш персоналізована та достовірна порівняно з електронною поштою або текстовими повідомленнями. Інтонація, впевненість мовлення та використання професійної термінології створюють у жертви відчуття легітимності запиту, що знижує рівень критичного мислення та сприяє розкриттю персональних або корпоративних даних. Особливо вразливими до таких атак є

співробітники, які працюють у стресових умовах або виконують функції, пов'язані з фінансовими операціями чи обробкою конфіденційної інформації.

Додатковим чинником успішності vishing-атак є використання підміни ідентифікатора абонента (caller ID spoofing). Завдяки цій техніці дзвінок відображається як такий, що надходить із легітимного або знайомого джерела, наприклад, з офіційного номера банку чи внутрішнього номера організації. Це створює ілюзію автентичності дзвінка та посилює довіру жертви до співрозмовника. У корпоративному середовищі такі атаки можуть призводити до розкриття облікових даних, одноразових кодів автентифікації або виконання дій, що відкривають шлях до подальшої компрометації інформаційних систем.



Рис.1.5 – Різновиди застосування Baiting-атаки [13]

Smishing (SMS-фішинг). Smishing (SMS-фішинг).

Smishing, або SMS-фішинг, є різновидом соціально-інженерних атак, у межах яких зловмисники використовують короткі текстові повідомлення (SMS) як канал комунікації для введення користувачів в оману та спонукання їх до виконання небезпечних дій. Основною метою таких атак є отримання конфіденційної інформації, зокрема облікових даних, фінансових реквізитів або одноразових кодів автентифікації, а також перенаправлення жертви на шкідливі вебресурси чи встановлення небезпечного програмного забезпечення на мобільні пристрої.

Особливістю smishing-атак є експлуатація високого рівня довіри користувачів до SMS-повідомлень. На відміну від електронної пошти, де більшість користувачів уже звикли до наявності спаму та фішингових повідомлень, SMS-канал традиційно сприймається як більш надійний і персоналізований засіб комунікації. Це призводить до зниження рівня критичного аналізу змісту повідомлення, особливо у випадках, коли воно містить ознаки терміновості або надходить нібито від відомої організації чи сервісу.

У корпоративних середовищах smishing-атаки набувають особливої небезпеки у зв'язку з широким використанням мобільних пристроїв для доступу до службових ресурсів. Багато організацій застосовують SMS як один із факторів багатофакторної автентифікації, що робить такі повідомлення привабливою ціллю для зловмисників. Отримавши доступ до одноразових кодів або переконавши користувача ввести їх на підробленому вебресурсі, зловмисники можуть обійти механізми захисту та отримати доступ до корпоративних систем.

Зловмисники, які здійснюють smishing-атаки, зазвичай використовують підроблені або тимчасові номери телефонів, а також сервіси масової розсилки повідомлень. Текст повідомлення часто містить шкідливе посилання або інструкції щодо негайних дій, наприклад підтвердження облікового запису, оновлення платіжної інформації або реагування на нібито підозрілу активність. Використання психологічних тригерів, таких як страх втрати доступу, фінансові санкції або обмеження функціональності сервісів, значно підвищує ефективність таких атак.

Окрему складність у виявленні smishing-атак становить те, що SMS-повідомлення часто не проходять через корпоративні шлюзи електронної пошти та засоби фільтрації, які застосовуються для захисту від традиційного фішингу. У результаті відповідальність за розпізнавання загрози покладається безпосередньо на користувача, що збільшує ризик успішної компрометації. Крім того, мобільні пристрої часто мають обмежені можливості для перевірки достовірності посилань або відображення повної інформації про відправника.

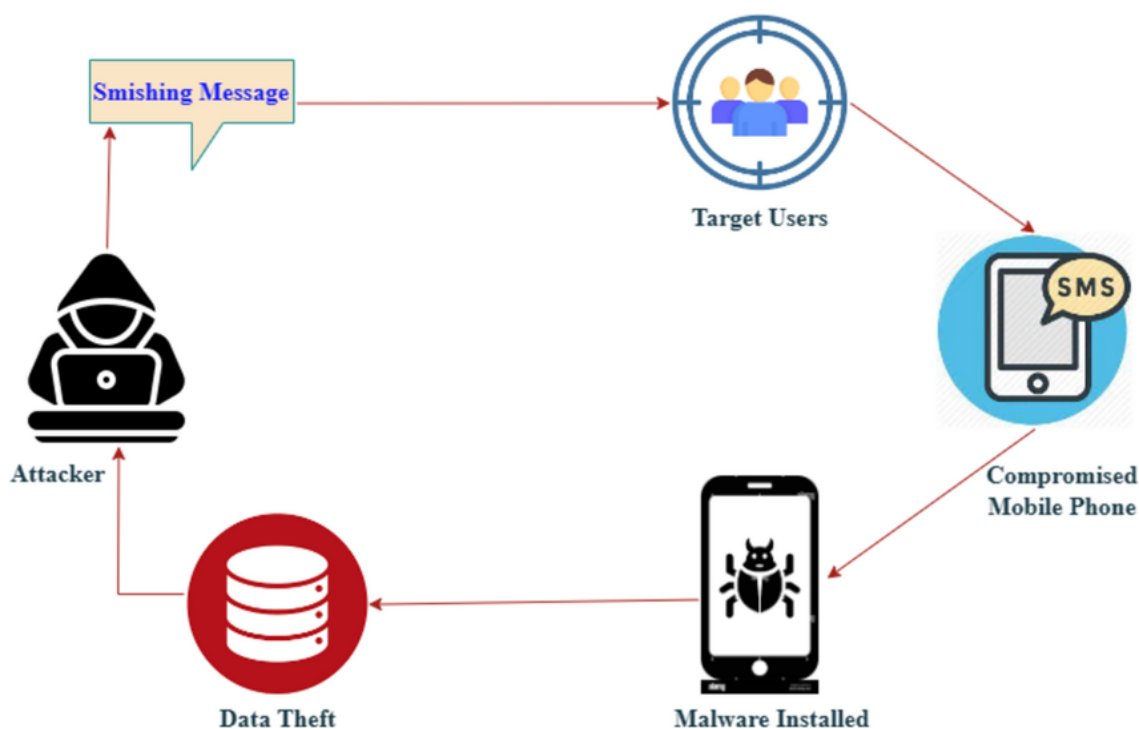


Рис.1.6 – Схема реалізації SMS-фішингу [14]

Pretexting. Pretexting є видом соціально-інженерної атаки, що ґрунтується на створенні правдоподібного сценарію (легенди), який спонукає жертву добровільно розкрити конфіденційну інформацію або виконати дії, вигідні зловмиснику. Ключовою особливістю цього підходу є не одноразовий запит, а послідовне формування довіри шляхом логічно вибудованого контексту взаємодії.

У межах pretexting-атак зловмисники часто видають себе за представників авторитетних структур, зокрема співробітників служби безпеки, технічної підтримки, державних органів або партнерських організацій. Використовуючи знання внутрішніх процесів, термінології та організаційної ієрархії, нападники створюють враження легітимності та професійності, що знижує рівень настороженості з боку жертви

У корпоративних середовищах pretexting є особливо небезпечним, оскільки дозволяє отримувати доступ до службової інформації без застосування технічних засобів злому. Наслідками таких атак можуть бути витік конфіденційних даних, компрометація облікових записів або підготовка підґрунтя для подальших фішингових, ВЕС чи внутрішніх атак. Ефективність pretexting зумовлена експлуатацією довіри, формальних процедур та недостатньої перевірки

автентичності запитів у процесах внутрішньої комунікації.

Honeytrap. Honeytrap є видом соціально-інженерної атаки, що базується на встановленні емоційного або міжособистісного зв'язку з жертвою з метою подальшої маніпуляції. Зловмисник створює фіктивну особу та поступово вибудовує довірчі відносини, використовуючи симпатію, зацікавленість або співчуття як основні інструменти впливу.

У корпоративному контексті honeytrap-атаки спрямовані на співробітників, які мають доступ до службової інформації або внутрішніх систем. У процесі тривалої взаємодії жертва може несвідомо розкривати конфіденційні відомості, ділитися деталями внутрішніх процесів або виконувати дії, що призводять до компрометації доступів. Небезпека таких атак полягає в їхній непомітності та складності виявлення, оскільки вони розвиваються поступово та маскуються під особисте спілкування.

Tailgating. Tailgating, є видом фізичної соціально-інженерної атаки, що полягає в отриманні несанкціонованого доступу до приміщень або захищених зон організації шляхом використання ввічливості, неуважності або довіри співробітників. Зловмисник зазвичай слідує за легітимним працівником і просить утримати двері, пред'являючи правдоподібну причину своєї присутності.

У корпоративному середовищі такі атаки часто супроводжуються видаванням себе за кур'єра, підрядника або нового співробітника, що знижує ймовірність перевірки доступу. Отримавши фізичний доступ, нападник може здійснювати розвідку, викрадати пристрої чи документи або встановлювати шкідливе програмне забезпечення. Небезпека tailgating полягає в тому, що атака відбувається без технічного зламу та використовує недотримання фізичних політик безпеки.



Рис.1.7 – Схема реалізації Tailgating [15]

Найпопулярнішим типом атак соціальної інженерії проти організацій протягом усього досліджуваного періоду залишається фішинг. Це пояснюється його універсальністю, низькою вартістю проведення та можливістю масштабування. Фішингові атаки адаптувалися до корпоративного контексту, використовуючи службову лексику, імітацію внутрішніх повідомлень, повідомлення від постачальників або партнерів, а також повідомлення, пов'язані з безпекою облікових записів. Починаючи з 2022–2023 років спостерігається зростання частки таргетованого фішингу (spear phishing), який базується на попередній розвідці щодо конкретних співробітників і підрозділів компанії.

Починаючи з 2023 року, суттєво зросла роль pretexting-атак, у межах яких

зловмисник створює переконливий сценарій або легенду для маніпуляції жертвою. Такі атаки часто поєднуються з фішингом, телефонними дзвінками або месенджерами і є складнішими для виявлення через їхню контекстну правдоподібність. Pretexting особливо ефективний у великих організаціях зі складною ієрархією, де співробітники звикли виконувати запити від «служб підтримки», «аудиторів» або «керівництва».

Окремої уваги заслуговує стрімке зростання голосових атак (vishing), особливо у 2024–2025 роках. Використання технологій синтезу голосу та deepfake дозволяє зловмисникам імітувати голоси керівників або партнерів компанії, значно підвищуючи рівень довіри з боку жертви. Такі атаки часто застосовуються у фінансових відділах або під час кризових ситуацій, коли рішення необхідно приймати швидко.

Додатково спостерігається зростання атак через альтернативні канали комунікації, зокрема smishing (SMS-фішинг) та quishing (фішинг через QR-коди). Їх популярність пояснюється зміною поведінки користувачів, активним використанням мобільних пристроїв у корпоративному середовищі та нижчим рівнем контролю безпеки порівняно з електронною поштою.

Таким чином, еволюція атак соціальної інженерії у період з 2020 по 2025 роки характеризується переходом від масових, шаблонних кампаній до більш цільових, контекстно обґрунтованих та технічно підтриманих сценаріїв.

1.3. Аналіз підходів для моделювання фішингових атак

З огляду на зростаючу роль соціальної інженерії у структурі сучасних кіберзагроз, фішингові атаки посідають провідне місце серед методів початкового доступу до корпоративних інформаційних систем. Як показує аналіз актуальних тенденцій, фішинг не лише зберігає свою актуальність, але й постійно еволюціонує, адаптуючись до змін у поведінці користувачів, архітектурі корпоративних сервісів та впровадженні нових механізмів захисту, зокрема багатофакторної автентифікації. У таких умовах ефективна протидія фішинговим загрозам потребує

не лише теоретичного вивчення їхніх характеристик, а й практичного аналізу сценаріїв атак у контрольованому середовищі.

Моделювання фішингових атак у межах організацій дозволяє оцінити рівень обізнаності персоналу, виявити слабкі місця в процедурах інформаційної безпеки, а також перевірити ефективність технічних і організаційних заходів захисту. На відміну від реальних інцидентів, симульовані фішингові кампанії дають змогу здійснювати системний аналіз поведінки користувачів без створення реальних ризиків для інформаційних ресурсів компанії. Саме тому спеціалізовані платформи для моделювання фішингових атак стали важливим інструментом у практиці корпоративної кібербезпеки, зокрема в процесах навчання персоналу та проведення внутрішніх оцінок безпеки.

Сучасні інструменти для моделювання фішингових кампаній суттєво відрізняються за своїм функціоналом, підходами до реалізації атак та рівнем технічної складності. Частина з них орієнтована на класичні фішингові сценарії з використанням електронної пошти та підроблених вебсторінок, тоді як інші імітують більш складні атаки, зокрема обходи механізмів багатофакторної автентифікації та перехоплення сесій. Вибір конкретного інструменту безпосередньо впливає на реалістичність моделювання атак і, відповідно, на практичну цінність отриманих результатів.

У межах цього розділу доцільним є детальний розгляд найбільш поширених і репрезентативних платформ, що застосовуються для симуляції фішингових атак у корпоративному середовищі. Особливу увагу привертають платформи Gophish та Evilginx, які репрезентують різні підходи до моделювання фішингових кампаній. Gophish переважно використовується для створення та керування класичними фішинговими кампаніями з акцентом на навчання персоналу та оцінку людського фактора, тоді як Evilginx дозволяє моделювати складні сценарії фішингових атак із використанням технік проксіювання та перехоплення автентифікаційних сесій.

У зв'язку з цим, у цьому підрозділі буде здійснено аналіз функціоналу платформ Gophish та Evilginx для моделювання фішингових кампаній, з метою визначення їхніх можливостей, обмежень та доцільності використання в контексті

оцінювання стійкості корпоративних користувачів до фішингових атак.

Gophish — це спеціалізована open-source платформа, призначена для моделювання та проведення фішингових кампаній у контрольованому середовищі. Вона використовується організаціями, фахівцями з кібербезпеки та командами Blue Team/Red Team з метою оцінювання рівня обізнаності персоналу щодо соціально-інженерних загроз, перевірки ефективності внутрішніх політик безпеки, а також навчання користувачів розпізнаванню фішингових атак.

Основна ідея Gophish полягає не у здійсненні реальних зловмисних дій, а у відтворенні типових сценаріїв фішингу, які застосовуються кіберзлочинцями, з подальшим збором аналітичних даних про поведінку користувачів. Платформа дозволяє емулювати як масові, так і цільові (spear phishing) кампанії, використовуючи електронну пошту та фішингові веб-сторінки. Завдяки відкритому вихідному коду та активній спільноті Gophish часто використовується у навчальних програмах, пентестах та внутрішніх аудитах інформаційної безпеки.

З архітектурної точки зору Gophish являє собою вебзастосунок із централізованою панеллю керування, що забезпечує повний цикл роботи з фішинговою кампанією: від підготовки контенту до аналізу результатів. Нижче наведено аналіз ключового функціоналу платформи відповідно до офіційної документації.

- **User Management (Керування користувачами).** Функціонал керування користувачами забезпечує контроль доступу до адміністративної панелі Gophish. Платформа підтримує створення облікових записів із різними правами доступу, що дозволяє розмежовувати ролі між адміністраторами, аналітиками та операторами кампаній. Це є важливим з точки зору організаційної безпеки, оскільки знижує ризик несанкціонованого доступу до результатів кампаній або конфіденційних даних.

- **Email Templates (Шаблони електронних листів).** Даний модуль призначений для створення та керування шаблонами фішингових листів. Користувач може формувати HTML- або текстові листи, використовуючи змінні для персоналізації (наприклад, ім'я отримувача, адреса електронної пошти,

посада). Це дозволяє імітувати реальні фішингові повідомлення, які часто містять індивідуалізований контент з метою підвищення довіри жертви.

- **Landing Pages (Фішингові сторінки).** Функціонал Landing Pages використовується для створення веб-сторінок, на які перенаправляються користувачі після переходу за посиланням у фішинговому листі. Платформа дозволяє як створювати власні сторінки, так і клонувати легітимні сайти. Основне призначення цього модуля — відстеження взаємодії користувачів зі сторінкою (перехід, введення облікових даних), що є ключовим показником успішності кампанії.

- **Sending Profiles (Профілі відправлення).** Цей компонент відповідає за налаштування способу відправлення електронних листів. Gophish підтримує використання SMTP-серверів, що дозволяє імітувати відправлення листів від різних доменів або сервісів. Профілі відправлення можуть включати параметри автентифікації, порти, шифрування, а також ім'я відправника, що підвищує реалістичність фішингових сценаріїв.

- **Groups & Targets (Групи та цільові користувачі).** Модуль груп дозволяє імпортувати та керувати списками цільових користувачів кампанії. Підтримується додавання адрес вручну або через CSV-файли. Групування користувачів дає можливість проводити сегментовані кампанії, наприклад, окремо для різних підрозділів або ролей в організації, що відповідає сучасним підходам до цільового фішингу.

- **Campaign Management (Керування кампаніями).** Центральний елемент платформи, який об'єднує всі підготовчі компоненти в єдину фішингову кампанію. У межах цього функціоналу визначаються шаблон листа, фішингова сторінка, профіль відправлення та цільова група. Кампанії можуть запускатися вручну або за розкладом, що дозволяє моделювати атаки у різний час та за різних умов.

- **Tracking & Metrics (Відстеження та метрики).** Gophish автоматично збирає статистику щодо дій користувачів: відкриття листів, переходи за посиланнями, введення облікових даних. Ці дані представлені у вигляді зручних

метрик та подій, що дозволяє оцінити рівень вразливості персоналу до фішингових атак та визначити найбільш проблемні аспекти кібергігієни.

- **Reporting & Visualization (Звіти та візуалізація).** Платформа надає інструменти для формування звітів за результатами кампаній. Аналітичні дані можуть бути використані для внутрішніх аудитів, навчальних програм та обґрунтування необхідності підвищення рівня обізнаності співробітників. Візуалізація результатів спрощує сприйняття інформації керівництвом та нефахівцями з технічної безпеки. [16]

Таким чином, Gophish є комплексним інструментом для моделювання фішингових кампаній, який охоплює всі ключові етапи — від підготовки сценарію до глибокого аналізу поведінки користувачів. Його функціонал дозволяє не лише відтворювати реалістичні атаки соціальної інженерії, а й отримувати об'єктивні дані для підвищення загального рівня кібербезпеки організації.

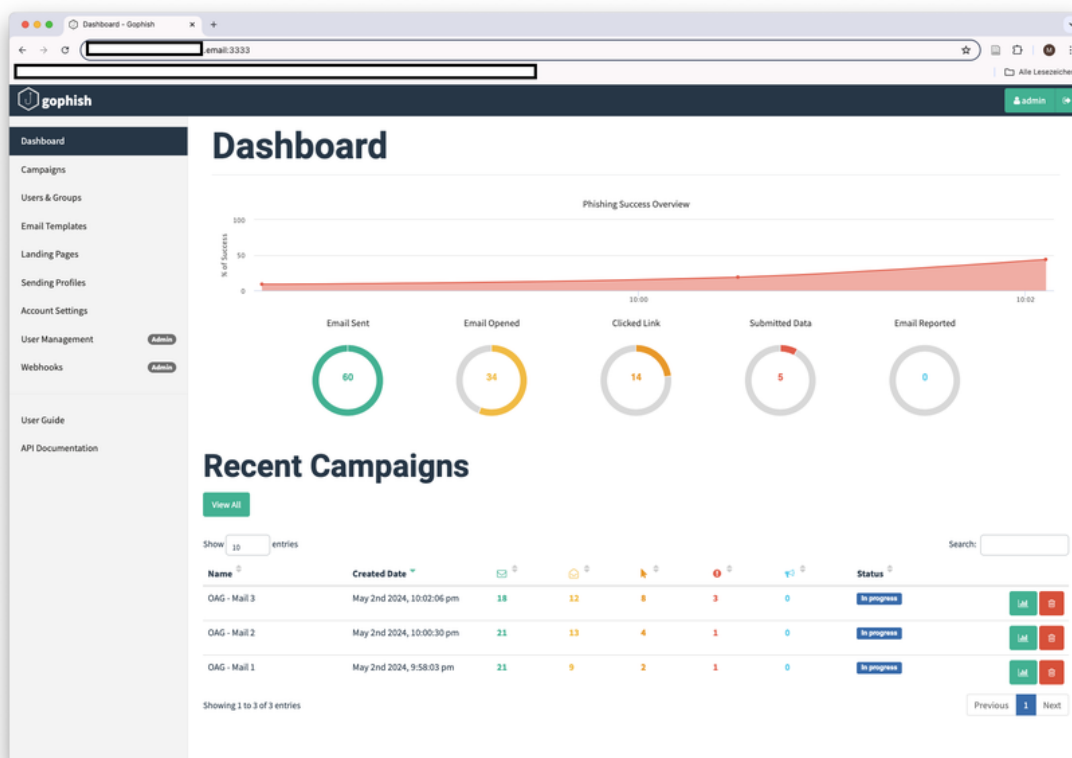


Рис.1.8 – Інтерфейс платформи GoPhish [17]

Evilginx — це спеціалізований інструмент з відкритим вихідним кодом, призначений для моделювання сучасних фішингових атак типу adversary-in-the-middle (AiTM). На відміну від класичних платформ для симуляції фішингу, Evilginx

орієнтований на відтворення технічно складних сценаріїв атак, спрямованих на перехоплення сесійних cookie, токенів автентифікації та обхід механізмів багатофакторної автентифікації (MFA), включно з одноразовими паролями та push-повідомленнями.

Основне призначення Evilginx полягає у демонстрації реальних ризиків, пов'язаних із фішингом нового покоління, а також у перевірці ефективності захисних механізмів організацій, зокрема conditional access, phishing-resistant MFA та інших. Інструмент широко використовується у Red Team-операціях, під час контрольованих тестів на проникнення та в навчальних цілях для підвищення обізнаності фахівців із кібербезпеки щодо актуальних загроз.

З технічної точки зору Evilginx функціонує як зворотний проксі-сервер, який прозоро розміщується між користувачем та легітимним вебресурсом. У процесі взаємодії жертви з підробленим доменом весь трафік передається через Evilginx, що дозволяє перехоплювати облікові дані та сесійні артефакти без порушення логіки роботи автентифікаційних механізмів. Нижче наведено аналіз ключового функціоналу Evilginx відповідно до офіційної документації.

Phishlets (Фішлети). Phishlets є основним конфігураційним компонентом Evilginx. Вони описують правила проксування конкретних вебсервісів, включно з доменами, піддоменами, шляхами URL, cookie та параметрами автентифікації. Кожен phishlet фактично визначає логіку атаки на окремий сервіс (наприклад, Microsoft 365, Google, GitHub). Призначення цього функціоналу полягає у точному відтворенні поведінки легітимного ресурсу з одночасним перехопленням чутливих даних.

Reverse Proxy Engine (Механізм зворотного проксі). Даний компонент відповідає за перехоплення та перенаправлення HTTP/HTTPS-трафіку між жертвою та цільовим ресурсом. Evilginx динамічно модифікує відповіді сервера, підміняючи посилання та домени на фішингові, зберігаючи при цьому повну функціональність вебзастосунку. Це дозволяє користувачу не помітити підміни та успішно пройти всі етапи автентифікації.

Session Cookie Capture (Перехоплення сесійних cookie). Одна з ключових

функцій Evilginx — автоматичне вилучення та збереження cookie автентифікованих сесій. Після успішного входу користувача платформа фіксує значення cookie, що дозволяє зловмиснику застосувати автентифіковану сесію без повторного введення облікових даних або MFA. Саме цей механізм робить можливим обхід багатофакторної автентифікації.

Credential Harvesting (Збір облікових даних). Evilginx здатний перехоплювати логіни та паролі, які вводяться користувачем на фішинговій сторінці. Облікові дані зберігаються разом із метаданими сесії, що дозволяє корелювати їх із конкретним користувачем, IP-адресою та часом атаки. Цей функціонал доповнює перехоплення cookie, але не є єдиною ціллю атаки.

TLS Certificate Management (Керування TLS-сертифікатами). Платформа підтримує автоматичне отримання та оновлення TLS-сертифікатів (зокрема через Let's Encrypt), що забезпечує коректне HTTPS-з'єднання з фішинговими доменами. Призначення цього модуля — підвищення довіри з боку користувачів та браузерів, а також уникнення попереджень про небезпечне з'єднання.

Logging & Session Management (Журнали та керування сесіями). Платформа веде детальні журнали активності, включно з інформацією про відвідування фішингових сторінок, спроби входу та успішні компрометації сесій. Окремо реалізовано керування активними та збереженими сесіями, що дозволяє аналізувати результати атаки та використовувати їх для подальших етапів тестування безпеки. [18]

У підсумку, Evilginx є високотехнологічним інструментом для моделювання фішингових атак нового покоління, які виходять за межі класичного викрадення облікових даних. Його функціонал дозволяє на практиці продемонструвати обмеження традиційних механізмів захисту, зокрема MFA, та підкреслює необхідність впровадження стійких до фішингу методів автентифікації й комплексних стратегій захисту користувачів.

АНАЛІЗ ІНСТРУМЕНТІВ МОДЕЛЮВАННЯ ФІШИНГОВИХ АТАК: МОЖЛИВОСТІ GORNISH ТА EVILGINX У ПОБУДОВІ СЦЕНАРІЇВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

2.1 Архітектура компонентів інфраструктури для проведення соціально-інженерних атак у корпоративних середовищах

Для успішної реалізації таких атак зловмисники дедалі частіше застосовують спеціалізовану інфраструктуру, яка дозволяє масштабувати кампанії, підвищувати їх правдоподібність та ускладнювати виявлення з боку засобів захисту.

Архітектура інфраструктури для проведення соціально-інженерних атак у корпоративних середовищах є багаторівневою та включає сукупність взаємопов'язаних компонентів, кожен з яких виконує чітко визначену функцію в межах атаки. До таких компонентів належать системи керування фішинговими кампаніями, сервери доставки контенту, доменна та мережева інфраструктура, засоби збору та обробки облікових даних. Особливу роль у цій архітектурі відіграє її гнучкість і масштабованість. Сучасні соціально-інженерні атаки часто проводяться у вигляді цілеспрямованих кампаній проти конкретних організацій або груп користувачів (spear phishing), що потребує попередньої підготовки інфраструктури з урахуванням особливостей корпоративного середовища жертви. Це включає аналіз використовуваних поштових сервісів, систем автентифікації, політик безпеки, а також типових сценаріїв взаємодії користувачів з інформаційними ресурсами. Відповідно, архітектура атакуючої інфраструктури формується таким чином, щоб максимально точно відтворювати ці сценарії.

Розуміння архітектури компонентів інфраструктури соціально-інженерних атак є важливим не лише з точки зору аналізу дій зловмисників, але й для побудови ефективних механізмів захисту в корпоративних середовищах. Детальний розгляд взаємодії окремих елементів такої інфраструктури дозволяє виявити критичні точки, на яких можливе виявлення атаки, її блокування або мінімізація наслідків

компрометації. Саме тому в межах даного підрозділу доцільно перейти до наочного представлення типової архітектури інфраструктури, що використовується для проведення соціально-інженерних атак у корпоративних середовищах, з подальшим аналізом її основних компонентів та їх функціонального призначення.

Схема, представлена на рисунку, ілюструє типову модель такої інфраструктури, яка поєднує хмарні обчислювальні ресурси, сервіси доставки електронної пошти, проксі-рівень та спеціалізовані інструменти для моделювання фішингових кампаній і перехоплення облікових даних.

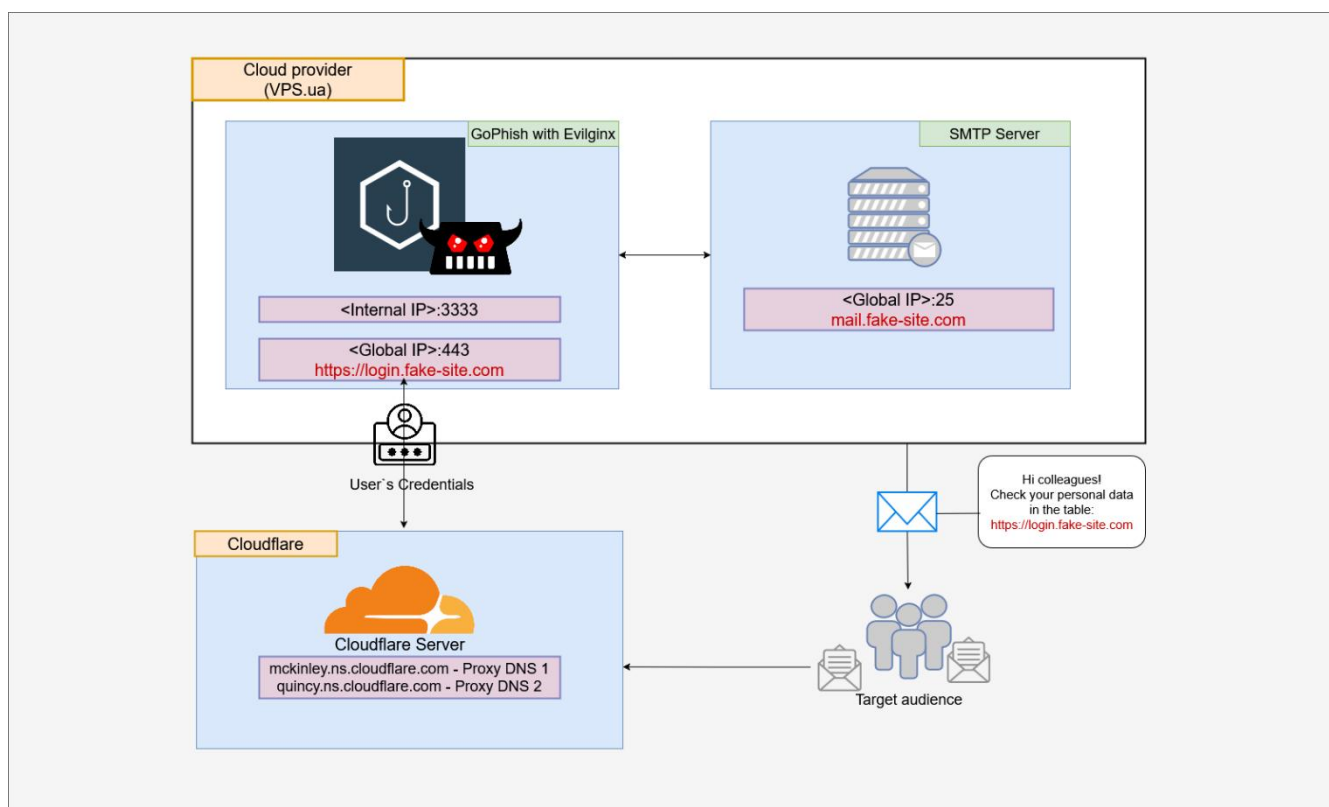


Рис.2.1 – Архітектура компонентів фішингової інфраструктури

Наведена архітектурна схема відображає типову інфраструктуру, що використовується для проведення соціально-інженерних атак у корпоративних середовищах, зокрема фішингових кампаній із використанням сучасних платформ керування атаками та засобів обходу механізмів захисту. Така інфраструктура не є випадковим набором компонентів, а являє собою продуману, логічно вибудовану систему, у якій кожен елемент виконує окрему функцію та взаємодіє з іншими компонентами з метою підвищення ефективності атаки, її стійкості до виявлення та зниження ризиків для оператора атаки.

Cloud Provider (VPS). Основою представленої інфраструктури є хмарний провайдер віртуальних приватних серверів (VPS), на базі якого розгортаються всі ключові серверні компоненти, необхідні для проведення соціально-інженерних атак у корпоративних середовищах. Вибір саме VPS-рішень є обґрунтованим з технічної, організаційної та операційної точок зору, оскільки вони поєднують у собі гнучкість, доступність і певний рівень анонімності для реалізації подібних сценаріїв.

Однією з ключових переваг використання VPS-провайдера є можливість швидкого розгортання інфраструктури без необхідності фізичного доступу до апаратного забезпечення. Сервер може бути створений упродовж кількох хвилин із заздалегідь підготовленого образу операційної системи, що значно скорочує час підготовчого етапу атаки або тестування. Це особливо важливо в умовах, коли соціально-інженерні кампанії мають обмежений часовий проміжок або потребують оперативної адаптації під конкретну цільову організацію.

Важливим нюансом є також масштабованість хмарної інфраструктури. У разі збільшення обсягу фішингової кампанії, кількості цільових користувачів або навантаження на сервер (наприклад, при масових переходах за фішинговими посиланнями), ресурси VPS можуть бути оперативно збільшені — шляхом додавання обчислювальної потужності, оперативної пам'яті або дискового простору. Така гнучкість практично недосяжна при використанні фізичних серверів і дозволяє підтримувати стабільну роботу інфраструктури без помітних затримок або збоїв, які могли б викликати підозру у користувачів.

Окремої уваги заслуговує питання мережевої гнучкості та управління IP-адресами. Хмарні провайдери, як правило, надають можливість швидкої заміни публічної IP-адреси сервера або навіть повного його пересоздання з новими мережевими параметрами. Це є критично важливим у випадках, коли інфраструктура потрапляє до чорних списків систем фільтрації, поштових шлюзів або засобів Threat Intelligence. Замість тривалих процедур відновлення репутації IP-адреси, оператор інфраструктури може швидко мігрувати сервіси на новий VPS, мінімізуючи перерви в роботі кампанії.

Ще одним суттєвим аспектом є можливість географічного вибору розташування серверів. Багато VPS-провайдерів пропонують дата-центри в різних країнах і регіонах, що дозволяє адаптувати інфраструктуру під конкретний корпоративний контекст. Наприклад, розміщення сервера в тому ж регіоні, де знаходиться цільова організація, може знизити затримки мережевого з'єднання та зробити взаємодію з фішинговим ресурсом більш «природною» з точки зору користувача. Крім того, географічна близькість може зменшити кількість додаткових перевірок з боку систем безпеки, які враховують аномальні геолокаційні ознаки.

GoPhish з Evilginx. У межах хмарного VPS розгортається сервер, на якому поєднуються платформа GoPhish та проксі-рішення Evilginx, що разом формують ядро всієї соціально-інженерної інфраструктури. Інтеграція платформи GoPhish із проксі-рішенням Evilginx є важливим елементом сучасної інфраструктури соціально-інженерних атак, оскільки дозволяє об'єднати організаційно-керуючі можливості фішингової платформи з технічними механізмами перехоплення автентифікаційних даних. Така взаємодія реалізується на рівні прикладного програмного інтерфейсу (API) GoPhish і забезпечує узгоджену роботу обох компонентів у межах єдиної кампанії.

GoPhish виступає центральною системою управління, яка відповідає за створення, запуск і моніторинг фішингових кампаній. Evilginx, у свою чергу, інтегрується в цю модель як зовнішній сервіс, що обробляє запити користувачів після переходу за фішинговим посиланням. Для забезпечення взаємодії Evilginx отримує доступ до API GoPhish шляхом використання унікального API-ключа та адреси адміністративного інтерфейсу платформи. Це дозволяє Evilginx ідентифікувати кампанії, передавати інформацію про події та корелювати дії користувачів із конкретними записами в системі GoPhish.

На практиці взаємодія між цими компонентами починається ще на етапі підготовки кампанії. Під час створення фішингового шаблону в GoPhish у тіло електронного листа вставляється спеціальне посилання, яке веде не на статичну фішингову сторінку, а на домен і маршрут, що обслуговується Evilginx. Це

посилання формується таким чином, щоб зберігати унікальні ідентифікатори кампанії та конкретного користувача. Завдяки цьому після переходу за посиланням Evilginx може однозначно визначити, в межах якої кампанії відбувається взаємодія, і зіставити її з даними GoPhish.

Коли користувач відкриває фішинговий лист і переходить за посиланням, GoPhish фіксує сам факт кліку, використовуючи власні механізми трекінгу. Далі управління процесом фактично переходить до Evilginx, який починає виконувати роль проксі між користувачем і легітимним цільовим ресурсом. У цей момент Evilginx обробляє HTTP(S)-запити, проксіює їх до справжнього сервісу та повертає відповіді користувачу, зберігаючи повну прозорість взаємодії.

У процесі автентифікації користувача Evilginx перехоплює введені облікові дані, одноразові коди або сесійні cookie. Після фіксації таких подій Evilginx може передавати відповідну інформацію назад у GoPhish через API. Це дозволяє платформі керування кампаніями відобразити результат атаки в загальній статистиці — наприклад, як факт успішного введення облікових даних конкретним користувачем. Таким чином, GoPhish отримує не лише базову інформацію про кліки, але й розширені результати, пов'язані з компрометацією облікових записів.

Інтерфейс адміністрування GoPhish, як правило, ізольований від зовнішньої мережі та доступний лише через внутрішню IP-адресу сервера і нестандартний порт (наприклад, 3333). Таке рішення має одразу кілька переваг. По-перше, воно суттєво зменшує поверхню атаки та ймовірність випадкового виявлення керуючого інтерфейсу автоматизованими сканерами. По-друге, у разі компрометації доменного імені або зовнішнього веб-ресурсу доступ до панелі управління залишається обмеженим, що підвищує загальну стійкість інфраструктури.

Зовнішній доступ до сервера Evilginx організований через стандартний HTTPS-порт 443 і прив'язаний до доменного імені, яке візуально та семантично імітує легітимний корпоративний ресурс. Використання стандартного порту та TLS-шифрування має не лише технічне, але й психологічне значення. Більшість користувачів асоціює HTTPS-з'єднання з безпечністю та легітимністю ресурсу, а сучасні браузері відкрито попереджають про небезпеку при відсутності

шифрування. Відповідно, коректно налаштований HTTPS є обов'язковою умовою для збереження довіри жертви та уникнення автоматичних блокувань з боку браузерів, поштових клієнтів і захисних шлюзів.

SMTP-сервер. Окремим, але критично важливим компонентом інфраструктури є SMTP-сервер, який використовується для розсилки фішингових повідомлень цільовій аудиторії. Особливість цього компонента полягає в тому, що під час налаштування та експлуатації SMTP-служби практично неминуче відбувається розкриття реальної IP-адреси сервера, з якого здійснюється відправлення електронної пошти. Ця IP-адреса фігурує в заголовках листів, логах поштових серверів та перевіряється системами фільтрації під час аналізу SPF, DKIM і DMARC. У зв'язку з цим SMTP-сервер є одним із найбільш «чутливих» елементів усієї інфраструктури з точки зору виявлення та блокування.

Саме тому в архітектурі соціально-інженерних атак SMTP-сервер часто виноситься в окремий вузол, фізично або логічно ізольований від сервера з фішинговими сторінками чи проксі-компонентами. Такий підхід дозволяє мінімізувати наслідки виявлення поштової інфраструктури. У разі внесення IP-адреси SMTP-сервера до чорних списків або її блокування поштовими провайдерами, основний сервер із GoPhish та Evilginx залишається недоторканим і може продовжувати використовуватися після заміни або міграції поштового вузла.

У сценаріях активності Red Team, де важливо зберігати операційну стійкість і можливість швидкої адаптації до дій захисної сторони, розгортання SMTP-сервера на окремому VPS є практично обов'язковим. Це дозволяє оперативно змінювати IP-адреси, домени або навіть повністю пересоздавати поштову інфраструктуру без впливу на інші компоненти атаки. Така гнучкість є критичною в умовах, коли системи захисту корпоративної мережі активно реагують на підозрілу поштову активність, а кожна хвилина простою може знизити ефективність кампанії.

Водночас у випадках звичайного моделювання атак або проведення контрольованих фішингових перевірок, про які заздалегідь поінформовані підрозділи інформаційної безпеки організації, вимоги до ізоляції SMTP-компонента можуть бути значно нижчими. У таких сценаріях SMTP-служба може

бути розгорнута на тому ж сервері, що й платформа керування кампаніями, без суттєвих ризиків для інфраструктури. Оскільки блокування або розкриття IP-адреси не розглядається як критичний інцидент, акцент робиться не на операційній стійкості, а на спрощенні архітектури та зменшенні витрат на її підтримку.

Незалежно від обраного варіанту розгортання, SMTP-сервер зазвичай налаштовується з використанням доменного імені та коректних DNS-записів SPF, DKIM і DMARC. Це дозволяє підвищити показники доставлюваності електронних листів і зменшити ймовірність їх автоматичної фільтрації як спаму.

Cloudflare. Наступним ключовим елементом цієї архітектури є використання сервісу Cloudflare як проміжного шару між цільовою аудиторією та реальними серверами інфраструктури. Cloudflare виконує одразу декілька функцій. По-перше, він приховує реальну IP-адресу сервера Evilginx, виступаючи як реверс-проксі та DNS-посередник. Це значно ускладнює пряме технічне виявлення та блокування серверів атакуючої інфраструктури, оскільки зовнішні системи бачать лише IP-адреси Cloudflare, а не реального хостингу.

По-друге, використання Cloudflare підвищує рівень довіри до ресурсу з боку користувачів і автоматизованих систем захисту. Багато корпоративних мереж і поштових шлюзів сприймають домени, що працюють через Cloudflare, як менш підозрілі, оскільки цей сервіс широко використовується легітимними компаніями. Наявність коректно налаштованих DNS-серверів Cloudflare також створює враження професійно адміністрованого ресурсу, що є важливим фактором у соціальній інженерії.

По-третє, Cloudflare забезпечує базовий захист від DDoS-атак, автоматизованого сканування та деяких типів мережеских атак. Хоча в контексті соціально-інженерних кампаній це не є основною метою, такий захист підвищує загальну стабільність інфраструктури та зменшує ризик її передчасного виходу з ладу.

Взаємодія всіх компонентів інфраструктури відбувається за чітко визначеним сценарієм. SMTP-сервер надсилає фішингові повідомлення цільовій аудиторії, у яких міститься посилання на домен, захищений Cloudflare. Користувач, переходячи

за цим посиланням, фактично звертається до інфраструктури Cloudflare, яка проксіює запит до реального сервера GoPhish/Evilginx. Evilginx обробляє запит, відображає фішингову сторінку або проксіює легітимний сервіс і перехоплює облікові дані чи сесійні токени, передаючи їх до системи збору даних. Усі ці процеси відбуваються прозоро для користувача, який вважає, що взаємодіє з легітимним корпоративним ресурсом.

Таким чином, представлена архітектура демонструє, що ефективність соціально-інженерних атак у корпоративних середовищах значною мірою залежить не лише від психологічних аспектів впливу на користувачів, але й від правильно побудованої технічної інфраструктури. Використання хмарних сервісів, проксі-рішень і платформ керування кампаніями дозволяє створювати стійкі, масштабовані та важковиявлювані системи, розуміння яких є критично важливим для розробки ефективних заходів захисту та підвищення рівня кіберстійкості організацій.

2.2 Особливості побудови реалістичних сценаріїв соціально-інженерних атак у корпоративному контексті

Побудова ефективних і реалістичних сценаріїв соціально-інженерних атак у корпоративному середовищі базується на глибокому розумінні організаційної структури компанії, поведінкових особливостей її співробітників, а також внутрішніх процесів комунікації. На відміну від масових фішингових кампаній, таргетовані сценарії орієнтовані на максимальну відповідність реальному робочому контексту, що суттєво підвищує ймовірність успішної компрометації.

1. Проведення розвідки (Information Gathering). Розвідка є фундаментальним етапом формування соціально-інженерного сценарію, оскільки саме на цьому етапі збирається інформація, яка дозволяє змодельовати правдоподібну взаємодію з корпоративними користувачами.

У межах корпоративного контексту розвідка може включати:

- **Аналіз контингенту співробітників:** вивчення вікової структури персоналу, рівня цифрової грамотності, досвіду роботи з інформаційними системами та загального розподілу ролей дозволяє визначити, які групи користувачів є більш схильними до певних типів впливу. Наприклад, технічні спеціалісти зазвичай більш обізнані у питаннях кібербезпеки, тоді як адміністративний або фінансовий персонал частіше зосереджується на дотриманні процедур і термінів.

- **Збір інформації про посади та ролі:** особливу цінність становлять дані про осіб, які мають доступ до критичних ресурсів або регулярно взаємодіють з зовнішніми контрагентами та сервісами: бухгалтерія, відділ кадрів, служба технічної підтримки, менеджери проєктів, керівний склад. Саме ці ролі найчастіше стають первинними цілями соціально-інженерних атак.

- **Моніторинг публічних подій компанії:** аналізуються офіційні вебресурси, соціальні мережі, професійні платформи, пресрелізи та новинні публікації. Інформація про реорганізації, внутрішні аудити, оновлення інфраструктури, впровадження нових систем або кадрові зміни створює сприятливий контекст для формування правдоподібних приводів комунікації.

- **Використання персоналізованих тригерів:** виявлення днів народження співробітників, річниць роботи, корпоративних заходів, хобі та інтересів, що можуть бути використані як привід для комунікації.

- **Тестування комунікації:** надсилання нейтральних запитів, таких як:
 - звернення до служби технічної підтримки з типовим питанням;
 - запит щодо процедури працевлаштування;
 - уточнення контактів або формату взаємодії з підрозділом;
 - та інші.

Надсилання нейтральних запитів, що не містять шкідливого навантаження, дозволяє дослідити реальні механізми внутрішньої взаємодії: стиль відповідей, рівень формалізації, структуру листів, формат підписів, швидкість реагування та ієрархію прийняття рішень.

2. Аналіз отриманих результатів. На основі зібраної в ході розвідувального етапу інформації здійснюється комплексний та систематичний аналіз, основною метою якого є формування цілісної поведінкової та організаційної моделі компанії. Така модель дозволяє зрозуміти внутрішні комунікаційні процеси, ієрархію взаємодії між співробітниками, а також особливості корпоративної культури, що безпосередньо впливають на сприйняття інформації персоналом.

Аналіз зосереджується не лише на окремих технічних або формальних елементах комунікації, але й на непрямих поведінкових ознаках, які можуть бути використані для підвищення правдоподібності соціально-інженерних сценаріїв.

Ключовими аспектами аналізу є:

- **Визначення типових шаблонів листування.**

Проводиться аналіз стилю корпоративної електронної комунікації, зокрема характеру звертань (формальний, напівформальний або неформальний), використання стандартних фраз початку та завершення листів, структури теми повідомлення, а також типових мовних конструкцій. Окрема увага приділяється частоті використання скорочень, внутрішньої термінології, англomовних запозичень та професійного жаргону. Це дозволяє відтворити автентичний стиль листування, характерний саме для даної організації.

- **Аналіз підписів та ідентифікаційних елементів.**

Досліджується формат електронних підписів співробітників, включаючи порядок розміщення імені, посади, назви підрозділу, контактних даних, а також наявність стандартних дисклеймерів щодо конфіденційності інформації. Аналізується використання корпоративної символіки, логотипів, кольорового оформлення та гіперпосилань. Така інформація дозволяє уникнути відхилень від звичних для співробітників елементів візуальної ідентифікації.

- **Виявлення довірчих ланцюгів усередині організації.**

На цьому етапі визначаються особи, посади або підрозділи, повідомлення від яких сприймаються співробітниками як авторитетні та не потребують додаткової перевірки. Зазвичай до таких ланцюгів належать керівництво, служба інформаційної безпеки, IT-відділ, бухгалтерія або відділ кадрів. Розуміння цих

довірчих зв'язків дозволяє правильно обрати джерело ініціації комунікації в майбутніх сценаріях.

- **Оцінка типових сценаріїв взаємодії між співробітниками.**

Аналізуються стандартні робочі запити та процеси, з якими персонал стикається на регулярній основі: скидання або зміна паролів, підтвердження доступу до внутрішніх ресурсів, оновлення або погодження документів, фінансові операції, погодження платежів, запити від керівництва у терміновому режимі. Визначення таких сценаріїв дозволяє інтегрувати соціально-інженерні елементи в уже знайомий для співробітників контекст.

- **Аналіз часових та контекстних факторів комунікації.** Додатково оцінюються часові рамки, в яких зазвичай відбувається активна внутрішня комунікація (початок робочого дня, кінець тижня, періоди звітності, корпоративні події, реорганізації або кризові ситуації). Також враховується контекст зовнішніх і внутрішніх подій, які можуть впливати на підвищену чутливість співробітників до певних типів повідомлень. Використання відповідного часу та контексту значно знижує ймовірність виникнення підозр.

Отримані результати аналізу дозволяють мінімізувати використання нетипових або підозрілих елементів у подальших сценаріях соціально-інженерних атак, підвищуючи їх реалістичність та ефективність. Крім того, сформована модель поведінки компанії є основою для побудови адаптивних і контекстно обґрунтованих атак, які відповідають реальним внутрішнім процесам організації.

3. Формування сценаріїв соціально-інженерної атаки. Після завершення етапу аналізу отриманих результатів наступним логічним кроком є безпосереднє формування сценаріїв соціально-інженерної атаки. На цьому етапі зібрана та структурована інформація трансформується у конкретні прикладні сценарії, спрямовані на досягнення визначеної цілі атаки. Формування сценаріїв не зводиться до механічного копіювання виявлених шаблонів, а передбачає їх адаптацію, комбінування та контекстуалізацію з урахуванням людського фактора.

Основною метою даного етапу є створення правдоподібних, логічно обґрунтованих та внутрішньо узгоджених сценаріїв, які органічно вписуються в

повсякденну діяльність компанії та не викликають у співробітників відчуття аномальності або загрози.

Формування сценаріїв соціально-інженерної атаки включає такі ключові складові:

- **Визначення цілі та очікуваного результату сценарію.** На початковому етапі чітко формулюється мета атаки: отримання облікових даних, доступу до внутрішніх систем, виконання фінансової операції, встановлення шкідливого програмного забезпечення або збір додаткової розвідувальної інформації. Від обраної мети безпосередньо залежить тип сценарію, канал комунікації та рівень складності атаки.

- **Вибір та комбінування каналів комунікації та типів соціально-інженерних атак.** Однією з ключових умов успішної реалізації соціально-інженерного сценарію у корпоративному середовищі є коректний вибір каналів комунікації та відповідних типів атак. Канал взаємодії безпосередньо впливає на сприйняття повідомлення, рівень довіри до джерела та готовність співробітника виконати запропоновану дію. У корпоративному контексті комунікація здебільшого відбувається через обмежену кількість стандартизованих каналів, що формує очікування користувачів щодо легітимності повідомлень.

Найпоширенішим каналом залишається електронна пошта, яка використовується для офіційних повідомлень, внутрішніх розпоряджень, запитів та обміну документами. Саме через електронну пошту реалізується більшість фішингових атак, оскільки цей канал дозволяє імітувати корпоративний стиль комунікації, використовувати фірмові шаблони та вкладення, а також маскувати шкідливі посилання під внутрішні ресурси або зовнішні сервіси, що регулярно застосовуються в роботі.

Месенджери дедалі частіше стають об'єктом соціально-інженерного впливу. Повідомлення в таких каналах сприймаються як менш формальні, але більш термінові, що знижує рівень критичного аналізу з боку співробітників. Через месенджери ефективно реалізуються сценарії pretexting та impersonation, коли

зловмисник видає себе за колегу, керівника або представника технічної підтримки з проханням оперативно виконати певну дію.

Телефонний зв'язок залишається важливим каналом для реалізації vishing-атак, особливо у сценаріях, де необхідно створити відчуття авторитету або терміновості. Дзвінки від імені служби безпеки, фінансового відділу або зовнішніх партнерів дозволяють безпосередньо впливати на емоційний стан співробітника та швидко адаптувати сценарій залежно від реакції жертви. Телефонна комунікація часто використовується як допоміжний елемент для підтвердження легітимності попереднього електронного листа.

СМС-повідомлення та месенджери поза корпоративним середовищем застосовуються рідше, однак можуть бути ефективними у сценаріях smishing, зокрема для імітації повідомлень від зовнішніх сервісів, служб доставки або багатофакторної автентифікації. У корпоративному контексті такі атаки зазвичай використовуються як додатковий тригер для спонукання співробітника перейти за посиланням або зв'язатися з ініціатором атаки.

Окрему категорію становлять багатоканальні (multi-channel) сценарії, які поєднують декілька засобів комунікації. Наприклад, первинний контакт може здійснюватися електронною поштою, після чого надходить повідомлення в корпоративному месенджері або телефонний дзвінок з посиланням на попередній лист.

- **Адаптація сценарію до ролі цільового співробітника.** Сценарії формуються з урахуванням посади, рівня доступу та функціональних обов'язків потенційної жертви. Повідомлення, адресоване рядовому співробітнику, суттєво відрізняється за змістом і тоном від звернення до керівника або представника фінансового підрозділу. Така адаптація підвищує ймовірність позитивної реакції на запит.

- **Формування правдоподібного приводу (pretext).** Створюється логічний та переконливий привід для ініціювання комунікації, який безпосередньо пов'язаний з реальними бізнес-процесами компанії. Такий привід може базуватися

на внутрішніх процедурах, термінових завданнях, організаційних змінах, регламентних роботах або зовнішніх подіях. Важливо, щоб запропонований контекст не вимагав від співробітника дій, які виходять за межі його звичних обов'язків.

- **Інтеграція психологічних тригерів.** У сценаріях свідомо використовуються психологічні фактори, що впливають на поведінку людини: авторитет, терміновість, дефіцит часу, страх порушення регламентів, бажання допомогти або уникнути негативних наслідків. Важливо, щоб такі тригери застосовувалися помірковано та відповідали корпоративному контексту, не виглядаючи надмірно маніпулятивними.

6. Ітеративне вдосконалення сценаріїв. Реалістичні сценарії соціально-інженерних атак не є статичними конструкціями. Вони потребують постійного коригування з урахуванням реакцій користувачів, змін у внутрішніх процесах компанії та розвитку захисних механізмів. Аналіз результатів застосування сценаріїв дозволяє виявляти слабкі місця як у поведінці персоналу, так і в самих сценаріях, що створює основу для їх подальшого вдосконалення.

Таким чином, побудова реалістичних сценаріїв соціально-інженерних атак у корпоративному контексті є багатоетапним процесом, що поєднує розвідку, аналітичне моделювання, психологічний вплив та адаптивний підхід. Саме комплексність і глибина цього процесу визначають ефективність соціально-інженерних атак та рівень загрози для сучасних корпоративних інформаційних систем.

2.3 Методика оцінювання рівня обізнаності користувачів та аналіз їх поведінкових реакцій під час тестових кампаній

Оцінювання рівня обізнаності користувачів у сфері інформаційної безпеки є одним із ключових завдань при проведенні тестових фішингових кампаній у корпоративному середовищі. На відміну від технічних вразливостей, людський фактор має динамічний і контекстно залежний характер, що потребує застосування

спеціалізованих методик аналізу поведінки персоналу в умовах змодельованих соціально-інженерних атак.

Використання платформ моделювання фішингових атак, таких як **Gophish** та **Evilginx**, дозволяє не лише імітувати реалістичні сценарії соціальної інженерії, але й збирати кількісні та якісні показники, необхідні для комплексної оцінки реакцій користувачів. У цьому контексті методика оцінювання базується на поєднанні статистичного аналізу дій користувачів, інтерпретації поведінкових моделей та зіставлення отриманих результатів з очікуваними показниками безпеки.

Загальні принципи оцінювання рівня обізнаності користувачів. Методика оцінювання рівня обізнаності користувачів передбачає аналіз їхньої реакції на контрольовані соціально-інженерні стимули, які максимально наближені до реальних загроз. Основним принципом такого оцінювання є акцент на виявленні слабких місць у знаннях і поведінці персоналу.

Оцінювання здійснюється за такими напрямками:

- здатність користувачів розпізнавати ознаки фішингових повідомлень;
- готовність виконувати дії, що суперечать внутрішнім політикам безпеки;
- рівень критичного мислення при взаємодії з електронними повідомленнями;
- дотримання процедур повідомлення про інциденти інформаційної безпеки.

На відміну від анкетування або теоретичного тестування, практичні фішингові кампанії дозволяють оцінювати не декларовані знання, а фактичну поведінку користувачів у робочому середовищі. Теоретичні опитування часто демонструють завищений рівень обізнаності, оскільки користувачі надають соціально бажані відповіді. Натомість симульовані атаки відображають реальні реакції персоналу в умовах, наближених до справжніх загроз, що робить результати такого оцінювання значно більш репрезентативними.

При цьому принципово важливою є правильна інтерпретація результатів тестових кампаній. Реальною метою оцінювання не є досягнення ситуації, за якої

жоден користувач не здійснює помилкових дій, оскільки повна відсутність кліків або взаємодій з фішинговими повідомленнями є практично недосяжною навіть у високозахищених організаціях. Людський фактор завжди залишається змінним і залежним від зовнішніх обставин, навантаження та психологічного стану.

Натомість основною ціллю є поступове зменшення кількості користувачів, які піддаються соціально-інженерному впливу, а також скорочення часу реагування на потенційні інциденти. Ключовим показником ефективності методики є здатність організації виявити та локалізувати атаку до моменту першої фактичної компрометації облікових записів або систем. Це передбачає швидке повідомлення про підозріле повідомлення, своєчасне залучення служби безпеки та оперативне виконання заходів реагування.

Таким чином, методика оцінювання рівня обізнаності користувачів спрямована не на досягнення ідеалізованих показників, а на формування стійкої та адаптивної моделі поведінки персоналу. Регулярне проведення тестових фішингових кампаній дозволяє відстежувати динаміку змін, виявляти найбільш вразливі групи користувачів і коригувати навчальні програми з урахуванням реальних ризиків. У довгостроковій перспективі такий підхід сприяє підвищенню загального рівня кіберстійкості організації та зменшенню наслідків соціально-інженерних атак.

Кількісні метрики оцінювання в тестових кампаніях. Одним із ключових елементів методики є використання кількісних показників, які автоматично збираються платформами Gophish та Evilginx під час проведення кампаній. До базових метрик належать:

- **Open Rate** — частка користувачів, які відкрили фішингове повідомлення;
- **Click Rate** — відсоток користувачів, які перейшли за посиланням у листі;
- **Submission Rate** — кількість користувачів, які ввели облікові дані або іншу конфіденційну інформацію;

- **Session Rate** — кількість користувачів, які авторизувались та отримали сесійний токен;
- **Report Rate** — частка співробітників, які повідомили про підозріле повідомлення службі безпеки;
- **Time-to-Action** — час, що минув від моменту отримання повідомлення до виконання дії.

Gophish дозволяє ефективно відстежувати базові поведінкові реакції користувачів на рівні електронної пошти, тоді як Evilginx надає можливість аналізувати глибші сценарії компрометації, зокрема взаємодію з фішинговими проксі та обходом багатофакторної автентифікації. Це розширює спектр оцінюваних показників і дозволяє виявити не лише поверхневу необізнаність, а й критичні ризики компрометації облікових записів.

Аналіз поведінкових моделей користувачів

Окрім кількісних показників, важливе значення має якісний аналіз поведінкових реакцій користувачів. Поведінка співробітників у тестових кампаніях часто формується під впливом контексту, ролі в організації, рівня навантаження та психологічних чинників.

На основі зібраних даних можна виділити типові поведінкові моделі:

- імпульсивна реакція з негайним виконанням дії;
- умовно обережна поведінка з частковою перевіркою повідомлення;
- ігнорування повідомлення без подальших дій;
- проактивна поведінка з інформуванням служби безпеки.

Аналіз таких моделей дозволяє класифікувати користувачів за рівнем ризику та визначити групи, які потребують пріоритетного навчання або додаткових заходів підвищення обізнаності.

Порівняльний аналіз результатів кампаній. Порівняльний аналіз результатів тестових фішингових кампаній є ключовим етапом методики оцінювання рівня обізнаності користувачів, оскільки дозволяє перейти від разових спостережень до системного розуміння змін у поведінці персоналу з часом. На відміну від одноразового тестування, серія контрольованих кампаній створює

можливість відстежувати динаміку реакцій користувачів, виявляти стійкі поведінкові патерни та оцінювати ефективність впроваджених навчальних і організаційних заходів.

Методика передбачає проведення кількох кампаній, які відрізняються між собою за такими параметрами:

- тип сценарію (інформаційний запит, термінове повідомлення, службове сповіщення, повідомлення від керівництва);
- рівень технічної складності (простий фішинг без підміни доменів, використання схожих доменних імен, застосування HTTPS, інтеграція Evilginx);
- канал комунікації (електронна пошта, месенджери, SMS, комбіновані сценарії);
- ступінь психологічного тиску (терміновість, страх, авторитет відправника).

Порівняння результатів таких кампаній здійснюється за набором кількісних та якісних показників. Зниження Click Rate у повторних кампаніях за схожими сценаріями зазвичай свідчить про формування у користувачів базових навичок розпізнавання фішингових ознак, таких як нетипові формулювання, підозрілі посилання або невідповідність контексту повідомлення. Паралельне зростання Report Rate вказує на розвиток культури відповідального ставлення до інформаційної безпеки та підвищення довіри до внутрішніх каналів повідомлення про інциденти.

Окрему увагу в порівняльному аналізі приділяють кампаніям із використанням інструментів класу Evilginx, які імітують реальні атаки з перехопленням сесій та обходом багатофакторної автентифікації. Якщо показники введення облікових даних у таких сценаріях залишаються стабільно високими навіть після проведення навчальних заходів, це може свідчити про поверхневе розуміння співробітниками принципів роботи MFA та помилкове відчуття повної захищеності. У такому випадку результати аналізу вказують на необхідність коригування навчальних програм з акцентом не лише на “ознаки фішингу”, а й на сучасні техніки атак.

Важливим аспектом порівняльного аналізу є врахування контексту кампаній. Наприклад, зростання кількості помилкових кліків під час пікових робочих навантажень або в періоди організаційних змін (звітні періоди, кадрові перестановки, оновлення ІТ-систем) дозволяє пов'язати поведінкові реакції користувачів із зовнішніми факторами. Такий підхід дає змогу формувати більш реалістичні сценарії майбутніх тестів і точніше прогнозувати ризики.

У довгостроковій перспективі такий підхід дозволяє використовувати результати кампаній як інструмент стратегічного управління ризиками. На основі накопичених даних формуються рекомендації щодо пріоритетних напрямів навчання, коригування політик безпеки та оптимізації процедур реагування. Таким чином, порівняльний аналіз результатів фішингових кампаній стає не лише засобом оцінювання поточного рівня обізнаності, але й основою для побудови стійкої системи підвищення кібергігієни в організації.

Інтерпретація результатів у контексті тестування методом соціальної інженерії. Отримані результати аналізуються не ізольовано, а в контексті застосованих соціально-інженерних сценаріїв. Важливим є розуміння того, які саме елементи сценарію стали вирішальними для успіху або провалу атаки: авторитет джерела, терміновість, персоналізація або вибір каналу комунікації.

Інструменти Gophish та Evilginx у цьому контексті виступають не лише як засоби імітації атак, але і як платформи збору даних, що дозволяють досліджувати ефективність різних методів соціального впливу в корпоративному середовищі.

Значення методики для підвищення рівня безпеки організації. Застосування системної методики оцінювання рівня обізнаності користувачів дозволяє організаціям перейти від формального навчання до data-driven підходу у сфері кібербезпеки. Результати тестових кампаній слугують основою для:

- розробки цільових програм навчання;
- адаптації внутрішніх політик безпеки;
- підвищення ефективності реагування на інциденти;
- зниження ризику успішних соціально-інженерних атак у реальному середовищі.

Таким чином, методика оцінювання рівня обізнаності користувачів та аналіз їх поведінкових реакцій під час тестових кампаній є критично важливим елементом комплексного підходу до забезпечення інформаційної безпеки, а використання інструментів Gophish та Evilginx суттєво розширює можливості такого аналізу в умовах сучасних загроз соціальної інженерії.

ТЕХНОЛОГІЯ МОДЕЛЮВАННЯ СОЦІАЛЬНО-ІНЖЕНЕРНОЇ АТАКИ В КОРПОРАТИВНІЙ СИСТЕМІ З ВИКОРИСТАННЯМ GOPHISH ТА EVILGINX

3.1 Технологія проведення моделювання соціально-інженерних атак та збору результатів

Моделювання соціально-інженерних атак у корпоративному середовищі є ефективним підходом для оцінювання рівня обізнаності персоналу з питань інформаційної безпеки та виявлення потенційних вразливостей у людському факторі. На відміну від реальних атак, моделювання проводиться у контрольованих умовах і має дослідницький характер, що дозволяє отримати об'єктивні дані без завдання шкоди інформаційним активам організації.

У межах даної роботи для реалізації моделювання соціально-інженерних атак використовується платформа Gophish у поєднанні з інструментом Evilginx, що дозволяє відтворити реалістичні сценарії фішингових кампаній та проаналізувати поведінку користувачів. Технологія проведення моделювання представлена у вигляді схеми, яка відображає послідовність дій від ініціації атаки до збору та аналізу результатів.

Встановлення та підготовка Evilginx і Gophish.

На підготовчому етапі здійснюється розгортання інфраструктури для проведення моделювання. Платформа Gophish використовується як основний інструмент для створення, запуску та моніторингу фішингових кампаній. Вона забезпечує керування списками цільових користувачів, шаблонами листів, доменами відстеження та збором статистичних даних.

Для підвищення реалістичності атак додатково використовується Evilginx, який дозволяє моделювати сценарії перехоплення облікових даних або сесій автентифікації. Інтеграція Evilginx з Gophish дає змогу відстежувати не лише факт

переходу за посиланням, але й подальші дії користувача після взаємодії з фішинговим ресурсом.

Для встановлення було встановлено репозиторій з GitHub, у якому є скрипт швидкої збірки файлів у виконувальні.

```
(kali@kali)~[/University]
$ git clone https://github.com/fin3ss3g0d/evilgophish.git
Cloning into 'evilgophish' ...
remote: Enumerating objects: 4654, done.
remote: Counting objects: 100% (978/978), done.
remote: Compressing objects: 100% (539/539), done.
remote: Total 4654 (delta 646), reused 439 (delta 439), pack-reused 3676 (from 1)
Receiving objects: 100% (4654/4654), 37.11 MiB | 6.73 MiB/s, done.
Resolving deltas: 100% (2334/2334), done.

(kali@kali)~[/University]
$ cd evilgophish

(kali@kali)~[/University/evilgophish]
$ ls
CHANGELOG.md  ISSUE_TEMPLATE.md  LICENSE.md  README.md  diagram  evilfeed  evilginx3  gophish  images  replace_rid.sh  setup.sh

(kali@kali)~[/University/evilgophish]
$ ./setup.sh evil-site.com "login" false true user_id
zsh: permission denied: ./setup.sh

(kali@kali)~[/University/evilgophish]
$ chmod +x setup.sh
```

Рис.3.1 – Клонування репозиторію Evilginx з інтеграцією з Gophish

```
(kali@kali)~[/University/evilgophish/evilginx3]
$ sudo ./setup.sh evil-site.com "portal" false true user_id
[evilgophish setup] [*] Installing dependencies with apt
Hit:1 https://kali.download/kali kali-rolling InRelease
Reading package lists ... Done
W: https://kali.download/kali/dists/kali-rolling/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt)
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
Note, selecting 'certbot' instead of 'letsencrypt'
build-essential is already the newest version (12.12).
certbot is already the newest version (4.0.0-2).
wget is already the newest version (1.25.0-2).
git is already the newest version (1:2.51.0-1).
net-tools is already the newest version (2.10-2).
tmux is already the newest version (3.6a-2).
openssl is already the newest version (3.5.4-1).
jq is already the newest version (1.8.1-4).
The following packages were automatically installed and are no longer required:
  dnsmasq eyewitness figlet finger libblosc2-4 libpython3.12t64 libqt6openglwidgets6 libqt6sql6 libqt6sql6-sqlite
  python3-fuzzywuzzy python3-git python3-gitdb python3-levenshtein python3-numexpr python3-odf python3-pandas pyt
  python3-pyvirtualdisplay python3-qasync python3-rapidfuzz python3-serial-asyncio python3-smmmap python3-tables p
  wapiti
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 2384 not upgraded.
[evilgophish setup] [+] Installed dependencies with apt!
[evilgophish setup] [*] Installing Go from source
--2026-01-12 08:03:51-- https://go.dev/dl/go1.25.5.linux-amd64.tar.gz
Resolving go.dev (go.dev)... 216.239.34.21, 216.239.36.21, 216.239.32.21, ...
Connecting to go.dev (go.dev)|216.239.34.21|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://dl.google.com/go/go1.25.5.linux-amd64.tar.gz [following]
--2026-01-12 08:03:51-- https://dl.google.com/go/go1.25.5.linux-amd64.tar.gz
Resolving dl.google.com (dl.google.com)... 142.250.180.110, 2a00:1450:4008:807::200e
Connecting to dl.google.com (dl.google.com)|142.250.180.110|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 59768009 (57M) [application/x-gzip]
Saving to: 'go1.25.5.linux-amd64.tar.gz'

go1.25.5.linux-amd64.tar.gz 100%[=====]
2026-01-12 08:03:53 (34.1 MB/s) - 'go1.25.5.linux-amd64.tar.gz' saved [59768009/59768009]

[evilgophish setup] [+] Installed Go from source!
[evilgophish setup] [*] Configuring gophish
sed: can't read gophish/config.json: No such file or directory
../setup.sh: line 94: cd: evilfeed: No such file or directory
```

Рис.3.2 – Збірка та налаштування Evilginx з інтеграцією з Gophish за допомогою скрипту

```
(kali@kali)-[~/University/evilgophish/gophish]
$ ./gophish
time="2026-01-12T08:17:33-06:00" level=warning msg="No contact address has been configured."
time="2026-01-12T08:17:33-06:00" level=warning msg="Please consider adding a contact_address entry in your config.json"
goose: migrating db environment 'production', current version: 0, target: 20220321133237
OK 20160118194630_init.sql
OK 20160131153104_0.1.2_add_event_details.sql
OK 20160211211220_0.1.2_add_ignore_cert_errors.sql
OK 20160217211342_0.1.2_create_from_col_results.sql
OK 20160225173824_0.1.2_capture_credentials.sql
OK 20160227180335_0.1.2_store-smtp-settings.sql
OK 20160227180336_0.1.2_store-sms-settings.sql
OK 20160317214457_0.2_redirect_url.sql
OK 20160605210903_0.2_campaign_scheduling.sql
OK 20170104220731_0.2_result_statuses.sql
OK 20170219122503_0.2.1_email_headers.sql
OK 20170827141312_0.4_utc_dates.sql
OK 20171027213457_0.4.1_maillogs.sql
OK 20171027213458_0.4.1_smslogs.sql
OK 20171208201932_0.4.1_next_send_date.sql
OK 20180223101813_0.5.1_user_reporting.sql
OK 20180524203752_0.7.0_result_last_modified.sql
OK 20180527213648_0.7.0_store_email_request.sql
OK 20180830215615_0.7.0_send_by_date.sql
OK 20190105192341_0.8.0_rbac.sql
OK 20191104103306_0.9.0_create_webhooks.sql
OK 20200116000000_0.9.0_imap.sql
OK 20200619000000_0.11.0_password_policy.sql
OK 20200730000000_0.11.0_imap_ignore_cert_errors.sql
OK 20200914000000_0.11.0_last_login.sql
OK 20201201000000_0.11.0_account_locked.sql
OK 20220321133237_0.4.1_envelope_sender.sql
time="2026-01-12T08:17:33-06:00" level=info msg="Please login with the username admin and the password 9bdf0ca48926b309"
time="2026-01-12T08:17:33-06:00" level=info msg="Background Email Worker Started Successfully - Waiting for Campaigns"
time="2026-01-12T08:17:33-06:00" level=info msg="Starting IMAP monitor manager"
time="2026-01-12T08:17:33-06:00" level=info msg="Starting phishing server at https://127.0.0.1:8080"
time="2026-01-12T08:17:33-06:00" level=info msg="Starting new IMAP monitor for user admin"
time="2026-01-12T08:17:33-06:00" level=info msg="Starting admin server at https://127.0.0.1:3333"
time="2026-01-12T08:17:33-06:00" level=info msg="Background SMS Worker Started Successfully - Waiting for Campaigns"
time="2026-01-12T08:17:54-06:00" level=info msg="127.0.0.1 - - [12/Jan/2026:08:17:54 -0600] \"GET / HTTP/2.0\" 307 51 \"\" \"Mozilla/5.0 (X11; Linux
```

Рис.3.3 – Запуск Gophish

```
(kali@kali)-[~/University/evilgophish/evilginx3]
$ sudo ./evilginx3-developer -p phishlets/ -g ~/University/evilgophish/gophish/gophish.db


-- Community Edition --
by Kuba Gretzky (@mrgretzky) version 3.2.0

[08:23:33] [inf] Evilginx Mastery Course: https://academy.breakdev.org/evilginx-mastery (learn how to create phishlets)
[08:23:33] [inf] loading phishlets from: phishlets/
[08:23:33] [inf] loading configuration from: /root/.evilginx
[08:23:33] [inf] blacklist mode set to: unauth
[08:23:33] [inf] unauthorized request redirection URL set to: https://www.youtube.com/watch?v=dQw4w9WgXcQ
[08:23:33] [inf] https port set to: 443
[08:23:33] [inf] dns port set to: 53
[08:23:33] [inf] autocert is now enabled
[08:23:34] [inf] blacklist: loaded 0 ip addresses and 0 ip masks
[08:23:34] [war] server domain not set! type: config domain <domain>
[08:23:34] [war] server external ip not set! type: config ipv4 external <external_ipv4_address>

+-----+-----+-----+-----+-----+
| phishlet | status | visibility | hostname | unauth_url |
+-----+-----+-----+-----+-----+
| ukrnet   | disabled | visible   |           |             |
+-----+-----+-----+-----+-----+

: config domain evil-site.com
[08:23:54] [inf] server domain set to: evil-site.com
[08:23:54] [war] server external ip not set! type: config ipv4 external <external_ipv4_address>
: config ipv4 external 127.0.0.1
[08:24:21] [inf] server external IP set to: 127.0.0.1
: phishlets hostname evil-site.com
[08:34:00] [err] phishlets: invalid syntax: [hostname evil-site.com]
: phishlets hostname ukrnet evil-site.com
```

Рис.3.4 – Первинне налаштування Evilginx

```

: phishlets hostname ukrnet evil-site.com
[08:34:09] [inf] phishlet 'ukrnet' hostname set to: evil-site.com
[08:34:09] [inf] disabled phishlet 'ukrnet'
: phishlets enable ukrnet
[08:34:18] [inf] enabled phishlet 'ukrnet'
: lures create ukrnet
[08:34:28] [inf] created lure with ID: 0
: lures get-url 0

https://portal.evil-site.com/vVQxyYgP

:
[evil] 0:[tmux]*

```

Рис.3.5 – Налаштування параметрів фішингової сторінки та створення унікального URL

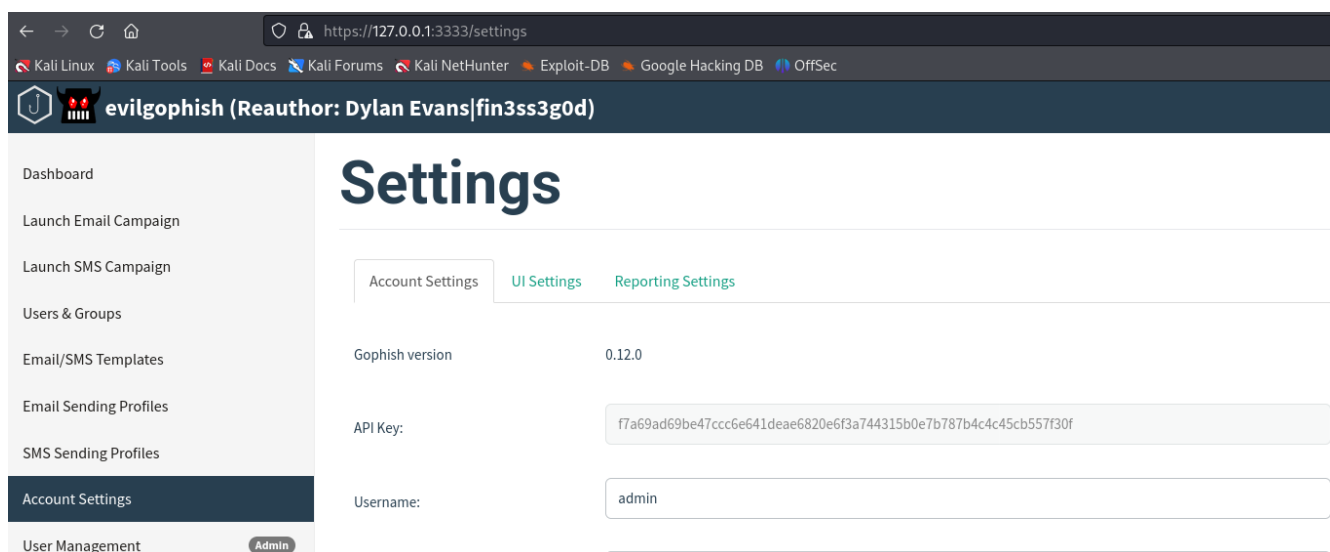


Рис.3.6 – Інтеграція Evilginx з Gophish за допомогою API-ключа

```

GNU nano 7.2 /root/.evilginx/config.json
{
  "blacklist": {
    "mode": "unauth"
  },
  "general": {
    "domain": "evil-site.com",
    "ipv4": "",
    "external_ipv4": "127.0.0.1",
    "bind_ipv4": "",
    "unauth_url": "https://www.youtube.com/watch?v=dQw4w9WgXcQ",
    "https_port": 443,
    "dns_port": 53,
    "autocert": true
  },
  "gophish": {
    "admin_url": "https://127.0.0.1:3333",
    "api_key": "f7a69ad69be47ccc6e641daee6820e6f3a744315b0e7b787b4c4c45cb557f30f",
    "insecure": true
  },
  "lures": [

```

Рис.3.7 – Інтеграція Evilginx з Gophish за допомогою API-ключа

Технологія проведення моделювання соціально-інженерних атак.

Технологія проведення моделювання реалізується у вигляді поетапної схеми, наведеної на рисунку, та включає наступні етапи.

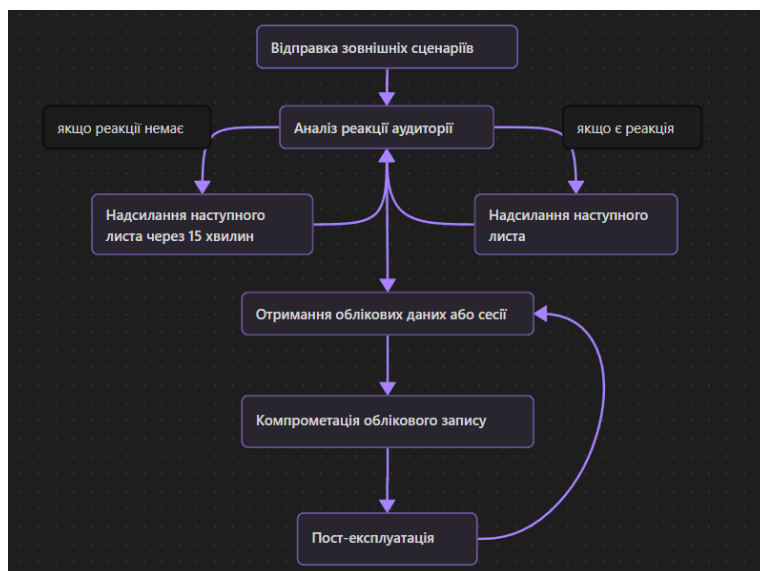


Рис.3.8 – Технологія проведення моделювання соціально-інженерних атак

1. На першому етапі здійснюється відправка зовнішніх сценаріїв. Користувачам корпоративного середовища надсилаються підготовлені фішингові повідомлення, що імітують легітимну внутрішню комунікацію. Надсилання виконується через платформу Gophish у межах визначеної кампанії.

2. Після відправлення повідомлень виконується аналіз реакції аудиторії. На цьому етапі відстежується поведінка користувачів: відкриття листів, переходи за посиланнями, взаємодія з вкладеним контентом. Залежно від наявності або відсутності реакції реалізуються різні сценарії подальших дій.

У разі, якщо реакція користувача відсутня, через визначений інтервал часу (у даному випадку 15 хвилин) здійснюється надсилання наступного листа. Це застосовується для запобігання ймовірності блокування на поштових шлюзах через отримання великої кількості листів з фішингового домену.

У разі, якщо реакція користувача присутня, виконується відразу надсилання наступного листа.

3. Наступним етапом моделювання соціально-інженерної атаки є отримання облікових даних або активної сесії користувача у разі, якщо співробітник взаємодіє з підготовленим фішинговим ресурсом та вводить свої автентифікаційні дані. Даний етап моделює успішну фазу атаки, що свідчить про потенційну компрометацію облікового запису внаслідок дії людського фактора.

4. Після фіксації факту введення облікових даних схема переходить до етапу їх умовної перевірки, який імітує процес валідації доступу до корпоративного ресурсу. Цей етап демонструє можливість компрометації облікового запису.

5. Завершальним етапом моделювання є пост-експлуатація, яка в контексті дослідження розглядається як аналіз можливих дій зловмисника після успішної компрометації облікового запису. До таких дій належить пошук доступів до інших ресурсів, виявлення чутливої інформації, а також можливість надсилання внутрішніх електронних листів зі скомпрометованого облікового запису з метою подальшого поширення атаки.

Особливістю даного етапу є його циклічний характер. У процесі доступу до корпоративного порталу зловмисник потенційно може отримати додаткові облікові дані, логіни, паролі або посилання на внутрішні ресурси, що дозволяє повторно повертатися до етапу отримання облікових даних. Аналогічний ефект може виникати внаслідок спрацювання внутрішніх фішингових повідомлень, надісланих від імені скомпрометованого користувача.

Збір та візуалізація статистики через Gophish

Збір результатів моделювання здійснюється автоматично за допомогою вбудованих механізмів Gophish. Платформа надає візуальну статистику щодо кількості відправлених листів, відкриттів, переходів за посиланнями та інших дій користувачів. Отримані дані використовуються для оцінювання ефективності сценаріїв соціально-інженерних атак та визначення найбільш вразливих етапів взаємодії персоналу з потенційно небезпечним контентом.

Наступний приклад отриманої статистики наведено на одній із проведених фішингових кампаній.

Profits for S2

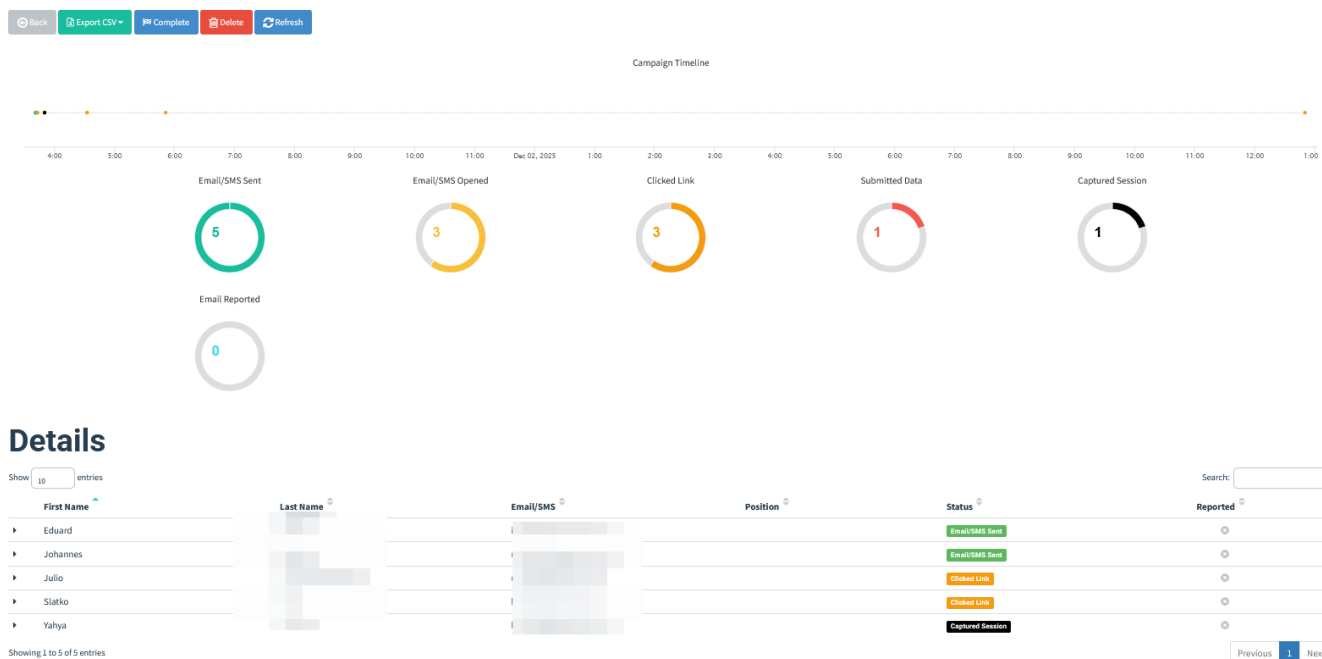


Рис.3.9 – Візуалізація результатів проведення тестування соціально-інженерних атак в платформі Gophish

Кожна фішингова кампанія в межах моделювання соціально-інженерних атак поділяється на окремі сценарії, які відрізняються тематикою повідомлень, стилем подачі інформації, рівнем персоналізації, а також використовуваними психологічними тригерами. Такий підхід дозволяє відтворити різні варіанти поведінки зловмисника та оцінити реакцію користувачів на різні типи соціально-інженерного впливу.

Після завершення кампанії здійснюється аналіз отриманих результатів за допомогою платформи Gophish, яка надає статистичні дані щодо відкриття листів, переходів за посиланнями, введення облікових даних та інших дій користувачів. На основі цих показників визначається ефективність кожного сценарію окремо.

Порівняльний аналіз результатів дає змогу встановити, який саме сценарій мав найбільший вплив на аудиторію, а також виявити фактори, що сприяли підвищенню рівня довіри користувачів до фішингових повідомлень. Отримані висновки використовуються для оцінки рівня обізнаності персоналу, виявлення найбільш уразливих категорій користувачів та формування рекомендацій щодо підвищення ефективності заходів з інформаційної безпеки.

3.2 Рекомендації щодо підвищення рівня захисту корпоративного середовища від соціально-інженерних атак

Соціально-інженерні атаки продовжують залишатися однією з найбільш ефективних загроз для корпоративних середовищ. Вони експлуатують психологічні та поведінкові особливості співробітників, використовуючи людський фактор як головний вектор компрометації. Враховуючи динамічний розвиток методів атак, забезпечення ефективного захисту корпоративної інформації потребує комплексного та системного підходу, який поєднує організаційні, навчальні та технічні заходи.

- **Організаційні заходи.** Організаційні заходи формують фундамент для управління ризиками соціально-інженерних атак. Вони спрямовані на створення чітких правил поведінки співробітників та визначення механізмів контролю за доступом до корпоративних ресурсів.
- **Розробка та впровадження внутрішніх політик безпеки.** Важливим елементом є створення комплексних політик, які визначають порядок роботи з електронною поштою, корпоративними документами та обліковими даними. Політики повинні включати інструкції щодо перевірки джерел повідомлень, алгоритми реагування на підозрілі дії та процедури повідомлення департаменту інформаційної безпеки. Чітко сформульовані правила допомагають стандартизувати поведінку користувачів і зменшують ризик інцидентів, пов'язаних із людським фактором.
- **Обмеження доступу до критичних ресурсів.** Для зниження потенційного впливу компрометації окремого облікового запису необхідно реалізовувати принцип мінімальних привілеїв. Кожен користувач повинен мати доступ лише до тих ресурсів, які необхідні для виконання його функціональних обов'язків. Це дозволяє обмежити поширення наслідків атаки і знизити ризик масштабних порушень безпеки.

- **Багатоканальні процедури підтвердження дій.** Для операцій, пов'язаних із передачею чутливої інформації, фінансовими транзакціями або доступом до конфіденційних ресурсів, рекомендується використовувати багатоканальні підтвердження: наприклад, поєднувати електронну пошту та телефонний дзвінок або застосовувати двоетапну верифікацію. Такий підхід ускладнює реалізацію атак навіть за умови компрометації одного каналу комунікації.

- **Стандартизація корпоративних листів.** Використання унікальних корпоративних шаблонів повідомлень і підписів допомагає співробітникам відрізняти легітимні повідомлення від потенційно шкідливих. Додатково рекомендується впроваджувати механізми верифікації легітимності листів, наприклад, цифрові підписи або спеціальні маркери безпеки

- **Формування культури безпеки.** Працівники повинні розуміти, що їхня поведінка безпосередньо впливає на загальний рівень захищеності компанії. Створення внутрішньої мотивації до дотримання політик безпеки сприяє більшій дисциплінованості та свідомості при роботі з інформацією.

- **Зворотний зв'язок і аналіз поведінки.** Регулярне оцінювання реакцій співробітників на контрольовані соціально-інженерні стимули дозволяє коригувати навчальні програми та політики безпеки. Це забезпечує адаптацію заходів захисту до нових методів атак та підвищує їх ефективність.

- **Актуалізація політик та процедур.** В умовах постійної еволюції технологій та атак, внутрішні політики безпеки та навчальні програми повинні регулярно оновлюватися та відповідати сучасним вимогам інформаційної безпеки.

- **Навчання та підвищення обізнаності користувачів.** Людський фактор залишається найбільш вразливим елементом захисту. Навчання та підвищення обізнаності користувачів є ключовим елементом будь-якої стратегії захисту.

- **Тренінги з кібергігієни.** Працівники повинні регулярно проходити навчання щодо основних методів соціально-інженерних атак, таких як фішинг, спір-фішинг, вішинг, смішинг та інші. Навчальні програми повинні включати

приклади реальних сценаріїв, пояснення ознак шкідливих повідомлень, а також методи безпечної взаємодії з корпоративними системами.

- **Регулярні практичні перевірки.** Для оцінки реальної поведінки користувачів рекомендується проводити контрольовані симуляції атак. Це дозволяє відокремити декларовані знання від практичних навичок і визначити слабкі місця в поведінці персоналу. Практичні перевірки повинні бути різноманітними за сценаріями, каналами комунікації та рівнем складності, щоб охопити широкий спектр можливих загроз.

- **Підвищення швидкості реагування.** Основна мета навчання полягає не в досягненні абсолютної відсутності помилкових дій, а у зменшенні кількості користувачів, які можуть стати жертвами атак, та скороченні часу реагування до моменту потенційної компрометації. Чим швидше співробітники розпізнають підозрілі дії та повідомляють про них, тим менше шансів у зловмисників реалізувати атаку.

Технічні заходи. Технічні засоби доповнюють організаційні та навчальні ініціативи та забезпечують автоматизований рівень захисту:

- **Багатофакторна автентифікація (MFA).** MFA суттєво знижує ризик несанкціонованого доступу навіть при компрометації облікових даних. Рекомендується застосовувати MFA для всіх користувачів, особливо для облікових записів із доступом до критичних систем.

- **Моніторинг та фільтрація підозрілих ресурсів.** Корпоративне середовище має оснащуватися інструментами для виявлення та блокування підробних веб-сайтів, шкідливих доменів та підозрілих вкладень. Такі засоби підвищують швидкість реагування на потенційні загрози та зменшують ймовірність успішної атаки.

Підвищення рівня захисту корпоративного середовища від соціально-інженерних атак можливе лише за умови комплексного підходу. Ефективна стратегія передбачає поєднання організаційних політик, навчання персоналу та технічних засобів захисту. Головна мета заходів полягає не у досягненні абсолютної безпеки, а у зменшенні ймовірності успішної атаки, підвищенні

швидкості реагування користувачів та формуванні стійкої культури кібергігієни в організації. Такий підхід забезпечує адаптивність захисної системи та дозволяє оперативно реагувати на нові загрози, тактики та інструменти зловмисників.

ВИСНОВКИ

Дослідження проблеми соціально-інженерних атак у корпоративних середовищах показало, що основним чинником їх успішності залишається людський фактор. Недостатній рівень обізнаності користувачів, довіра до внутрішніх комунікацій та відсутність систематичних навчальних програм підвищують ймовірність успішної взаємодії співробітників із фішинговими або соціально-маніпулятивними повідомленнями. Аналіз реальних інцидентів підтверджує, що навіть добре налаштовані технічні засоби захисту не здатні повністю запобігти атакам без відповідного рівня уваги та знань персоналу.

У ході роботи було проаналізовано основні види соціально-інженерних атак, зокрема фішинг, vishing, smishing, pretexting та tailgating, а також їх поширеність у корпоративних середовищах. Встановлено, що фішингові атаки залишаються найбільш поширеними, оскільки вони поєднують простоту реалізації з високою ефективністю завдяки психологічним тригерам, персоналізації повідомлень та використанню актуальних корпоративних подій для підвищення довіри користувачів. Аналіз динаміки атак за останні роки показав поступове ускладнення сценаріїв, зростання рівня соціальної інженерії та використання багатоканальних методів впливу.

Дослідження функціоналу платформ Gophish та Evilginx показало, що сучасні інструменти моделювання фішингових атак дозволяють ефективно оцінювати потенційні ризики та виявляти слабкі місця у поведінці користувачів. Навіть без проведення практичного моделювання, аналіз можливостей цих платформ дозволяє зрозуміти, які сценарії і які елементи персоналізації можуть мати найбільший вплив на співробітників. Це дає змогу прогнозувати можливі наслідки атак, планувати навчальні програми та впроваджувати заходи, спрямовані на зниження ризику компрометації облікових записів.

Особлива увага приділяється аналізу ролі людського фактора: реакції користувачів на фішингові повідомлення, психологічні особливості сприйняття інформації, поведінкові моделі та типові помилки. Виявлено, що ефективність

атаки значно підвищується, коли зловмисник використовує персоналізовані дані, пов'язані з посадою, внутрішніми подіями або інтересами співробітників. Такі спостереження підкреслюють важливість регулярного навчання, підвищення інформаційної обізнаності та впровадження процедур перевірки підозрілих повідомлень на всіх рівнях організації.

Загалом, дослідження підтверджує, що для ефективного захисту корпоративного середовища необхідно поєднувати технічні засоби захисту з навчанням персоналу, аналізом поведінки користувачів та використанням аналітики щодо потенційних сценаріїв атак. Це дозволяє формувати комплексний підхід до управління ризиками, знижувати ймовірність успішної соціально-інженерної атаки та мінімізувати загрози витоку чутливої інформації.

Результати роботи можуть бути використані для розробки навчальних програм з кібербезпеки, внутрішніх політик захисту інформації, а також для подальших досліджень у сфері соціальної інженерії та поведінкової аналітики користувачів у корпоративних системах.

ПЕРЕЛІК ПОСИЛАНЬ

1. What is Baiting: Types, Examples and Protection - Keepnet. *Keepnet Labs*. URL: <https://keepnetlabs.com/blog/what-is-baiting-in-cyber-security> (date of access: 28.12.2025).
2. 2025 Data Breach Investigations Report. URL: <https://www.verizon.com/business/resources/Tea/reports/2025-dbir-data-breach-investigations-report.pdf> (date of access: 28.12.2025).
3. Investigating targeted “payroll pirate” attacks affecting US universities | Microsoft Security Blog. Microsoft Security Blog. URL: <https://www.microsoft.com/en-us/security/blog/2025/10/09/investigating-targeted-payroll-pirate-attacks-affecting-us-universities/> (date of access: 28.12.2025).
4. New sophisticated email-based attack from NOBELIUM | Microsoft Security Blog. Microsoft Security Blog. URL: <https://www.microsoft.com/en-us/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/> (date of access: 28.12.2025).
5. Admin. Placing Threat Groups Under a Microscope: Lapsus\$. Secure What's Next | LevelBlue. URL: <https://levelblue.com/blogs/levelblue-blog/placing-threat-groups-under-a-microscope-lapsus> (date of access: 28.12.2025).
6. Page C. Twilio hacked by phishing campaign. TechCrunch. URL: <https://techcrunch.com/2022/08/08/twilio-breach-customer-data/> (date of access: 28.12.2025).
7. Microsoft seizes 340 websites linked to growing phishing subscription service. Reuters. URL: <https://www.reuters.com/sustainability/boards-policy-regulation/microsoft-seizes-340-websites-linked-growing-phishing-subscription-service-2025-09-16/> (date of access: 28.12.2025).
8. Phishing Statistics 2025: AI, Costs & Industry Targets. DeepStrike. URL: <https://deepstrike.io/blog/Phishing-Statistics-2025> (date of access: 28.12.2025).

9. Cybercrime: Lessons learned from a \$25m deepfake attack. World Economic Forum. URL: <https://www.weforum.org/stories/2025/02/deepfake-ai-cybercrime-arup/> (date of access: 28.12.2025).
10. Radware Captcha Page. Radware Captcha Page. URL: <https://www.radware.com/cyberpedia/bot-attacks/phishing-attack/> (date of access: 28.12.2025).
11. What Is A Social Engineering Attack? (& How To Prevent Them). PurpleSec. URL: <https://purplesec.us/learn/social-engineering-attacks/> (date of access: 28.12.2025).
12. 2025 Verizon DBIR: Key Facts, Trends & Statistics - Keepnet. Keepnet Labs. URL: <https://keepnetlabs.com/blog/2025-verizon-data-breach-investigations-report> (date of access: 28.12.2025).
13. What is a Vishing Attack? Definition, Examples & Prevention. Wallarm | Advanced API Security. URL: <https://www.wallarm.com/what/vishing-attack> (date of access: 28.12.2025).
14. Schematic Sequence of Smishing Attack. Researchgate. URL: https://www.researchgate.net/figure/Schematic-Sequence-of-Smishing-Attack_fig3_388423758 (date of access: 28.12.2025).
15. What is a tailgating attack + how to protect yourself – Norton. Norton AntiVirus, Privacy, Identity, & Advanced Scam Protection. URL: <https://us.norton.com/blog/emerging-threats/tailgating-attack> (date of access: 28.12.2025).
16. Documentation | Gophish User Guide. Introduction | Gophish User Guide. URL: <https://docs.getgophish.com/user-guide/documentation> (date of access: 28.12.2025).
17. Interface of GoPhish. Researchgate. URL: https://www.researchgate.net/figure/nterface-of-GoPhish-This-is-just-an-example-no-confidential-information-is-shown_fig3_391878214 (date of access: 28.12.2025).
18. Guides | Evilginx. Introduction | Evilginx. URL: <https://help.evilginx.com/category/guides> (date of access: 28.12.2025).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)