Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки та захисту
інформації
_____Іван ПАРХОМЕНКО
«___» червня 2025р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітній ступень бакалавр

освітня програма Кібербезпека
(назва освітньо-професійної програми)

на тему: «Механізми протидії методам соціальної інженерії орієнтованим на поширення шкідливого програмного забезпечення»

Виконавець: студенка IV курсу, групи КБ-42

_____ **Єлизавета СУХОМЛИН**
(підпис) (ім'я, прізвище)

	Підпис	**Ім'я ПРІЗВИЩЕ**
Керівник		Юрій ЩЕБЛАНІН
Нормоконтроль		Яніна ШЕСТАК

Київ 2025

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____Іван ПАРХОМЕНКО
«29» листопада 2024 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньо-професійної програми)

Студентці **КБ-42** **Сухомлин Єлизаветі Максимівні**
(група) (прізвище ім'я по батькові)

Тема кваліфікаційної роботи Механізми протидії методам соціальної інженерії орієнтованим на поширення шкідливого програмного забезпечення

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №6 від 28.11.2024 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Методи соціальної інженерії, шкідливе програмне забезпечення

3.ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Проаналізувати методи соціальної інженерії, проаналізувати типи шкідливого програмного забезпечення та вектори їх поширення, визначити організаційні заходи для підвищення захисту від атак соціальної інженерії, розробити алгоритм навчання користувачів з протидії методам соціальної інженерії

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Реалізація універсального алгоритму навчання користувачів з протидії методам соціальної інженерії

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29листопада 2024 року

Завдання видав _____ (підпис) Юрій ЩЕБЛАНІН (ім'я, прізвище)

Завдання прийняла до виконання _____ (підпис) Єлизавета СУХОМЛИН (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	29.11.2024 – 20.01.2025	*виконано*
2	Аналіз літератури	21.01.2025 – 11.02.2025	*виконано*
3	Обґрунтування вибору рішення	12.02.2025 – 15.02.2025	*виконано*
4	Написання загального плану роботи	16.02.2025 – 01.03.2025	*виконано*
5	Аналіз теоретичних основ соціальної інженерії та шкідливого програмного забезпечення	02.03.2025 – 20.03.2025	*виконано*
6	Дослідження основних методів соціальної інженерії спрямованих на поширення шкідливого програмного забезпечення	21.03.2025 – 14.04.2025	*виконано*
7	Визначення механізмів протидії поширенню шкідливого програмного забезпечення методами соціальної інженерії	15.04.2025 – 17.05.2025	*виконано*
8	Оформлення пояснювальної записки	18.05.2025 – 02.06.2025	*виконано*
9	Підготовка до захисту кваліфікаційної роботи	03.06.2025 –13.06.2025	*виконано*

Завдання видав _____ (підпис) Юрій ЩЕБЛАНІН (ім'я, прізвище)

Завдання прийняла до виконання _____ (підпис) Єлизавета СУХОМЛИН (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 13 червня 2025 року

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, має 70 сторінок основного тексту, 26 таблиць та 7 рисунків. Список використаних джерел містить 55 найменувань і займає 7 сторінок.

Метою даної роботи є розробка механізму протидії поширенню шкідливого програмного забезпечення методами соціальної інженеріїдля підвищення рівня кіберзахисту.

Для досягнення зазначеної мети поставлено наступні завдання**:**

- Проаналізувати поняття та класифікацію соціальної інженерії в контексті кібербезпеки.
- Дослідити шкідливе програмне забезпечення: цілі, види, механізми дії та розповсюдження.
- Дослідити методи та засоби соціальної інженерії, орієнтовані на поширення шкідливого програмного забезпечення
- Дослідити основні вектори розповсюдження шкідливого програмного забезпечення з використанням соціальної інженерії
- Описати типові сценарії атак і проаналізувати їх ефективність.
- Розробити рекомендації для користувачів та організацій щодо зниження ризиків зараження шкідливим програмним забезпеченням через соціально-інженерні впливи.

Об'єктом дослідження є процес протидії методам соціальної інженерії орієнтованим на поширення шкідливого програмного забезпечення.

Предметом дослідження є методи та засоби протидії поширенню шкідливого програмного забезпечення методами соціальної інженерії.

Практичною цінністю отриманих результатів є реалізація універсального алгоритму навчання користувачів з протидії методам соціальної інженерії.

Ключові слова: соціальна інженерія, людський фактор, шкідливе програмне забезпечення, фішинг, кібербезпека, методи захисту.

ЗМІСТ

ВСТУП

У сучасному світі кіберзагрози стали не лише технічно складними, але й дедалі більш витонченими з точки зору психологічного впливу на користувача. Однією з найефективніших тактик зловмисників залишається соціальна інженерія — комплекс методів, які експлуатують довіру, неуважність або нестачу знань користувача з метою отримання несанкціонованого доступу до інформаційних ресурсів або поширення шкідливого програмного забезпечення.

Особливу актуальність ця тема набуває в умовах зростання цифровізації всіх сфер життя — від побутових онлайн-сервісів до державного управління. У більшості випадків атаки на інформаційні системи починаються саме з маніпуляцій свідомістю людини, а не з технічного зламу захищених серверів. Зловмисники все частіше уникають складних технічних рішень, надаючи перевагу психологічним прийомам, які дозволяють обійти захист без застосування спеціалізованих інструментів.

Методи соціальної інженерії активно використовуються для поширення шкідливого програмного забезпечення: троянів, кейлогерів, програм-вимагачів (ransomware) тощо. Шкідливе програмне забезпечення, у свою чергу, може використовуватись як для фінансового зиску, так і в контексті кібершпигунства або диверсій. Це робить вивчення механізмів їхнього розповсюдження та протидії особливо значущим.

Складність полягає в тому, що класичні засоби кіберзахисту — антивіруси, фаєрволи, системи виявлення вторгнень — не завжди здатні розпізнати атаку, яка реалізується через людський фактор. Відтак, розуміння методів соціальної інженерії дозволяє не лише краще реагувати на існуючі загрози, а й створювати стратегії превентивного захисту.

Актуальність дослідження обумовлена також низьким рівнем обізнаності широкого кола користувачів з питаннями кібербезпеки. Часто навіть освічені фахівці стають жертвами атак соціальних інженерів через брак критичності в

оцінці інформації, що надходить ззовні. Це свідчить про необхідність системного вивчення й поширення знань про ці методи.

Таким чином, дослідження методів соціальної інженерії, зокрема тих, що спрямовані на поширення шкідливого програмного забезпечення, є надзвичайно актуальним як з точки зору теорії інформаційної безпеки, так і для розробки практичних рекомендацій щодо зниження ризиків у цифровому середовищі.

Об'єктом дослідження є процес протидіїметодам соціальної інженерії орієнтованим на поширення шкідливого програмного забезпечення.

Предметом дослідження є методи та засоби протидії поширенню шкідливого програмного забезпечення методами соціальної інженерії.

Метою дослідження є розробка механізму протидії поширенню шкідливого програмного забезпечення методами соціальної інженерії для підвищення рівня кіберзахисту.

Для досягнення поставленої мети необхідно вирішити наступні завдання:

1. Проаналізувати поняття та класифікацію соціальної інженерії в контексті кібербезпеки.
2. Дослідити шкідливе програмне забезпечення: цілі, види, механізми дії та розповсюдження.
3. Дослідити методи та засоби соціальної інженерії, орієнтовані на поширення шкідливого програмного забезпечення
4. Дослідити основні вектори розповсюдження шкідливого програмного забезпечення з використанням соціальної інженерії
5. Описати типові сценарії атак і проаналізувати їх ефективність.
6. Розробити рекомендації для користувачів та організацій щодо зниження ризиків зараження шкідливим програмним забезпеченням через соціально-інженерні впливи.

РОЗДІЛ 1

ТЕОРЕТИЧНІ ОСНОВИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ ТА ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

1.1 Визначення поняття соціальної інженерії та її місце в кібербезпеці

Соціальна інженерія являє собою комплекс психологічних та соціальних методів, технік і стратегій, які використовуються для маніпулювання людьми з метою отримання конфіденційної інформації або доступу до захищених систем. На відміну від суто технічних методів зламу, соціальна інженерія зосереджується на експлуатації людського фактора — психологічних особливостей, довірливості, страхів, бажань та інших емоційних реакцій людей. За визначенням експерта з кібербезпеки Кевіна Мітніка, соціальна інженерія — це "використання впливу і переконання для обману людей з метою отримання інформації або спонукання їх до дій, які можуть призвести до розкриття інформації або порушення безпеки" [1].

У сучасному контексті кібербезпеки соціальна інженерія посідає особливе місце, оскільки технології безпеки постійно вдосконалюються, роблячи технічні атаки більш складними та ресурсозатратними. Натомість людський фактор залишається найслабшою ланкою в системі захисту інформації. Дослідники з Стенфордського університету визначають соціальну інженерію як "науку та мистецтво психологічного маніпулювання, що має на меті отримання конфіденційної інформації або виконання певних дій цільовою особою без її усвідомлення про можливі наслідки".

Історично концепція соціальної інженерії виникла задовго до появи комп'ютерів та інтернету, проте в контексті кібербезпеки вона набула нового значення з розвитком інформаційних технологій. Перші задокументовані випадки використання методів соціальної інженерії для отримання

несанкціонованого доступу до телефонних систем з'явились у 1960-70-х роках [2].

Національний інститут стандартів і технологій США NIST пропонує більш формальне визначення: "Соціальна інженерія — це акт маніпулювання людьми з метою порушення процедур безпеки, зазвичай шляхом отримання особистої інформації, конфіденційних даних або доступу до комп'ютерних систем". Необхідно відзначити, що соціальна інженерія спирається на фундаментальні принципи психології, включаючи когнітивні упередження, автоматизм поведінки та соціальні норми [3].

У контексті кібербезпеки соціальна інженерія виконує значення своєрідного мосту між людським та технічним світами. Вона дозволяє перетворити психологічну вразливість на технічний доступ до систем. Соціальна інженерія часто характеризується як "хакінг людського розуму" або "психологічний злам", підкреслюючи її фундаментальну відмінність від суто технічних методів атак (рис. 1.1).

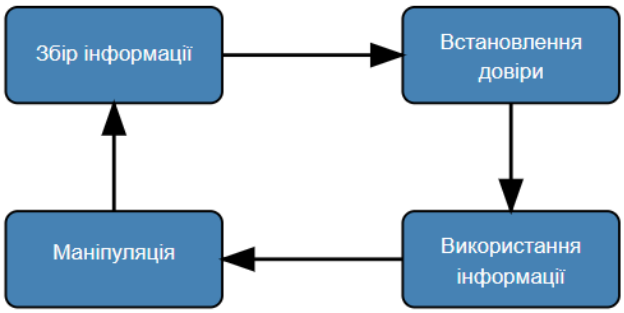

Рисунок 1.1. Типова модель соціальної інженерії.

У структурі сучасної кібербезпеки соціальна інженерія займає особливе місце, оскільки вона перетинає межі між технічним та нетехнічним елементами захисту інформації. Згідно з дослідженнями компанії Verizon, понад 30% усіх підтверджених випадків витоку даних включають елементи соціальної інженерії, а 90% кібератак починаються з фішингових листів — класичного прикладу атаки з використанням соціальної інженерії [4].

Український дослідник у галузі інформаційної безпеки Володимир Бурячок пропонує наступне визначення: "Соціальна інженерія — це сукупність методів управління діями людини без використання технічних засобів, що базується на використанні слабкостей людського фактора і є вельми ефективною у процесі розкриття інформації з обмеженим доступом" [5].

З точки зору таксономії кіберзагроз, соціальна інженерія може розглядатися як окрема категорія або як компонент більш складних багатоетапних атак. У багатьох випадках соціальна інженерія використовується як первинний вектор атаки для подальшого технічного проникнення в систему. Наприклад, зловмисник може використати фішинг для отримання облікових даних користувача, а потім використати ці дані для запуску технічної атаки на корпоративну мережу (рис. 1.2, табл. 1.1) [6].

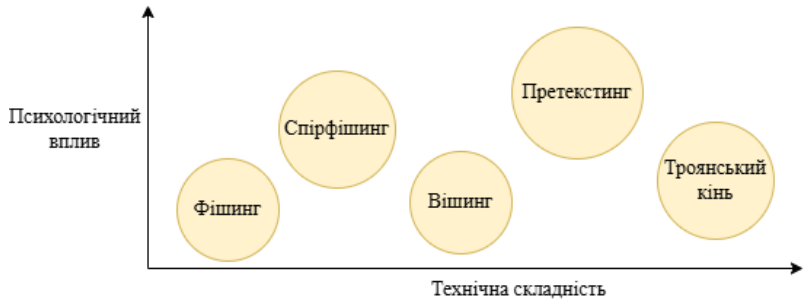

Рисунок. 1.2. Вектори атак соціальної інженерії.

Таблиця 1.1

Основні методи соціальної інженерії та їх характеристики

Метод	**Опис**	**Психологічний принцип**	**Приклад застосування**	**Рівень складності**
Фішинг	Масова розсилка підроблених електронних листів з метою виманювання конфіденційних даних	Авторитет, терміновість	Лист від "банку" з проханням підтвердити дані картки	Низький
Цільовий фішинг (спірфішинг)	Персоналізована атака на конкретну особу чи організацію	Авторитет, персоналізація	Лист від "керівника" з запитом на терміновий переказ	Середній

Продовження таблиці 1.1

Вішинг	Голосовий фішинг через телефонні дзвінки	Авторитет, соціальний доказ	Дзвінок від "служби підтримки" з проханням повідомити пароль	Середній
Претекстинг	Створення вигаданого сценарію для отримання інформації	Послідовність, взаємність	Імітація нового співробітника IT-відділу	Високий
Квіпрокво	Пропозиція допомоги або послуги в обмін на інформацію	Взаємність, послідовність	Фальшива технічна підтримка, яка просить надати доступ	Середній
Багінг	Підглядання за введенням конфіденційних даних	Використання неуважності	Спостереження за введенням PIN-коду в банкоматі	Низький
Тейлгейтинг	Несанкціонований фізичний доступ слідом за авторизованою особою	Соціальна нормативність	Проникнення в захищену зону слідом за співробітником	Середній
Троянський кінь	Маскування шкідливого програмного забезпечення під корисне	Цікавість, жадібність	Безкоштовне програмне забезпечення з прихованими шкідливими функціями	Високий
Вивідування інформації	Поступове отримання частин інформації через дружнє спілкування	Симпатія, соціальний доказ	Розмови в соціальних мережах для отримання особистих даних	Високий
Атаки через соціальні мережі	Використання відкритої інформації з профілів для підготовки таргетованих атак	Довіра до платформи	Створення фейкового профілю колеги або друга	Середній

У сучасній практиці забезпечення кібербезпеки особливого значення набуває концепція "людиноцентричної безпеки" (human-centric security), яка розглядає людину не лише як потенційну вразливість, але й як активний елемент системи захисту. Такий підхід визнає, що ефективна протидія соціальній інженерії неможлива без активної участі самих користувачів інформаційних систем [7].

Розвиток технологій штучного інтелекту та автоматизації також впливає на еволюцію методів соціальної інженерії. Наприклад, використання технологій глибинного навчання (deep learning) дозволяє створювати вкрай переконливі підробки голосу та відео (deepfakes), які можуть бути використані для більш ефективних таргетованих атак соціальної інженерії.

Адаптивність методів соціальної інженерії забезпечує їхню ефективність навіть за умов зростання обізнаності користувачів. Зловмисники постійно вдосконалюють підходи до обходу захисту, використовуючи, зокрема, феномен цифрової втоми — зниження пильності через інформаційне перевантаження [8].

Психологічна база соціальної інженерії включає фундаментальні принципи впливу. Серед них: принцип взаємності, принцип соціального підтвердження, принцип авторитету, принцип дефіциту, принцип послідовності та принцип симпатії. Кожен з цих принципів може бути використаний зловмисниками для маніпулювання жертвами (рис. 1.3).

Рисунок 1.3. Психологічні важелі соціальної інженерії.

1.2 Аналіз сучасного стану розповсюдження шкідливого програмного забезпечення

Сучасний кіберпростір характеризується безпрецедентним розповсюдженням шкідливого програмного забезпечення (malware), що становить одну з найбільших загроз для користувачів, організацій та критичної інфраструктури. За даними AV-TEST, щодня реєструється понад 450 000 нових зразків шкідливого програмного забезпечення, що демонструє колосальний масштаб проблеми. Проблема загострилася під час пандемії COVID-19, коли масовий перехід на віддалену роботу відкрив нові вектори для поширення шкідливого програмного забезпечення, що спричинило зростання успішних кібератак на 600% порівняно з допандемічним періодом(табл. 1.2.) [9].

Таблиця 1.2

Класифікація зловмисного програмного забезпечення

Категорія шкідливого програмного забезпечення	**Визначальні особливості**	**Принцип функціонування**	**Розповсю-дженість (%)**
Комп'ютерні віруси	Самореплікаційне програмне забезпечення з інтеграцією у файли-носії	Інфікування файлових об'єктів, програмних компонентів, системних областей	15%
Мережеві черв'яки	Самодостатні програми з автономним поширенням	Використання вразливостей мережевих протоколів, електронної кореспонденції	10%
Троянські програми	Маскування під легітимне програмне забезпечення	Створення прихованих каналів доступу, ексфільтрація даних	23%
Програми-вимагачі	Криптографічний захват даних з метою отримання викупу	Алгоритмічне шифрування інформаційних ресурсів, блокування функціоналу	27%

Продовження таблиці 1.2

Програми-шпигуни	Неавторизований збір користувацької активності	Відстеження дій користувача, перехоплення введених даних	12%
Руткіти	Технології приховування в системі	Модифікація системних компонентів, маскування процесів	4%
Завантажувальні кіти	Компрометація початкових етапів завантаження	Перехоплення процесу ініціалізації до запуску системи	2%
Рекламне програмне забезпечення	Нав'язування рекламного контенту	Перенаправлення пошукових запитів, модифікація налаштувань браузера	7%
Майнери криптовалют	Неавторизоване використання обчислювальних ресурсів	Активація прихованих процесів майнінгу, споживання системних ресурсів	4%

Програми-вимагачі (ransomware) залишаються однією з найпоширеніших форм шкідливого програмного забезпечення, що шифрує дані користувача та вимагає викуп за їх відновлення. За даними Cybersecurity Ventures, у 2024 році глобальні збитки від таких атак перевищили 24 млрд доларів США, що на 40% більше, ніж у 2023 році. Особливо небезпечними є атаки на критичну інфраструктуру та медичні установи, які можуть мати не лише фінансові, а й загрозливі для життя наслідки. (рис. 1.4) [10].

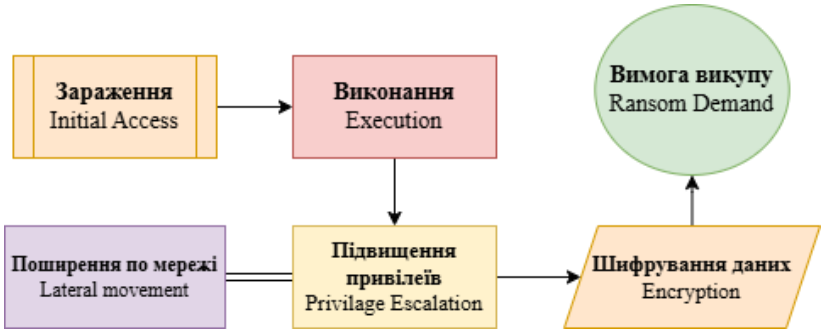

Рисунок 1.4. Життєвий цикл атаки програм-вимагачів.

Розробники зловмисного програмного забезпечення мають різні мотиви. Головними стимулами слугують матеріальне збагачення, заволодіння конфіденційними даними, отримання неавторизованого доступу до захищених мереж, а також дестабілізація роботи інформаційних систем. Значна частина шкідливого програмного забезпечення використовується для створення мереж компрометованих пристроїв, що стають платформою для подальших атак (табл. 1.3) [11].

Таблиця 1.3

Стратегічні наміри кіберзлочинців

Стратегічна мета	**Характеристика мети**	**Частка від загальної кількості випадків (2024)**
Економічний зиск	Викрадення фінансових реквізитів, криптовалютний майнінг, програми-вимагачі	71%
Заволодіння інформацією	Несанкціонований збір особистих даних, промислових секретів, інтелектуальної власності	63%
Кіберрозвідка	Прихований моніторинг активності користувачів та організацій	44%
Дестабілізація систем	Руйнівні дії для підриву функціональності інформаційних систем	36%
Формування зомбі-мереж	Об'єднання інфікованих комп'ютерів для проведення розподілених атак	33%
Геополітичний вплив	Атаки на стратегічні об'єкти, урядові структури, маніпулювання інформацією	25%

Методи поширення шкідливого програмного забезпечення суттєво еволюціонували. Зловмисники застосовують складні стратегії: водопійні атаки, компрометацію на етапі розробки (supply chain), соціальну інженерію та "drive-by download", коли програмне забезпечення завантажується при відвідуванні зараженого сайту. За даними Google Security Team, щоденно блокується доступ до близько 10 000 таких ресурсів [12].

Окрему категорію становить мобільне шкідливе програмне забезпечення, поширення якого зростає разом із кількістю смартфонів. За даними Kaspersky Lab, у 2023 році виявлено понад 5,6 млн зразків такого програмного забезпечення, 98% з яких були націлені на Android. Особливо активно поширюються банківські трояни, що перехоплюють SMS-коди, та шпигунські програми з доступом до персональних даних..

Розповсюдження шкідливого програмного забезпечення має суттєвий економічний вплив на організації та світову економіку. За даними Всесвітнього економічного форуму, у 2023 році збитки від кібератак, переважно пов’язаних зі шкідливим програмним забезпеченням, склали близько 8 трильйонів доларів США. Середня вартість інциденту для організації становить близько 4,35 млн доларів, враховуючи витрати на відновлення, простої та репутаційні втрати [13].

У відповідь на зростаючу загрозу шкідливого програмного забезпечення розвиваються технології захисту. Сучасні системи виявлення та попередження вторгнень поєднують сигнатурний аналіз, евристику та машинне навчання для виявлення шкідливої активності. Особливо ефективні поведінкові системи, що виявляють аномалії навіть нових варіантів шкідливого програмного забезпечення. За даними Gartner, витрати на кібербезпеку зростають на 15% щорічно і досягають 188,9 млрд доларів у 2024 році.

Аналіз поширення шкідливого програмного забезпечення неможливий без врахування соціального контексту. Пандемія COVID-19, геополітичні конфлікти та економічна нестабільність сприяють активізації кіберзлочинних угруповань. Цифровізація, зростання кількості підключених пристроїв, включно з Інтернетом речей, та залежність критичної інфраструктури від інформаційних технологій збільшують масштаби загроз. За прогнозами Cybersecurity Ventures, у 2025 року збитки від кіберзлочинності досягнуть 10,5 трлн доларів США щорічно, що підкреслює необхідність комплексного підходу — від індивідуальної кібергігієни до міжнародного правового регулювання [14].

Сучасний стан розповсюдження шкідливого програмного забезпечення характеризується високою динамікою, професіоналізацією кіберзлочинного

середовища, інтеграцією передових технологій та адаптацією до соціально-економічних змін. Ефективна протидія цій загрозі вимагає комплексного підходу, що включає технологічні рішення, освітні програми, правові механізми та міжнародну співпрацю. Особливого значення набуває проактивний підхід до кібербезпеки, що базується на принципі "припущення компрометації" (assume breach) та фокусується не лише на запобіганні атакам, але й на мінімізації їх потенційного впливу та швидкому відновленні після інцидентів [15].

1.3 Взаємозв'язок соціальної інженерії та методів поширення шкідливого програмного забезпечення

Взаємозв'язок соціальної інженерії та методів поширення шкідливого програмного забезпечення є одним із найбільш значущих аспектів сучасної кібербезпеки. Соціальна інженерія виступає головним компонентом у процесі розповсюдження шкідливого програмного забезпечення, оскільки дозволяє подолати технічні бар'єри захисту через маніпулювання людським фактором. За даними звіту Verizon Data Breach Investigations Report, понад 85% успішних кібератак включають елементи соціальної інженерії на певному етапі. Фішингові атаки залишаються найпоширенішим прикладом синергії соціальної інженерії та розповсюдження шкідливого програмного забезпечення, з щоденною кількістю атак понад 1,5 мільйона згідно з даними Anti-Phishing Working Group (рис. 1.5) [16].

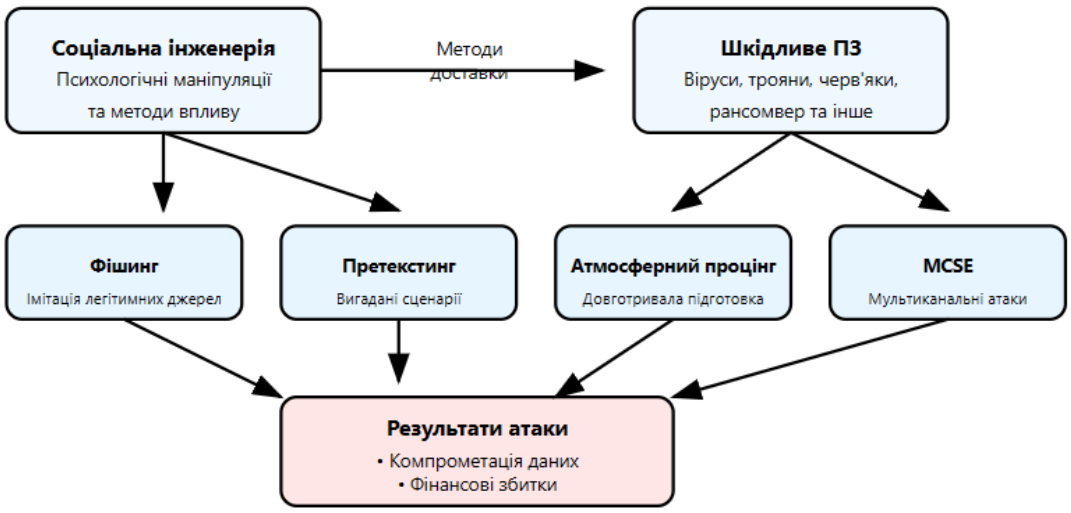

Рисунок 1.5. Загальна схема взаємозв'язку соціальної інженерії та поширення шкідливого програмного забезпечення.

Соціальна інженерія сприяє поширенню шкідливого програмного забезпечення, мотивуючи користувачів завантажувати його через маніпуляції психологічними факторами — цікавістю, страхом, жадібністю. За даними Symantec, близько 48% користувачів готові встановити програму з підозрілого джерела за умови безкоштовного функціоналу. Маркетингові техніки, такі як штучне створення відчуття терміновості або використання принципу соціального доказу, значно підвищують ефективність таких атак [17].

Розвиток технологій формує нові вектори атак на стику соціальної інженерії та поширення шкідливого програмного забезпечення. Застосування штучного інтелекту та машинного навчання підвищує ефективність фішингових повідомлень, які, за даними Microsoft Security Intelligence, мають на 40% більшу успішність. Діпфейки створюють реалістичні аудіо- та відеопідробки, ускладнюючи виявлення атак [18].

Соціальна інженерія виступає основним фактором у формуванні "ланцюжків інфікування" – багатоетапних процесів поширення шкідливого програмного забезпечення. Початковий етап часто включає використання психологічних маніпуляцій для отримання первинного доступу, після чого запускаються технічні компоненти атаки. Особливо небезпечним є поєднання

соціальної інженерії з методами поширення шкідливого програмного забезпечення через компрометацію ланцюгів постачання програмного забезпечення. У таких атаках зловмисники проникають у процес розробки або дистрибуції легітимного програмного забезпечення, впроваджуючи в нього шкідливий код.

У корпоративному середовищі соціальна інженерія у поєднанні зі шкідливим програмним забезпеченням проявляється через цільові атаки, зокрема злам корпоративної пошти (Business Email Compromise). Вони імітують комунікації керівництва для отримання конфіденційних даних або фінансових транзакцій.

Психологічні принципи, що лежать в основі соціальної інженерії, безпосередньо впливають на ефективність поширення шкідливого програмного забезпечення. Принципи авторитету, дефіциту, соціального підтвердження, взаємності та інші можуть бути використані для маніпулювання користувачами з метою встановлення шкідливого програмного забезпечення (рис.1.6) [19].

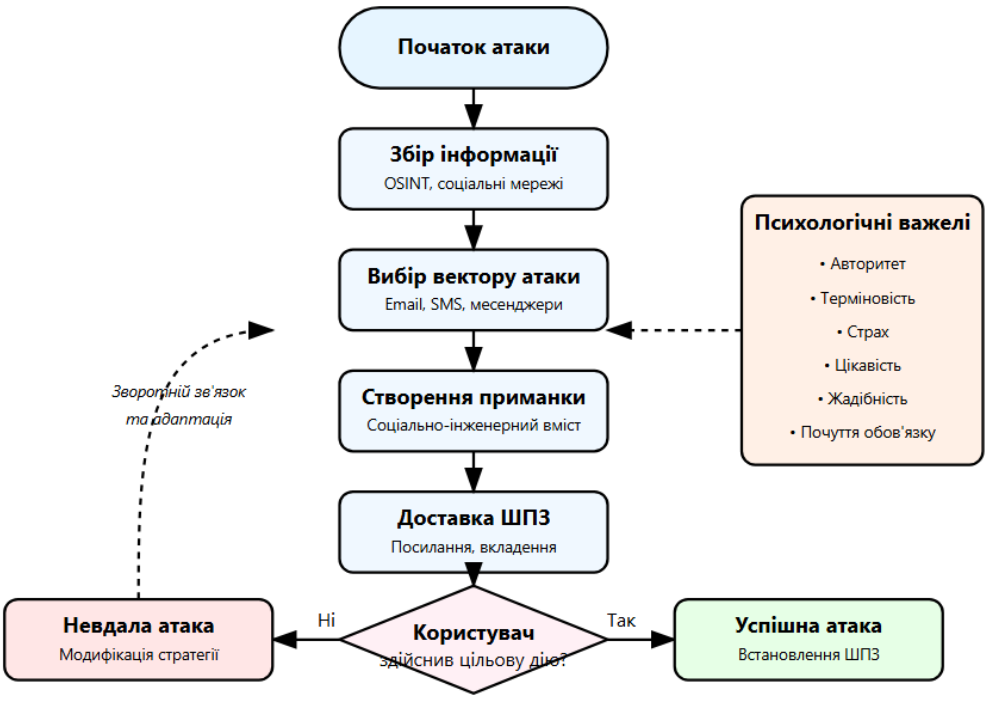

Рисунок 1.6. Алгоритм атаки з використанням соціальної інженерії для поширення шкідливого програмного забезпечення.

Протидія поєднанню соціальної інженерії та методів поширення шкідливого програмного забезпечення вимагає комплексного підходу, що охоплює технічні, освітні та організаційні заходи. На технічному рівні це включає впровадження багатофакторної автентифікації, систем фільтрації електронної пошти та інших механізмів захисту. Однак ключовим компонентом є регулярне навчання та підвищення обізнаності користувачів (рис.1.7).

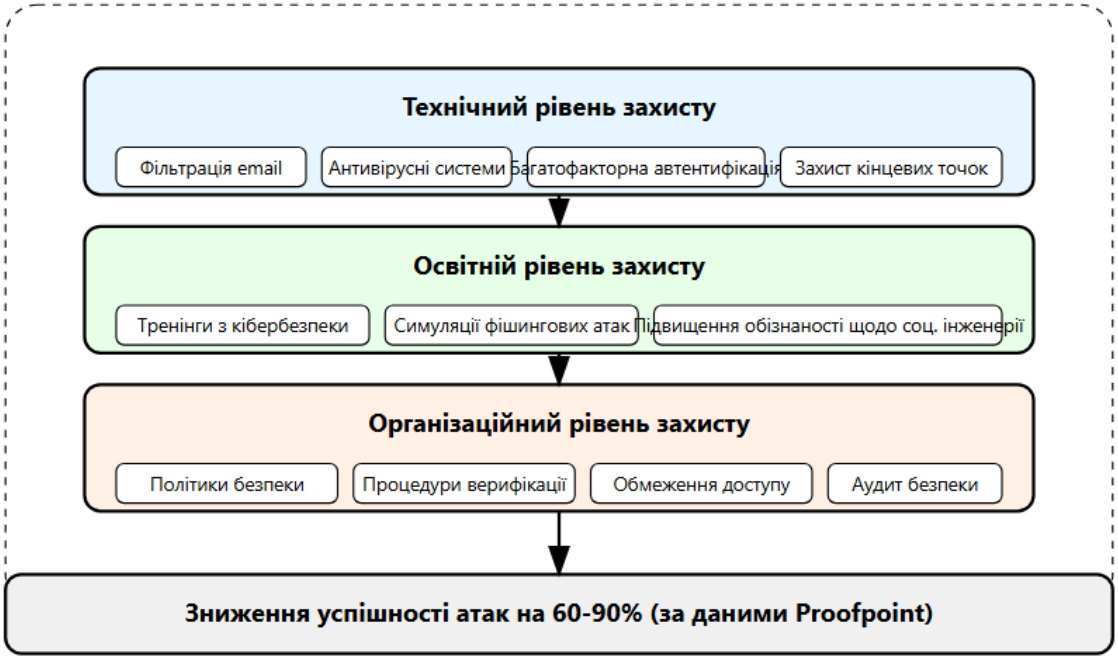

Рисунок 1.7. Комплексна модель захисту від соціально-інженерних атак.

Поява месенджер-орієнтованих методів соціальної інженерії сформувала новий вектор загроз для поширення шкідливого програмного забезпечення(табл. 1.4). На відміну від традиційних фішингових листів, атаки через месенджери (зокрема WhatsApp, Telegram та Viber) характеризуються вищим рівнем довіри користувачів та обмеженими можливостями для технічної фільтрації загроз. За даними компанії Check Point, у 2024 році кількість атак через месенджери зросла на 117%, причому більшість із них використовували соціально-інженерні сценарії для спонукання до переходу за шкідливими посиланнями або встановлення компрометованих додатків. Особливу небезпеку становлять так звані "ланцюгові повідомлення" (chain messages), де користувачів просять

поширити певну інформацію серед своїх контактів, тим самим збільшуючи радіус потенційного зараження.

Таблиця 1.4

Сучасні методи соціальної інженерії для поширення шкідливого програмного забезпечення

Метод	**Опис**	**Ефективність**	**Цільова аудиторія**	**Приклади застосування**
Фішинг	Імітація легітимних повідомлень від довірених джерел з метою отримання конфіденційних даних	30-45% для загальних кампаній, до 70% для таргетованих атак	Всі користувачі, особливо необізнані з питаннями кібербезпеки	Фальшиві повідомлення від банків, платіжних систем, соціальних мереж
Цільовий фішинг (Spear Phishing)	Персоналізовані фішингові атаки на конкретних осіб з використанням попередньо зібраної інформації	65-80%	Керівники організацій, працівники з високим рівнем доступу	Персоналізовані імейли з посиланнями на корпоративні документи
Атаки через месенджери	Розповсюдження шкідливих посилань або файлів через платформи миттєвого обміну повідомленнями	55-65%	Активні користувачі мобільних пристроїв	Шкідливі посилання в WhatsApp, Telegram, Viber
Етноцентричні методи	Адаптація атак до культурних, історичних та соціальних особливостей цільової аудиторії	На 76% вища успішність порівняно зі стандартними атаками	Національні та етнічні групи	Фішингові кампанії, що експлуатують тематику війни, гуманітарної допомоги

Продовження таблиці 1.4

Мультиканальна соціальна інженерія	Скоординоване використання різних комунікаційних каналів	До 87% навіть серед технічно обізнаних користувачів	Широкий спектр користувачів, включаючи технічно обізнаних	Комбінація електронної пошти, SMS, дзвінків та фейкових веб-сайтів
Гейміфікація	Створення інтерактивних сценаріїв з елементами гри змагання	74% серед користувачів 15-25 років	Молодша аудиторія	"Тести", "вікторини" з можливістю виграти призи
Злам корпоративної пошти (Business Email Compromise)	Імітація комунікацій від керівництва організації	Середній збиток - $130,000 на успішну атаку	Співробітники з доступом до фінансових систем	Фальшиві запити на переказ коштів від керівництва

Методи соціальної інженерії для поширення шкідливого програмного забезпечення все більше інтегруються з легітимними маркетинговими та психологічними техніками для підвищення ефективності. Зокрема, принцип FOMO (Fear Of Missing Out – страх пропустити щось значуще) активно використовується для створення відчуття терміновості та спонукання до негайних дій, таких як завантаження "обмеженої пропозиції" або "ексклюзивного контенту". Дослідження Стенфордського університету показало, що повідомлення, які апелюють до цього прнципу, збільшують вірогідність здійснення ризикованих дій користувачем на 43% [20].

Еволюція соціальної інженерії для поширення шкідливого програмного забезпеченнявключає впровадження методів нейролінгвістичного програмування та емоційного маніпулювання. Зловмисники адаптують психолінгвістичні патерни для різних демографічних груп, створюючи комунікації, що резонують з конкретною цільовою аудиторією.

Розширення використання корпоративних месенджерів та систем командної комунікації (Microsoft Teams, Discord) створило нові вектори для поєднання соціальної інженерії та розповсюдження шкідливого програмного забезпечення. Атаки через корпоративні комунікаційні платформи характеризуються високим рівнем контекстуалізації та надзвичайною переконливістю, оскільки зловмисники можуть використовувати внутрішні організаційні терміни, посилатися на поточні проєкти або імітувати стиль спілкування конкретних співробітників. За даними дослідження компанії Proofpoint, успішність соціально-інженерних атак через корпоративні месенджери на 63% вища порівняно з електронною поштою. Особливо небезпечними є атаки, що використовують компрометацію облікових записів (account takeover) для здійснення "lateral movement" – горизонтального поширення шкідливого програмного забезпеченнявсередині організації, коли зараження одного співробітника використовується для атак на його колег.

Значну загрозу становить інтеграція методів соціальної інженерії з технологіями цифрової мімікрії – здатності шкідливого програмного забезпечення адаптуватися до контексту та імітувати легітимні програми або сервіси. Сучасні трояни та інші типи шкідливого програмного забезпеченнячасто використовують динамічну адаптацію інтерфейсу користувача, змінюючи свій зовнішній вигляд залежно від географічного розташування, мови операційної системи або попередньої історії використання пристрою. За даними лабораторії кібербезпеки CERT-UA, такі адаптивні методи підвищують успішність інсталяції шкідливого програмного забезпечення на 58%. Особливо небезпечними є випадки, коли шкідливе програмне забезпечення імітує інтерфейси локальних банківських додатків або державних сервісів, що суттєво підвищує рівень довіри користувачів.

Етноцентричні методи соціальної інженерії для поширення шкідливого програмного забезпеченнянабувають все більшого поширення, особливо в умовах геополітичних конфліктів та інформаційних воєн. Зловмисники адаптують свої атаки до культурних, історичних та соціальних особливостей

цільової аудиторії, створюючи сценарії, що резонують з національними наративами або травматичним досвідом. Для України особливо актуальними є кібератаки, що експлуатують тематику війни, гуманітарної допомоги, мобілізації або переселення.

Мультиканальна соціальна інженерія (Multi-Channel Social Engineering, MCSE) стає стандартом для просунутих кампаній з розповсюдження шкідливого програмного забезпечення. Цей підхід передбачає скоординоване використання різних комунікаційних каналів для підвищення достовірності атаки та подолання скептицизму цільової аудиторії. Типовий сценарій може включати первинний контакт через електронну пошту, підтвердження через SMS або дзвінок від "служби підтримки", а також наявність фальшивого веб-сайту з правдоподібними відгуками в соціальних мережах. За даними компанії FireEye, успішність таких багатоетапних атак досягає 87% навіть серед технічно обізнаних користувачів [21].

Фактор гейміфікації все частіше використовується для поєднання соціальної інженерії та методів поширення шкідливого програмного забезпечення, особливо при таргетуванні молодшої аудиторії. Зловмисники створюють інтерактивні сценарії, де користувачам пропонується пройти "тест", "розгадати загадку" або взяти участь у "вікторині" з можливістю виграти віртуальні або реальні призи. В процесі такої взаємодії користувачі добровільно надають персональні дані або завантажують шкідливе програмне забезпечення під виглядом "необхідного для участі" додатка. Дослідження компанії Trend Micro виявило зростання кількості таких атак на 82% протягом останнього року, при цьому їх успішність серед користувачів віком 15-25 років досягає 74%. Особливо ефективними виявляються сценарії, що інтегруються з популярними трендами або челенджами в соціальних мережах [22].

Висновки за розділом 1

Соціальна інженерія, як комплекс психологічних і соціальних методів маніпулювання, відіграє ключову роль у сучасній кібербезпеці, використовуючи людський фактор як найслабшу ланку в системах захисту інформації. Її методи, що ґрунтуються на експлуатації психологічних особливостей, довірливості та когнітивних упереджень, дозволяють зловмисникам обходити навіть найсучасніші технічні засоби захисту. Визначення соціальної інженерії, запропоновані такими експертами, як Кевін Мітнік та дослідники NIST, підкреслюють її унікальну природу, що поєднує психологію, соціологію та технології, роблячи її ефективним інструментом для отримання несанкціонованого доступу до конфіденційної інформації.

Шкідливе програмне забезпечення становить одну з найбільших загроз сучасного кіберпростору, характеризуючись безпрецедентним масштабом поширення та різноманітністю форм, таких як програми-вимагачі, банківські трояни та шпигунські програми. Динаміка розвитку шкідливого програмного забезпечення, підкріплена інтеграцією передових технологій, таких як штучний інтелект, свідчить про високий рівень професіоналізації кіберзлочинного середовища. Зростання економічних збитків від кібератак, що сягають трильйонів доларів щорічно, підкреслює критичну необхідність розробки ефективних стратегій протидії цій загрозі.

Взаємозв’язок соціальної інженерії та методів поширення шкідливого програмного забезпечення є ключовим фактором успіху більшості сучасних кібератак. Соціальна інженерія виступає первинним вектором, що забезпечує доставку шкідливого програмного забезпечення через маніпулювання користувачами, зокрема за допомогою фішингових атак, які залишаються найпоширенішим методом. Використання психологічних принципів, таких як авторитет, взаємність чи страх пропустити щось важливе, значно підвищує ефективність цих атак, роблячи їх переконливими навіть для технічно обізнаних користувачів.

Сучасні методи соціальної інженерії ускладнюються завдяки інтеграції зі штучним інтелектом, дипфейками та нейролінгвістичним програмуванням, що забезпечує створення гіперперсоналізованих атак, адаптованих до соціокультурних особливостей жертв. Використання месенджерів, корпоративних платформ і гейміфікованих сценаріїв свідчить про високий рівень адаптивності зловмисників до цифрових змін, що ускладнює виявлення загроз.

Ефективна протидія поєднанню соціальної інженерії та шкідливого програмного забезпечення вимагає комплексного підходу, що охоплює технічні, освітні та організаційні заходи. Технічні рішення, такі як багатофакторна автентифікація та системи поведінкового аналізу, є важливими, але їхня ефективність обмежена без належного рівня обізнаності користувачів. Регулярне навчання, підвищення кібергігієни та формування культури критичного мислення є необхідними для зниження вразливості до маніпулятивних технік, що використовуються зловмисниками.

Соціально-економічні та геополітичні фактори — зокрема пандемія, цифровізація та інформаційні війни — створюють сприятливі умови для ескалації кіберзагроз. Етноцентричні атаки та мультиканальні стратегії з високим рівнем контекстуалізації підсилюють переконливість зловмисного впливу. Це потребує від фахівців з кібербезпеки не лише технічних навичок, а й глибокого розуміння психологічних, соціальних і культурних чинників, що формують користувацьку поведінку.

Еволюція соціальної інженерії та шкідливого програмного забезпечення вимагає переходу до людиноцентричної моделі кібербезпеки, де користувачі розглядаються як активний елемент захисту. Це зумовлює потребу в проактивних підходах, які враховують динаміку загроз, використання штучного інтелекту та психолінгвістичних технік, і базуються на принципі припущення компрометації. У цьому контексті важливо формувати глобальну культуру кібербезпеки та посилювати міжнародну співпрацю для забезпечення цифрової стійкості.

РОЗДІЛ 2

ДОСЛІДЖЕННЯ ОСНОВНИХ МЕТОДІВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ СПРЯМОВАНИХ НА ПОШИРЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

2.1 Методи та засоби соціальної інженерії, орієнтовані на поширення шкідливого програмного забезпечення

Соціальна інженерія становить потужний інструмент у арсеналі кіберзлочинців для поширення шкідливого програмного забезпечення, фокусуючись на експлуатації людського фактора замість технічних вразливостей. Розглянемо основні методи та засоби соціальної інженерії, що демонструють найвищу ефективність у контексті розповсюдження різних типів шкідливого програмного забезпечення [23].

Методи соціальної інженерії:

Фішинг — найпоширеніший метод, що включає наступні підвиди:

- Класичний фішинг (масові розсилки);
- Спеарфішинг (таргетовані персоналізовані атаки);
- Вішинг (голосовий фішинг через телефонні дзвінки);
- Смішинг (фішинг через SMS та месенджери);
- QR-фішинг (використання шкідливих QR-кодів).

Претекстинг (pretexting) — створення вигаданого сценарію для отримання інформації або спонукання до дій жертви (удавання співробітника техпідтримки, банківського працівника, державного службовця).

Приманка (baiting) — пропозиція чогось привабливого в обмін на дії або інформацію (безкоштовні завантаження, подарунки, акційні пропозиції).

Послуга за послугу (quid pro quo) — злочинець пропонує допомогу або послугу в обмін на інформацію або доступ (удавана технічна підтримка).

Водопійні атаки (watering hole) — компрометація веб-сайтів, які регулярно відвідує цільова аудиторія.

Технології глибинних підробок (deepfake) — створення переконливого фальсифікованого аудіо, відео та зображень для маніпуляції жертвами.

Таргетування на основі контексту — експлуатація актуальних подій, криз та інформаційних приводів для підвищення ефективності атак.

Засоби реалізації соціально-інженерних атак:

Електронна пошта — використання підроблених корпоративних шаблонів, додавання шкідливих вкладень, вбудовування зловмисних посилань.

Соціальні мережі та месенджери:

- Фальшиві профілі та групи;
- Шкідливі посилання в особистих повідомленнях;
- Підставні конкурси та акції;
- Компрометація облікових записів та розсилка з них;
- Шкідливі застосунки та розширення.

Телефонні дзвінки — використання технологій підміни номера, соціальних скриптів та психологічного тиску.

Фізичні носії — підкидання заражених USB-накопичувачів у публічних місцях компанії.

Технічні інструменти:

- Підроблені веб-сайти (клони легітимних ресурсів);
- URL-маскування (ідентичні домени);
- Генеративні системи штучного інтелекту для створення переконливого контенту;
- Автоматизовані системи розсилки та таргетування.

Розуміння методів соціальної інженерії (табл. 2.1), засобів та їх ефективності у поширенні шкідливого програмного забезпечення є критичним для розробки ефективного захисту. Особливо небезпечні гібридні атаки, що поєднують кілька методів соціальної інженерії з адаптацією до різних каналів комунікації та психологічних профілів жертв [24].

Таблиця 2.1

Найефективніші комбінації методів соціальної інженерії та типів шкідливого програмного забезпечення

Метод соціальної інженерії	**Тип шкідливого програмного забезпечення**	**Ефективність поширення**	**Ключові вектори доставки**
Спеарфішинг	RAT (Remote Access Trojan)	84%	Корпоративна електронна пошта, LinkedIn
Претекстинг (удавана техпідтримка)	Інфостілери, кейлогери	78%	Телефонні дзвінки, підроблені портали підтримки
Deepfake-маніпуляції	Банківські трояни, вимагачі	82%	WhatsApp, Telegram, відеоконференції
Приманка через соціальні мережі	Рекламне програмне забезпечення, криптомайнери	76%	Facebook, Instagram, TikTok
Послуга за послугу (технічна допомога)	Бекдори, шпигунське програмне забезпечення	71%	Удалений доступ, підроблені інструменти підтримки
Таргетування на основі актуальних подій	Мобільні трояни, фейкові застосунки	79%	Соціальні мережі, e-mail, SMS
Фішинг через месенджери	Стілери криптогаманців, стілери паролів	75%	Telegram, WhatsApp, Facebook Messenger
QR-фішинг	Мобільне шкідливе програмне забезпечення, банківські трояни	68%	Публічні місця, підроблені рекламні матеріали

Соціальна інженерія — ефективний інструмент кіберзлочинців, що експлуатує людський фактор замість технічних вразливостей. Психологічні маніпуляції, емоційний вплив і маскування під довірені джерела дозволяють обходити захист, використовуючи когнітивні упередження та низький рівень обізнаності користувачів для поширення шкідливого програмного забезпечення.

Основою соціальної інженерії є експлуатація психологічних механізмів, таких як страх, цікавість, довіра, жадібність і альтруїзм, які стимулюють цільових осіб до ризикованої поведінки. Ці маніпулятивні техніки інтегруються з технічними засобами, формуючи складні гібридні атаки, що поєднують психологічний вплив із цифровими методами доставки шкідливого програмного забезпечення (табл. 2.2) [19].

Таблиця 2.2

Фундаментальні принципи соціальної інженерії в кіберпросторі

Психологічний принцип	**Механізм експлуатації**	**Ефективність маніпуляції**	**Типові сценарії застосування**
Авторитет	Маскування під керівництво, експертів, державні органи	76%	Фальшиві директиви, запити від "керівництва"
Дефіцит часу	Створення ілюзії терміновості, обмеженості пропозиції	69%	"Останній шанс", "термінова дія потрібна"
Соціальне підтвердження	Апеляція до масовості, "всі так роблять"	58%	"Приєднайтесь до тисяч користувачів..."
Взаємність	Спонукання до відповідних дій за отриману "послугу"	65%	Безкоштовні пропозиції з прихованими умовами
Симпатія	Формування позитивного образу, встановлення емоційного зв'язку	71%	Романтичні шахрайства, удавана дружба
Страх та занепокоєння	Використання почуття тривоги, загрози	82%	Попередження про компрометацію даних, штрафи
Цікавість	Експлуатація природного бажання дізнатися таємниці	74%	"Подивіться, що про вас пишуть", сенсаційний контент

Фішинг залишається одним із найпоширеніших і найефективніших методів соціальної інженерії, що постійно адаптується до зростання обізнаності

користувачів і вдосконалення захисту. Сучасні атаки вирізняються високою персоналізацією, застосуванням штучного інтелекту для створення переконливого контенту та складними технічними засобами обходу фільтрів. Інтеграція з легітимними сервісами та використання психологічних профілів цільових аудиторій дозволяють зловмисникам формувати надзвичайно реалістичні сценарії, важко відрізнити від справжньої комунікації.

Сучасні соціально-інженерні атаки демонструють тенденцію до підвищеної спеціалізації, фокусуючись на конкретних галузях, організаціях або навіть окремих посадових особах. Зловмисники проводять ретельну підготовчу роботу, збираючи інформацію з відкритих джерел, соціальних мереж та корпоративних ресурсів для створення персоналізованих атак, що враховують специфіку діяльності, корпоративну культуру та індивідуальні характеристики цілей. Цей підхід, відомий як спеарфішинг (spear phishing), значно підвищує ймовірність успіху атаки та ускладнює її виявлення стандартними засобами захисту (табл. 2.3) [25].

Таблиця 2.3

Спеціалізація та таргетування в сучасних соціально-інженерних атаках

Цільовий сектор	**Домінуючі методи соціальної інженерії**	**Рівень персоналізації**	**Успішність проникнення**
Фінансові установи	Корпоративний фішинг, удавані аудити безпеки	Надвисокий	42%
Охорона здоров'я	Маскування під регуляторні органи, екстрені медичні ситуації	Високий	38%
Енергетичний сектор	Імітація внутрішніх технічних комунікацій, галузевих заходів	Високий	35%
Державний сектор	Підроблені урядові документи, національні ініціативи	Середній	27%

Продовження таблиці 2.3

Виробництво	Фальшиві запити постачальників, промислові стандарти	Середній	31%
Освіта	Студентські запити, наукові співпраці, грантові можливості	Низький	49%
Роздрібна торгівля	Підроблені програми лояльності, акційні пропозиції	Низький	44%
Телекомуніка ції	Технічні попередження, оновлення обладнання	Середній	29%

Сучасні кібератаки демонструють тенденцію до синергетичного поєднання методів соціальної інженерії з технічними експлойтами, створюючи багатовекторні комплексні загрози. Зловмисники використовують соціальну інженерію як первинний вектор проникнення, отримуючи доступ до системи через дії користувача, після чого застосовують технічні інструменти для закріплення, розширення присутності та реалізації кінцевої мети атаки. Така інтеграція значно підвищує ефективність атак, оскільки дозволяє обходити як технічні засоби захисту, так і заходи з підвищення обізнаності персоналу [26].

Соціальні мережі, месенджери та інші комунікаційні платформи стали головним вектором для реалізації соціально-інженерних атак та розповсюдження шкідливого програмного забезпечення. Висока довіра користувачів до контенту, отриманого від контактів, широкі можливості мультимедійної комунікації та масовий характер цих платформ створюють ідеальне середовище для різноманітних маніпуляцій. Зловмисники активно використовують фальшиві акаунти, групи підтримки, тематичні спільноти та особисті повідомлення для поширення шкідливих посилань, файлів та застосунків під виглядом цікавого контенту, корисних інструментів або головних сповіщень (табл. 2.4).

Таблиця 2.4

Використання соціальних платформ для розповсюдження шкідливого програмного забезпечення

Соціальна платформа	**Превалюючі техніки соціальної інженерії**	**Типи шкідливого програмного забезпечення**	**Зростання інцидентів (2024)**
Facebook/Instagram	Підроблені конкурси, фішингові групи, додатки	Інфостілери, троянські програми	+32%
LinkedIn	Фальшиві вакансії, професійні контакти, галузеві дослідження	Шпигунське ПЗ	+47%
Twitter	Вірусні виклики, трендові хештеги, скорочені URL	Бот-мережі, криптомайнери	+28%
TikTok	Челенджі з шкідливими посиланнями, підроблені фільтри	Мобільне шкідливе ПЗ, рекламне ПЗ	+53%
Telegram/WhatsApp	Фіктивні групи підтримки, підміна особистості	Банківські трояни, вимагачі	+41%
Discord	Ігрові модифікації, преміум-контент, спільноти	Стілери облікових даних, криптогаманців	+39%
Reddit	Підроблені пости підтримки, тематичні сабредіти	Інфостілери, троянські програми	+21%

Корпоративний сектор є пріоритетною мішенню соціоінженерних атак через фінансову вигоду та доступ до цінної інформації. Зловмисники використовують галузеві особливості, ієрархію та внутрішні комунікації. Найчастіше застосовуються Business Email Compromise, CEO Fraud і атаки на ланцюги постачання, спрямовані на фінансове шахрайство або доступ до інфраструктури [27].

Сучасні соціально-інженерні атаки активно адаптуються до актуального інформаційного порядку, використовуючи важливі суспільні події, кризи та глобальні тенденції для підвищення ефективності маніпуляцій. Пандемії, катастрофи, політичні та економічні кризи слугують основою для переконливих сценаріїв, що експлуатують емоційне сприйняття та потребу в актуальній інформації. Такий контекстуальний підхід значно збільшує ймовірність успіху атаки через зниження пильності користувачів (табл. 2.5).

Таблиця 2.5

Контекстуалізація атак на основі суспільних подій та тенденцій

Контекстуальна подія	**Сценарії соціально-інженерних атак**	**Психологічний тригер**	**Ефективність маніпуляції**
Пандемії та епідемії	Фальшиві медичні рекомендації, підроблені вакцинаційні сертифікати	Страх за здоров'я	84%
Природні катастрофи	Шахрайські збори пожертв, фейкові списки постраждалих	Співчуття, бажання допомогти	78%
Політичні вибори	Підроблені політичні матеріали, фальшиві дослідження	Політичні переконання	67%
Економічні кризи	Шахрайські інвестиційні можливості, фіктивні компенсації	Фінансова тривога	75%
Спортивні події	Фальшиві квитки, псевдо-ексклюзивний контент	Ентузіазм, азарт	63%
Технологічні релізи	Підроблені попередні версії, фіктивні бета-тестування	Технологічний інтерес	71%
Сезонні свята	Фальшиві акції, шахрайські подарункові карти	Святковий настрій, щедрість	69%

Технологічний розвиток у сфері генерації та маніпуляції мультимедійним контентом відкрив нові можливості для соціальної інженерії. Технології глибинних підробок (deepfake), синтезу голосу, генеративного штучного інтелекту та обробки зображень дозволяють створювати надзвичайно переконливий фальсифікований контент, який важко відрізнити від автентичного без спеціальних засобів. Зловмисники активно використовують ці технології для створення фальшивих відеозвернень, голосових повідомлень і фотографій, що значно підвищує ефективність соціально-інженерних атак та ускладнює їх виявлення [28].

Сучасні методи соціальної інженерії автоматизуються та масштабуються, дозволяючи зловмисникам одночасно атакувати тисячі цілей з мінімальними ресурсами. Використання штучного інтелекту, машинного навчання та аналізу великих даних дозволяє створювати системи для автоматичного профілювання жертв, генерації персоналізованого фішингового контенту, імітації людської поведінки та динамічного адаптування тактик. Це забезпечує масштабність атак при збереженні високої персоналізації, раніше притаманної лише ручним кампаніям.

Соціальна інженерія все частіше є складовою гібридних інформаційних операцій, що поєднують кібератаки з інформаційним впливом, пропагандою та маніпуляцією громадською думкою. Методи соціальної інженерії використовуються не лише для розповсюдження шкідливого програмного забезпечення, але й для формування інформаційного середовища, що посилює ефективність технічних атак. Інформаційний шум, дезінформація, підрив довіри до офіційних джерел і дискредитація експертів підвищують вразливість користувачів до традиційних методів соціальної інженерії.

Ефективна протидія соціально-інженерним атакам вимагає комплексного підходу, що поєднує технічні засоби захисту з підвищенням обізнаності користувачів та формуванням культури кібербезпеки. Сучасні методики протидії включають регулярні тренінги з розпізнавання фішингу, симуляції атак для практичного закріплення навичок, впровадження багатофакторної

автентифікації, розгортання спеціалізованих систем виявлення фішингу та встановлення чітких процедур верифікації чутливих запитів. Особливого значення набуває формування критичного мислення та здорової підозрілості щодо незвичних комунікацій, несподіваних запитів та емоційно заряджених повідомлень (табл. 2.6) [26].

Таблиця 2.6

Методики протидії сучасним технікам соціальної інженерії

Метод протидії	**Механізм захисту**	**Ефективність запобігання**	**Термін збереження ефекту**
Спеціалізовані тренінги	Підвищення обізнаності, розвиток навичок розпізнавання	68%	3-6 місяців
Симуляції фішингових атак	Практичне закріплення навичок, створення реалістичних сценаріїв	74%	4-8 місяців
Автоматизовані системи фільтрації	Технічна ідентифікація підозрілих повідомлень	82%	Постійно (потребує оновлення)
Багатофакторна автентифікація	Додатковий рівень захисту при доступі до ресурсів	91%	Постійно
Чіткі процедури верифікації	Формалізовані протоколи перевірки чутливих запитів	79%	Постійно (потребує підтримки)
Регулярні інформаційні кампанії	Підтримка обізнаності, інформування про нові загрози	56%	1-3 місяці
Інструменти аналізу URL та вкладень	Автоматична перевірка посилань та файлів	87%	Постійно (потребує оновлення)
Сегментація доступу	Обмеження потенційних наслідків успішної атаки	81%	Постійно

Дослідження демонструють значні відмінності в уразливості різних демографічних груп до методів соціальної інженерії, що зумовлені віковими, освітніми, професійними та культурними факторами. Розуміння цих відмінностей дозволяє розробляти таргетовані програми підвищення обізнаності та специфічні захисні заходи для найбільш вразливих категорій користувачів. Основними факторами, що впливають на уразливість, є рівень цифрової грамотності, досвід використання технологій, загальна обізнаність щодо кіберзагроз, схильність до ризикованої поведінки та культурні особливості сприйняття авторитетів і соціальних зв'язків.

Розвиток соціально-інженерних технік атаки та захисту піднімає складні правові та етичні питання щодо меж допустимого тестування, відповідальності за використання психологічних маніпуляцій та балансу між безпекою і приватністю. Правове регулювання соціальної інженерії залишається фрагментованим, з суттєвими відмінностями між юрисдикціями щодо класифікації цих дій, встановлення відповідальності та визначення допустимих меж тестування на проникнення з використанням соціально-інженерних технік. Особливо складними є питання транскордонних атак, де зловмисники та жертви знаходяться в різних юрисдикціях з різними правовими підходами до кіберзлочинності [29].

Аналіз сучасних тенденцій дозволяє прогнозувати подальший розвиток соціально-інженерних технік у напрямку глибшої інтеграції з технологіями штучного інтелекту, персоналізації атак на основі цифрових слідів користувачів та використання нових комунікаційних каналів. Особливої уваги заслуговує потенціал використання розширеної та віртуальної реальності для створення імерсивних фішингових сценаріїв, а також розвиток методів мультиканальних атак, що синхронізовано використовують різні вектори комунікації для підвищення довіри жертви.

Головним фактором стане здатність зловмисників адаптуватися до нових методів автентифікації та верифікації, включаючи біометричні системи та

поведінкову аналітику. Експерти прогнозують появу гібридних атак, що поєднують маніпулятивні техніки з автоматизованим аналізом даних для виявлення оптимальних векторів впливу на конкретну ціль. Окремою загрозою є потенційне використання генеративного штучного інтелекту для автоматичного створення переконливих наративів, персоналізованих під психологічний профіль жертви, що здатні викликати миттєву емоційну реакцію та спонукати до необачних дій (табл. 2.7).

Таблиця 2.7

Майбутні тенденції розвитку соціально-інженерних технік

Інноваційний напрямок	**Технологічна основа**	**Потенційний вплив**
Гіперперсоналізовані атаки	Інтегрований аналіз цифрового сліду, психометрія	Критичний
Мультисенсорний фішинг	Технології віртуальної реальності, імерсивні середовища	Високий
Синтетичні ідентичності	Генеративні алгоритми, deepfake технології	Критичний
Адаптивні конверсаційні боти	Прогресивні мовні моделі, аналіз емоцій	Високий
Нейролінгвістичні маніпуляції	Обробка природної мови, психолінгвістика	Середній
Колаборативні атаки	Розподілені системи, синхронізовані сценарії	Високий
Атаки на нові інтерфейси	Нейроінтерфейси, голосові асистенти, жестові технології	Середній

Незважаючи на технологічний розвиток засобів захисту, людський фактор залишається одночасно найбільшою вразливістю та найпотужнішим інструментом протидії соціально-інженерним атакам. Формування культури кібербезпеки, розвиток критичного мислення та підвищення ситуаційної обізнаності користувачів є фундаментальними елементами ефективної системи захисту. Особливого значення набуває розвиток емоційного інтелекту та психологічної стійкості до маніпулятивних технік, що дозволяє користувачам

розпізнавати спроби емоційного впливу та зберігати раціональність в умовах стресу, терміновості або дефіциту інформації.

Соціально-інженерні атаки на критичну інфраструктуру демонструють галузеві відмінності, адаптуючись до специфіки виробничих процесів, корпоративної культури та регуляторного середовища. В енергетиці домінують сценарії, пов’язані з аваріями, технічними збоями та перевірками; у фінансах — з аудитами, шахрайством і комплаєнсом; в охороні здоров’я — з медичними даними, страховими випадками та контролем якості. Це потребує індивідуалізованих підходів до підвищення обізнаності та захисту, що враховують унікальні ризики кожного сектора (табл. 2.8).

Таблиця 2.8

Галузеві особливості соціально-інженерних атак у критичній інфраструктурі

Сектор критичної інфраструктури	**Домінуючі сценарії атак**	**Специфічні вразливості**	**Потенційні наслідки успішної атаки**
Енергетика	Фальшиві аварійні сповіщення, підроблені технічні інструкції	Географічна розподіленість, застарілі системи	Порушення енергопостачання, аварії
Водопостачання	Підроблені результати аналізу якості, фіктивні перевірки	Обмежені ресурси безпеки, критичність для громад	Забруднення водних ресурсів, збої в постачанні
Транспорт	Підроблені навігаційні дані, фальшиві сповіщення про затримки	Висока залежність від точності даних, часові обмеження	Транспортний колапс, аварії
Охорона здоров'я	Фішинг медичних даних, підроблені медикаменти/обладнання	Пріоритет швидкості реагування, чутливість даних	Порушення надання медичних послуг, компрометація даних

Продовження таблиці 2.8

Фінансові установи	Підроблені авторизації транзакцій, фіктивні запити регуляторів	Висока цінність активів, складні системи доступу	Фінансові втрати, порушення довіри клієнтів
Телекомунікації	Фальшиві технічні оновлення, підроблені інструкції з конфігурації	Складність інфраструктури, широкий доступ	Збої у комунікаціях, компрометація даних
Ядерні об'єкти	Фіктивні аварійні протоколи, підроблені результати моніторингу	Високі стандарти безпеки, обмежений персонал	Радіаційні загрози, екологічні катастрофи

Особливо небезпечним вектором атак є комбінування методів соціальної інженерії з інсайдерськими загрозами, коли зловмисники навмисно впливають на співробітників організації з метою отримання несанкціонованого доступу або порушення встановлених політик безпеки. Такі загрози можуть реалізовуватись як через пряме вербування персоналу, так і шляхом прихованого психологічного впливу, що поступово призводить до втрати об’єктивності та сприяє виконанню дій, шкідливих для безпеки. Особливої уваги заслуговують техніки "довготривалого культивування" інсайдерів, коли зловмисники поступово, протягом тривалого періоду, встановлюють довірчі відносини з цільовим співробітником, поступово підводячи його до вчинення дій, що порушують безпеку організації.

Сучасні соціально-інженерні атаки все активніше використовують психолінгвістичні методи впливу, адаптуючи мовні конструкції, термінологію та стилістику комунікації для максимального психологічного впливу на цільову аудиторію. Зловмисники враховують культурні та соціальні особливості аудиторії, професійну лексику, емоційні тригери та когнітивні упередження для створення повідомлень, що викликають довіру та спонукають до необачних дій.

Особливого значення набувають техніки "штучного дефіциту", створення ілюзії терміновості, апеляція до авторитетів та використання мовних конструкцій, що активують автоматичні поведінкові патерни та знижують критичне мислення (табл. 2.9) [30].

Таблиця 2.9

Психолінгвістичні методи в сучасній соціальній інженерії

Психолінгвістична техніка	**Механізм впливу**	**Типові мовні маркери**	**Ефективність маніпуляції**
Ілюзія терміновості	Активація режиму "бий-біжи", блокування критичного мислення	"Терміново", "останній шанс", "до завтра"	78%
Штучний дефіцит	Використання страху втрати можливості	"Обмежена пропозиція", "лише для обраних", "закінчується"	74%
Апеляція до авторитету	Експлуатація соціальних ієрархій, довіри до експертів	"Директор доручив", "за рекомендацією", "експерти підтверджують"	72%
Набудова лінгвістичного резонансу	Імітація стилю спілкування жертви, віддзеркалення	Використання специфічних зворотів, темпу, структури речень цілі	81%
Насичення технічними термінами	Створення ілюзії експертності, подолання критичного сприйняття	Перевантаження технічним жаргоном, абревіатурами	67%
Емоційна ескалація	Викликання сильних емоцій для блокування раціонального аналізу	Емоційно заряджені слова, драматизація	76%

Економічні наслідки соціально-інженерних атак суттєво перевищують прямі фінансові втрати від компрометації систем або шахрайських транзакцій.

Комплексна оцінка має враховувати витрати на розслідування інцидентів, відновлення систем, компенсації постраждалим, юридичні витрати, регуляторні штрафи, а також довгострокові наслідки, пов’язані з репутаційними втратами, зниженням довіри клієнтів і партнерів, падінням вартості акцій та втратою конкурентних позицій. Особливо значущими є непрямі збитки від витоку інтелектуальної власності, комерційних таємниць і стратегічної інформації, що можуть проявлятися упродовж тривалого часу після атаки.

Соціальна інженерія залишається одним із найбільш ефективних векторів компрометації інформаційних систем, постійно еволюціонуючи у відповідь на розвиток захисних технологій та підвищення обізнаності користувачів. Ефективна протидія цим загрозам вимагає комплексного підходу, що поєднує технічні засоби захисту з систематичним навчанням персоналу, формуванням культури кібербезпеки та впровадженням надійних процедур верифікації критичних запитів та транзакцій.

2.2 Основні вектори розповсюдження шкідливого програмного забезпечення з використанням соціальної інженерії

Соціальна інженерія залишається одним із найефективніших методів розповсюдження шкідливого програмного забезпечення, оскільки спрямована на експлуатацію людського фактора, який часто виявляється найслабшою ланкою в системі кібербезпеки. Кіберзлочинці постійно вдосконалюють свої методи, використовуючи психологічні прийоми для маніпулювання користувачами та обходу технічних засобів захисту. Успішність соціальної інженерії базується на розумінні особливостей людської психології [31].

На сучасному етапі розвитку інформаційних технологій спостерігається тенденція до створення комплексних атак, які поєднують кілька векторів соціальної інженерії одночасно. Така стратегія значно підвищує ймовірність успіху зловмисників, оскільки дозволяє обходити різноманітні захисні механізми та психологічні бар'єри користувачів. Особливо небезпечними

стають цільові атаки, що розробляються під конкретну організацію або навіть особу, враховуючи специфіку їхньої діяльності та вразливі місця [32].

Електронна пошта залишається одним із основних каналів поширення шкідливого програмного забезпечення через свою поширеність і вразливість до соціальної інженерії. Фішингові листи, що імітують повідомлення від довірених осіб чи організацій, спонукають користувачів відкривати шкідливі вкладення або переходити за підозрілими посиланнями. Зловмисники ретельно відтворюють фірмову символіку, офіційний стиль комунікації та створюють відчуття терміновості для примусу до необдуманих дій [33].

Фішингові атаки через електронну пошту часто використовують сильні емоційні тригери. Зловмисники імітують повідомлення від банків про проблеми з рахунком, податкових органів, сповіщення про виграші, вигідні інвестиції чи працевлаштування. У корпоративному середовищі особливу загрозу становлять листи від імені керівництва або партнерів із фальшивими рахунками чи договорами з вбудованими макросами [34].

Месенджери й соціальні мережі є ефективним каналом поширення шкідливого програмного забезпечення через високий рівень довіри між користувачами та інтенсивність обміну повідомленнями. Кіберзлочинці використовують скомпрометовані акаунти для розсилки шкідливих посилань, маскуючи їх під відео, фото або новини. Особливо небезпечні атаки "на довірі", коли зловмисник спочатку встановлює дружні відносини з жертвою, а потім використовує цю довіру для інсталяції програмного забезпечення або витоку конфіденційної інформації [35].

Публічні Wi-Fi мережі у кафе, аеропортах, готелях та інших громадських місцях створюють сприятливе середовище для розповсюдження шкідливого програмного забезпечення методами соціальної інженерії. Зловмисники створюють підроблені точки доступу з назвами, подібними до легітимних мереж, або компрометують існуючі для здійснення атак "людина посередині". Підключившись до такої мережі, користувач може отримати сповіщення про необхідність оновлення програмного забезпечення або встановлення

спеціального сертифіката безпеки, які насправді є шкідливими програмами. Подібні атаки ефективні через природне бажання людей залишатися на зв'язку та отримувати безкоштовний доступ до інтернету (табл. 2.10) [36].

Таблиця 2.10

Порівняльний аналіз ефективності різних векторів соціальної інженерії

Вектор атаки	**Рівень успішності**	**Складність реалізації**	**Масштабованість**	**Середній рівень шкоди**
Фішингові електронні листи	Високий	Середня	Дуже висока	Високий
Цільовий фішинг (спірфішинг)	Дуже високий	Висока	Низька	Дуже високий
Соціальні мережі	Середній	Низька	Висока	Середній
Підроблені веб-сайти	Високий	Середня	Висока	Високий
Телефонні дзвінки (вішинг)	Високий	Середня	Низька	Високий
SMS-повідомлення (смішинг)	Середній	Низька	Висока	Середній
USB-носії	Дуже високий	Низька	Низька	Дуже високий
QR-коди	Середній	Низька	Середня	Середній

Телефонний зв’язок і надалі використовується зловмисниками для поширення шкідливого програмного забезпечення, незважаючи на появу нових комунікаційних каналів. Техніка "вішинг" (голосовий фішинг) полягає у дзвінках від імені банків, державних органів або технічної підтримки з метою переконати жертву встановити шкідливе програмне забезпечення або надати доступ до пристрою. Ефективність таких атак зумовлена психологічним впливом живого голосу, що викликає більшу довіру, ніж текстові повідомлення, а також вмінням досвідчених соціальних інженерів оперативно коригувати сценарій розмови відповідно до поведінки жертви, підсилюючи переконливість аргументів [37].

Фізичні носії інформації, зокрема USB-накопичувачі, залишаються ефективним засобом поширення шкідливого програмного забезпечення через прямий доступ до цільових систем, минаючи мережевий захист. Зловмисники залишають заражені носії в публічних місцях або біля офісів, розраховуючи на цікавість співробітників. Для підвищення ймовірності їх використання пристрої маркують написами типу "Зарплата" або "Конфіденційно". Особливо небезпечні цільові атаки, коли носії оформлені у корпоративному стилі компанії-жертви, що підвищує рівень довіри [38].

Підроблені веб-сайти є значною загрозою поширення шкідливого програмного забезпечення, оскільки їх важко візуально розпізнати навіть досвідченим користувачам. Зловмисники копіюють дизайн, логотипи та структуру легітимних ресурсів, змінюючи лише елементи URL. Користувачам пропонують встановити шкідливі оновлення, плагіни або завантажити заражені документи. Основні канали залучення на такі сайти — спам-розсилки, контекстна реклама та маніпуляції пошуковою видачею (табл. 2.11) [39].

Таблиця 2.11

Динаміка зростання атак з використанням різних векторів соціальної інженерії

Рік	**Фішингові листи**	**Соціальні мережі**	**Віши нг**	**Сміши нг**	**USB-атаки**	**QR-коди**
2021	43%	18%	12%	8%	15%	4%
2022	39%	22%	14%	11%	10%	4%
2023	35%	25%	16%	14%	6%	4%
2024	32%	27%	17%	16%	4%	4%

Використання QR-кодів для поширення шкідливого програмного забезпечення стало актуальним після пандемії COVID-19 через зростання популярності безконтактних технологій. Зловмисники розміщують підроблені коди на публічних стендах, рекламних матеріалах або поверх легітимних кодів у громадських місцях. Сканування веде на фішингові сайти або запускає завантаження шкідливих додатків. Особливу загрозу становить неможливість

візуального визначення вмісту QR-коду без спеціального програмного забезпечення [40].

Атаки на ланцюги постачання програмного забезпечення набувають поширення як вектори поширення шкідливого коду через соціальну інженерію. Зловмисники компрометують довірені джерела оновлень або облікові записи розробників, застосовуючи фішинг, вішинг або шантаж. Також використовують підробку офіційних джерел оновлень із схожими доменами та експлуатацію вразливостей систем автентифікації.

Платформи дистанційного навчання та віддаленої роботи відкривають нові можливості для соціальних інженерів через зниження безпосереднього контакту. Зловмисники надсилають фальшиві запрошення на конференції, пропонуючи завантажити шкідливе програмне забезпечення або оновити додатки. Ефективність атак зростає завдяки прагненню користувачів підтримувати професійні зв’язки і розвиватися дистанційно.

Кібершахрайство з використанням технологій глибокої підробки (deepfake) — новий й особливо небезпечний вектор соціальної інженерії для поширення шкідливого програмного забезпечення. Реалістичні відео- та аудіоімітації керівників дають "термінові інструкції" для компрометації систем. Психологічний вплив візуального і голосового підтвердження значно підвищує довіру порівняно з текстом. Виявлення таких підробок ускладнене навіть для експертів з інформаційної безпеки, що збільшує ризики успішних атак [41].

Удосконалення методів соціальної інженерії супроводжується розвитком штучного інтелекту, що дає змогу зловмисникам створювати персоналізовані та переконливі сценарії поширення шкідливого програмного забезпечення. Машинне навчання аналізує великі обсяги відкритих даних із соціальних мереж, професійних платформ і форумів для формування психологічних профілів жертв. На їх основі генеруються індивідуалізовані повідомлення з урахуванням інтересів, професії та мовних особливостей, що підвищує ймовірність успішної атаки та інфікування систем [42].

Висновки за розділом 2

Дослідження основних методів соціальної інженерії, спрямованих на поширення шкідливого програмного забезпечення, підкреслює їхню високу ефективність та постійну еволюцію в сучасному кіберпросторі. Шкідливе програмне забезпечення, включаючи віруси, трояни, програми-вимагачі та шпигунські програми, становить серйозну загрозу через різноманітність цілей, таких як економічний зиск, викрадення даних чи дестабілізація систем. Соціальна інженерія відіграє ключову роль у реалізації цих атак, використовуючи психологічні маніпуляції для обходу технічних засобів захисту. Поєднання психологічних принципів, таких як авторитет, дефіцит чи страх, із сучасними технологіями, зокрема штучним інтелектом та дипфейками, значно підвищує переконливість атак, роблячи їх важковідтворюваними для користувачів.

Аналіз векторів розповсюдження шкідливого програмного забезпечення демонструє багатогранність підходів, що застосовуються кіберзлочинцями. Фішингові електронні листи залишаються домінуючим каналом завдяки своїй масштабованості та здатності імітувати легітимну комунікацію, тоді як месенджери та соціальні мережі набувають популярності через високий рівень довіри користувачів. Нові вектори, такі як підроблені QR-коди, атаки через публічні Wi-Fi мережі та компрометація ланцюгів постачання, свідчать про адаптивність зловмисників до сучасних технологічних трендів. Особливо небезпечними є цільові атаки, такі як спеарфішинг чи вішинг, які враховують специфіку жертви, що ускладнює їх виявлення стандартними захисними механізмами.

Соціально-інженерні атаки демонструють високий рівень контекстуалізації, використовуючи актуальні суспільні події, кризові ситуації та галузеві особливості для створення переконливих сценаріїв. Пандемії, політичні події чи економічні кризи стають основою для маніпуляцій, що експлуатують емоційні реакції користувачів. У корпоративному секторі атаки

типу злам корпоративної пошти та інсайдерські загрози, підкріплені психолінгвістичними техніками, створюють значні ризики через доступ до цінних інформаційних активів. Галузева спеціалізація атак, особливо в критичній інфраструктурі, вимагає розробки індивідуалізованих захисних стратегій, що враховують унікальні вразливості кожного сектора.

Технологічний прогрес, зокрема використання генеративного штучного інтелекту, автоматизованих фішингових платформ та технологій глибоких підробок, відкриває нові можливості для масштабування та персоналізації атак. Автоматизовані системи дозволяють зловмисникам одночасно атакувати тисячі цілей, адаптуючи маніпулятивний контент до психологічних профілів жертв. Водночас розвиток мобільних платформ та інтернету речей створює додаткові вектори для соціальної інженерії, експлуатуючи обмеженість інтерфейсів та високу інтеграцію цих пристроїв у повсякденне життя. Прогнозується подальше ускладнення атак через інтеграцію з імерсивними технологіями, такими як віртуальна реальність, та використання нейролінгвістичних методів для точкового впливу.

Ефективна протидія соціально-інженерним атакам вимагає комплексного підходу, що поєднує технічні, освітні та організаційні заходи. Впровадження багатофакторної автентифікації, систем фільтрації та поведінкового аналізу є необхідним, але недостатнім без підвищення обізнаності користувачів. Регулярні тренінги, симуляції атак та формування культури критичного мислення відіграють вирішальну роль у зниженні вразливості до маніпуляцій. Особливу увагу слід приділяти розвитку емоційного інтелекту та психологічної стійкості, що дозволяють користувачам розпізнавати маніпулятивні техніки та зберігати раціональність у стресових ситуаціях. У контексті глобальних тенденцій кіберзагроз, формування міжнародної співпраці та гармонізації правового регулювання соціальної інженерії є критично важливим для забезпечення безпеки цифрового середовища.

РОЗДІЛ 3

МЕХАНІЗМИ ПРОТИДІЇ ПОШИРЕННЮ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ МЕТОДАМИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

3.1 Типові сценарії атак та їх ефективність

Сучасні кібератаки характеризуються надзвичайною різноманітністю та постійним удосконаленням, що робить їх все складнішими для виявлення та нейтралізації. Кіберзлочинці розробляють комплексні сценарії, які поєднують технічні експлойти з методами соціальної інженерії, створюючи багатовекторні атаки, здатні подолати навіть добре налаштовані системи захисту. Ефективність цих сценаріїв значною мірою залежить від рівня підготовки, ресурсів зловмисників та обізнаності цільової аудиторії щодо принципів кібербезпеки.

Атаки типу "людина посередині" (Man-in-the-Middle) залишаються одними з найнебезпечніших через здатність перехоплювати та змінювати дані під час передачі між двома сторонами. Зловмисник позиціонується між клієнтом і сервером, часто використовуючи підроблені сертифікати або скомпрометовані точки доступу Wi-Fi. Користувачі таких мереж зазвичай не помічають підміни і вважають з'єднання безпечним. Особливо вразливі публічні місця з великою кількістю користувачів — аеропорти, кафе, торговельні центри та конференц-зали [43].

Розподілені атаки на відмову в обслуговуванні (Distributed Denial of Service - DDoS) — потужний інструмент кіберзлочинців для блокування мережевих ресурсів. Сучасні атаки використовують масштабні ботнети з тисяч скомпрометованих пристроїв, включно з погано захищеним обладнанням Інтернету речей, і можуть досягати терабітної потужності, повністю блокуючи доступ. Крім порушення доступності, DDoS часто служать відволіканням, щоб

зловмисники могли здійснювати інші атаки, поки IT-персонал відновлює сервіси.

Ransomware продовжують завдавати значних збитків, використовуючи складне шифрування, що ускладнює відновлення даних без викупу. Особливо небезпечні атаки подвійного вимагання, коли зловмисники шифрують і викрадають дані, погрожуючи їх оприлюднити. Атаки починаються з компрометації одного пристрою через фішинг або вразливості, після чого зловмисники рухаються мережею, збирають дані і одночасно шифрують системи для максимального тиску (табл. 3.1).

Таблиця 3.1

Порівняння ефективності різних методів вхідного вектору атак

Метод проникнення	**Середній час виявлення**	**Рівень складності для зловмисника**	**Ефективність подолання периметра**	**Потенційний вплив на бізнес**
Фішингові кампанії	3-4 дні	Низький	Високий (76%)	Критичний
Вразливості веб-додатків	1-2 тижні	Високий	Середній (64%)	Високий
Скомпрометовані облікові дані	4-6 тижнів	Низький	Дуже високий (94%)	Критичний
Вразливості постачальників	2-3 місяці	Дуже високий	Високий (78%)	Критичний
Фізичний доступ	1-2 дні	Дуже високий	Дуже високий (96%)	Критичний
Соціальна інженерія	1-2 тижні	Середній	Високий (85%)	Критичний

Бічний рух мережею (lateral movement)— критичний етап багатьох сучасних кібератак для тривалого доступу до корпоративної інфраструктури. Після проникнення зловмисники збирають облікові дані, перехоплюють хеші паролів, використовують довірчі відносини між системами та вбудовані інструменти операційної системи.

Цілеспрямовані фішингові атаки (spear phishing) стали небезпечнішими завдяки глибокому збору інформації про жертв через соцмережі та професійні

платформи. Зловмисники вивчають корпоративну структуру, проекти та лексику, щоб створювати переконливі повідомлення від імені керівництва чи колег. Такі листи містять специфічні деталі, що підвищує ймовірність успіху навіть у організаціях з високою обізнаністю персоналу (табл. 3.2)[44].

Таблиця 3.2

Динаміка успішних атак за типом та сектором економіки (2022-2024)

Сектор	**Ransomware**	**Цільований фішинг**	**Експлуатація вразливостей**	**Атаки на ланцюги поставок**	**Інсайдерські загрози**
Фінансовий	24%	37%	12%	18%	9%
Охорона здоров'я	42%	23%	15%	12%	8%
Виробництво	38%	19%	22%	16%	5%
Державний сектор	29%	34%	16%	11%	10%
Енергетика	31%	18%	28%	15%	8%
Роздрібна торгівля	35%	29%	14%	17%	5%
Освіта	40%	32%	15%	8%	5%
Телекомунікації	22%	25%	31%	16%	6%

Особлива небезпека атак на ланцюги поставок програмного забезпечення полягає у використанні довірчих каналів розповсюдження, що дає змогу зловмисникам обходити традиційні засоби захисту периметра. Через технічну складність і великі ресурси такі операції часто пов’язують із державними або державно-спонсорованими групами, які мають значні можливості та чіткі цілі. Зловмисники компрометують процеси розробки або розповсюдження програмного забезпечення, впроваджуючи шкідливий код у легітимні оновлення, які потім поширюються серед тисяч чи мільйонів клієнтів.

Внутрішні загрози становлять один із найбільш складних викликів у системах кібербезпеки через легітимний доступ інсайдерів до корпоративних

ресурсів. Такі атаки можуть бути спрямованими, здійснюваними невдоволеними працівниками, або випадковими, пов’язаними з необережністю співробітників, які стали жертвами соціальної інженерії. Особливу загрозу становлять випадки вербування працівників із привілейованим доступом шляхом фінансової винагороди або шантажу.Ефективність таких атак значно зростає через знання інсайдерами внутрішньої структури організації, розташування цінних даних та особливостей систем захисту, що дозволяє їм цілеспрямовано атакувати найбільш вразливі або цінні активи [45].

Використання шкідливих скриптів у документах Microsoft Office залишається ефективним методом початкового проникнення, попри посилення захисту з боку Microsoft. Атаки часто починаються з фішингових листів із привабливими назвами документів: "Преміальні виплати", "Перегляд заробітної плати", "Терміновий договір" тощо. Їхня ефективність значною мірою базується на психологічному факторі довіри до нібито стандартних корпоративних матеріалів.

Розвинені цільові атаки (Advanced Persistent Threats, APT) є характерними для державно-спонсорованих угруповань з ресурсами та стратегічними цілями. Вони передбачають збір розвідданих, складні методи маскування та тривалу присутність у мережах жертви. APT-групи створюють спеціалізовані інструменти, що ускладнює їх виявлення. Особливо вразливими є сфери енергетики, оборони, критичної інфраструктури та держуправління.

Комплексні атаки на мобільні пристрої стають дедалі поширенішими через зростаюче значення смартфонів у корпоративному середовищі. Сучасні атаки включають експлуатацію вразливостей нульового дня, встановлення шкідливих програм через офіційні магазини або соціальну інженерію, компрометацію автентифікації через SMS та злам додатків для зберігання паролів. Особливу загрозу становлять комерційні шпигунські програми (наприклад, Pegasus), здатні повністю контролювати пристрої без видимих ознак, перехоплюючи повідомлення, фото, геодані та активуючи мікрофон і камеру.

Кібератаки на системи керування промисловими процесами вирізняються високою технічною складністю та потенційно катастрофічними наслідками. Особливо ефективними є атаки на інтерфейси між IT-системами та операційними технологіями, де зловмисники використовують відсутність єдиних стандартів безпеки та різницю в підходах до управління.

Атаки на хмарні середовища набули актуальності через масовий перехід організацій на хмарні технології та гібридні інфраструктури. Вони включають експлуатацію неправильно налаштованих сервісів, крадіжку токенів доступу, компрометацію інтерфейсу прикладного програмування (Application Programming Interface – API) та атаки на системи оркестрації контейнерів. Особливо небезпечні атаки на serverless-функції, що дозволяють виконувати код із високими привілеями. Складність хмарних екосистем із різними постачальниками та моделями безпеки ускладнює координацію заходів захисту та підвищує ризики експлуатації вразливостей (табл. 3.3)[46].

Таблиця 3.3

Порівняння середнього часу виявлення різних типів кібератак

Тип атаки	**Середній час виявлення (дні)**	**Середній час реагування (години)**	**Типова вартість інциденту (тис. USD)**
Програми-вимагачі	4.2	18.3	750-1,200
Крадіжка даних	73.5	24.7	350-800
Компрометація бізнес-електронної пошти	11.6	12.1	120-350
DDoS-атаки	0.8	6.4	50-200
Цільові APT-атаки	204.3	48.2	900-2,500
Експлойти нульового дня	89.7	36.5	600-1,800
Атаки на веб-додатки	33.1	14.8	300-700
Скомпрометовані облікові записи	55.2	16.9	200-450

Атаки із застосуванням штучного інтелекту становлять новий етап кіберзагроз, поєднуючи традиційні методи з можливостями машинного навчання. Системи глибокого навчання забезпечують створення фішингових

повідомлень, що імітують стиль конкретних осіб, генерацію переконливих deepfake-матеріалів, а також автоматизоване виявлення вразливостей [47].

3.2 Організаційні заходи для підвищення захисту від атак соціальної інженерії

Організаційний захист від соціальної інженерії потребує комплексного підходу, що враховує технічні аспекти та людський фактор. Ефективна стратегія базується на розумінні психології маніпуляцій і методів обходу технічного захисту. Необхідно впроваджувати багаторівневу систему, що включає навчання персоналу, формування культури кібербезпеки та процедури верифікації запитів, пов’язаних із конфіденційною інформацією чи фінансовими операціями.

Програми з підвищення обізнаності персоналу з кібербезпеки мають враховувати специфіку організації та галузі. Замість традиційних щорічних тренінгів впроваджуються безперервні навчальні формати — симуляції фішингових атак, інтерактивні семінари та короткі модулі, інтегровані в робочі процеси. Особливу увагу слід приділяти навчанню розпізнаванню сучасних технік соціальної інженерії, зокрема цільового фішингу, вішингу та атак із використанням штучного інтелекту для створення фальшивих аудіо- та відеоматеріалів [48].

Розробка та впровадження процедур верифікації запитів на доступ до ключових систем, переказ коштів або розкриття конфіденційної інформації є основою організаційного захисту. Процедури повинні включати багатофакторну автентифікацію та підтвердження запитів через альтернативні канали зв’язку. Важливо формувати культуру, де перевірка автентичності сприймається як професіоналізм, а не недовіра.

Сегментація доступу за принципом мінімальних привілеїв знижує ризики від атак соціальної інженерії. Впровадження політик розмежування, регулярний аудит привілеїв та автоматизоване управління ідентифікацією запобігають

несанкціонованому доступу навіть при компрометації облікових даних. Важливо постійно оновлювати схеми доступу при зміні ролей або звільненні співробітників (табл. 3.4).

Таблиця 3.4

Ефективність різних підходів до навчання персоналу протидії соціальній інженерії

Метод навчання	**Короткострокова ефективність**	**Довгострокова ефективність**	**Залучення співробітників**	**Вартість впровадження**
Традиційні лекційні заняття	42%	31%	Низьке	Середня
Інтерактивні навчальні модулі	58%	49%	Середнє	Середня
Симуляції фішингових атак	76%	64%	Високе	Висока
Гейміфіковані програми	81%	73%	Дуже високе	Висока
Наставництво та обмін досвідом	72%	84%	Високе	Середня
Практичні лабораторні заняття	84%	79%	Дуже високе	Дуже висока
Навчання на реальних інцидентах	89%	86%	Високе	Низька

Створення відкритої комунікації з питань кібербезпеки сприяє своєчасному виявленню атак соціальної інженерії. Впровадження програм заохочення повідомлень про підозрілі інциденти, анонімних каналів та політики відсутності санкцій за ненавмисні помилки дозволяє швидко реагувати на загрози. Ефективним є запровадження амбасадорів кібербезпеки в підрозділах як першого контакту для співробітників.

Регулярне тестування стійкості персоналу до соціальної інженерії через контрольовані фішингові кампанії дозволяє оцінити ефективність навчання та виявити вразливі групи. Тести проводяться за затвердженими методиками з поступовим ускладненням сценаріїв і подальшим аналізом результатів. Основний акцент робиться на навчальному характері тестів із негайним зворотним зв’язком та рекомендаціями, а не на дисциплінарних заходах.

Розробка комплекснихпланів реагування на інциденти соціальної інженерії передбачає розподіл відповідальності, комунікаційні протоколи та процедури ізоляції скомпрометованих систем. Важливо готувати групи реагування до типових сценаріїв і регулярно проводити навчальні симуляції. Плани мають враховувати мінімізацію репутаційних ризиків і взаємодію з правоохоронними органами у разі серйозних інцидентів (табл. 3.5).

Таблиця 3.5

Порівняння ефективності організаційних заходів захисту від соціальної інженерії за секторами економіки

Сектор	**Навчання персоналу**	**Процедури верифікації**	**Регламенти реагування**	**Технічні засоби захисту**	**Культура безпеки**
Фінансовий	78%	89%	81%	92%	76%
Охорона здоров'я	65%	72%	77%	74%	63%
Виробництво	56%	68%	64%	76%	59%
Державний сектор	71%	83%	75%	67%	68%
Енергетика	75%	81%	84%	89%	72%
ІТ та телекомуніка ції	84%	79%	86%	93%	88%
Освіта	61%	64%	58%	65%	72%
Роздрібна торгівля	58%	76%	67%	71%	64%

Впровадження автоматизованих систем аналізу комунікацій підвищує здатність виявляти та блокувати шкідливі повідомлення. Сучасні рішення

застосовують машинне навчання для аналізу електронної пошти, корпоративних месенджерів та інших каналів на ознаки фішингу, маніпуляцій і порушень політик безпеки. Особливо ефективні системи, що враховують контекст і стиль спілкування конкретних осіб [49].

Розробка та оновлення внутрішніх стандартів обробки конфіденційної інформації є ключовим елементом захисту від несанкціонованого доступу. Стандарти мають визначати класифікацію інформації, правила передачі, вимоги до шифрування та строки зберігання. Особлива увага приділяється навчанню персоналу розпізнавати легітимні запити та процедурам їх верифікації, особливо від нових контактів або через нетипові канали (табл. 3.6).

Таблиця 3.6

Ефективність методів протидії різним векторам атак соціальної інженерії

Вектор атаки	**Технічні заходи**	**Навчання персоналу**	**Організаційні процедури**	**Загальна ефективність захисту**
Фішинг електронною поштою	87%	76%	81%	83%
Телефонний вішинг	43%	89%	78%	72%
SMS-фішинг (смішинг)	65%	72%	69%	69%
Атаки через соціальні мережі	54%	81%	63%	67%
Фізичне проникнення	72%	83%	91%	84%
USB-дропінг	76%	87%	69%	78%
Підробка ідентичності	61%	79%	86%	76%
Атаки з використанням штучного інтелекту	68%	64%	71%	68%

Впровадження строгих політик управління доступом до фізичних об’єктів є ключовим елементом захисту від атак соціальної інженерії з фізичним проникненням. Політики мають регламентувати ідентифікацію відвідувачів, супровід гостей, контроль винесення обладнання та реагування на несанкціонований доступ. Особлива увага приділяється навчанню персоналу щодо розпізнавання типових технік соціальної інженерії, таких як імітація авторитету чи створення штучної терміновості [45].

Регулярний аудит та тестування системи захисту від соціальної інженерії дозволяє вчасно виявляти й усувати вразливості. Аудити охоплюють оцінку навчальних програм, перевірку дотримання політик, аналіз інцидентів і тестування технічних заходів. Залучення зовнішніх експертів для незалежної оцінки та симуляцій складних атак забезпечує об’єктивний огляд рівня захищеності і виявлення прихованих вразливостей [50].

Інтеграція ментальних моделей у прийняття рішень підвищує здатність персоналу реагувати на нестандартні ситуації в інформаційній безпеці. Вони охоплюють перевірку легітимності, виявлення підозрілих запитів та дії у разі сумнівів. Найефективнішими є моделі типу «стоп-думай-дій», що формують звичку аналізувати ризики й звертатися до фахівців (табл. 3.7).

Таблиця 3.7

Вплив часу проведення навчань з кібербезпеки на стійкість до атак соціальної інженерії

Інтервал повторення навчань	**Рівень успішності фішингових тестів**	**Час виявлення підозрілих інцидентів**	**Частка повідомлень про підозрілі активності**
Щорічно	42%	3.7 годин	27%
Двічі на рік	58%	2.4 години	43%
Щоквартально	67%	1.8 годин	61%
Щомісячно	83%	0.9 годин	79%
Безперервне навчання	91%	0.5 годин	86%

Формування корпоративної культури кібербезпеки є одним із найефективніших довгострокових заходів захисту від соціальної інженерії. Вона базується на відкритому обговоренні безпекових питань, підтримці ініціатив керівництва та заохоченні відповідальної поведінки співробітників. Важливою є роль керівників вищої ланки, які своїм прикладом встановлюють стандарти поведінки. Впровадження культури безпеки потребує регулярних комунікацій, інтеграції кібербезпеки в управлінські процеси та визнання її як складової успіху організації [51].

3.3 Розробка алгоритму навчання користувачів з протидії методам соціальної інженерії

Ефективний алгоритм навчання протидії соціальній інженерії базується на розумінні психологічних механізмів та поведінкових патернів, що роблять людей вразливими. Розробка алгоритму потребує мультидисциплінарного підходу, поєднуючи кібербезпеку, когнітивну психологію, педагогіку та поведінкову економіку. Основою є навчальна програма, яка інформує про загрози, розвиває критичне мислення та формує захисні реакції. Важлива адаптація методів до професійних груп, рівня технічної грамотності та психологічних особливостей учасників [52].

Початковим етапом розробки алгоритму навчання є аналіз цільової аудиторії та актуальних загроз соціальної інженерії для конкретної організації чи галузі. Аналіз включає вивчення статистики атак, рівня обізнаності користувачів, особливостей робочих процесів і сценаріїв взаємодії з зовнішніми контактами. Визначаються категорії співробітників з підвищеним ризиком і найпоширеніші вектори атак. Результати слугують основою для формування персоналізованих навчальних траєкторій.

Навчальна програма має включати теоретичні основи соціальної інженерії та практичні навички протидії маніпуляціям. Теоретична частина охоплює психологічні тригери, що використовують зловмисники: страх, цікавість, жадібність, бажання допомогти та соціальні очікування. Практичний блок спрямований на розвиток умінь розпізнавати підозрілі повідомлення, верифікувати джерела інформації та адекватно реагувати на загрози. Важливим є аналіз реальних кейсів атак із розбором методів маніпуляції та можливостей їх запобігання (табл. 3.8) [53].

Таблиця 3.8

Ефективність різних методів навчання протидії соціальній інженерії залежно від рівня посади

Рівень посади	**Інтерактивні симуляції**	**Кейс-стаді**	**Традиційні лекції**	**Мікронавчання**	**Гейміфікація**	**Групові обговорення**
Топ-менеджмент	73%	89%	56%	61%	42%	78%
Середня ланка управління	81%	76%	61%	73%	68%	82%
Спеціалісти з IT	92%	83%	59%	87%	76%	71%
Адміністративний персонал	68%	72%	58%	84%	79%	66%
Виробничий персонал	76%	61%	53%	89%	82%	59%
Новоприйняті співробітники	84%	74%	63%	71%	88%	76%

Методологія ґрунтується на принципах андрагогіки, орієнтованих на специфіку навчання дорослих. Алгоритм поєднує мікровідео, інтерактивні вебінари, практичні завдання й дискусії, забезпечуючи самостійну роботу в корпоративній системі управління навчанням з адаптивним контентом і моніторингом прогресу. Особливий акцент робиться на емоційно залучаючому контенті, що демонструє реальні наслідки атак соціальної інженерії для компанії та персоналу.

Основою алгоритму навчання є регулярні симуляції фішингових атак, що оцінюють практичне застосування знань у наближених до реальних умовах. Симуляції поступово ускладнюються від простих до складних сценаріїв, що відтворюють сучасні методи зловмисників. Обов’язковим є негайний зворотний зв’язок із поясненнями ознак підозрілих повідомлень та рекомендаціями щодо

правильної реакції. Аналіз результатів допомагає виявляти вразливі категорії співробітників і коригувати навчальну програму з урахуванням прогалин.

Важливою частиною навчання є формування ментальних моделей і автоматичних реакцій на підозрілі комунікації. Застосовуються мнемонічні правила на кшталт "STOP-THINK-ACT", що активуються у ризикових ситуаціях. Моделі охоплюють перевірку відправника альтернативним каналом, аналіз контексту та виявлення ознак маніпуляції (терміновість, погрози, нетипові запити). Ефективність зростає завдяки регулярному повторенню та симуляціям (табл. 3.9).

Таблиця 3.9

Порівняння ефективності різних форматів надання зворотного зв'язку після симуляцій фішингових атак

Формат зворотного зв'язку	**Рівень засвоєння інформації**	**Зміна поведінки**	**Емоційний відгук**	**Довгострокова ефективність**
Автоматичне повідомлення	51%	43%	Нейтральний	37%
Детальна письмова інструкція	64%	57%	Помірно позитивний	53%
Короткий відеоурок	76%	68%	Позитивний	61%
Персональна консультація	89%	81%	Дуже позитивний	78%
Групове обговорення результатів	72%	74%	Позитивний	69%
Гейміфікований інтерактивний модуль	81%	77%	Дуже позитивний	72%

Застосування гейміфікаційних елементів у навчальних алгоритмах сприяє підвищенню мотивації користувачів і покращенню засвоєння знань. До найбільш ефективних інструментів належать система досягнень, рейтингові таблиці, візуалізація прогресу та відзнаки за успіхи у сфері інформаційної

безпеки. Водночас критично важливо дотримуватися оптимального співвідношення між ігровими механіками та змістовною серйозністю, аби зберегти належне ставлення до теми кібербезпеки.

Персоналізація навчання є ключовою умовою ефективної протидії соціальній інженерії. Адаптивні алгоритми вибудовують індивідуальні траєкторії, спираючись на результати тестів, дії в симуляціях і взаємодію з контентом, зосереджуючись на актуальних ризиках та виявлених вразливостях. Найбільшу результативність забезпечують моделі, що враховують не лише службову роль, а й психологічний портрет користувача, підвищуючи його опір до специфічних маніпулятивних технік [54].

Оцінка ефективності навчального алгоритму є критичним компонентом його циклічного вдосконалення. Система має поєднувати об’єктивні метрики — результати тестів, симуляцій фішингу, кількість інцидентів — із суб’єктивними індикаторами, як-от зміна безпекової поведінки та рівень впевненості користувача. Особливе значення має аналіз зв’язку між освітніми активностями та фактичною стійкістю до атак, що дає змогу виявити найбільш результативні компоненти та раціоналізувати їх застосування (табл. 3.10).

Таблиця 3.10

Динаміка ефективності навчання з протидії соціальній інженерії в часі

Часовий період після навчання	**Здатність розпізнавати фішинг**	**Дотримання політик безпеки**	**Повідомлення про інциденти**	**Загальна стійкість до атак**
1 місяць	83%	81%	86%	84%
3 місяці	76%	74%	79%	76%
6 місяців	64%	62%	68%	65%
12 місяців	51%	53%	54%	53%
Після повторного навчання	91%	89%	94%	92%

Запровадження системи наставництва та інституту "амбасадорів кібербезпеки" у структурних підрозділах організації сприяє підвищенню

ефективності навчального алгоритму. Амбасадори, які проходять спеціалізовану підготовку та регулярно оновлюють знання про актуальні загрози, виконують роль локальних експертів і консультантів для колег. Такий підхід забезпечує оперативне поширення критичної інформації, інтеграцію питань кібербезпеки у щоденну роботу та формування культури відповідального ставлення до захисту від соціальної інженерії [55].

Інтеграція навчання з протидії соціальній інженерії в систему корпоративного розвитку є критичною умовою підтримання належного рівня кібербезпеки. Відповідні компоненти мають бути невід'ємною частиною програм адаптації, професійної підготовки та підвищення кваліфікації. Найбільш ефективною є модель, що розглядає навички протидії соціальній інженерії як елемент професійної компетентності, необхідної для успішної діяльності в цифровому середовищі (табл. 3.11).

Таблиця 3.11

Кореляція між методами атак соціальної інженерії та ефективними навчальними підходами

Метод соціальної інженерії	**Найефективніший навчальний підхід**	**Головні навички для протидії**	**Частота оновлення навчання**
Цільовий фішинг	Симуляції в реальному середовищі	Верифікація джерел	Щомісячно
Вішинг (голосовий фішинг)	Рольові ігри + аудіозаписи реальних атак	Протоколи підтвердження	Щоквартально
Претекстинг	Аналіз кейсів + поведінкові тренінги	Критичне мислення	Щоквартально
Квіпрокво	Відеосимуляції + тестові сценарії	Процедури автентифікації	Раз на півроку
Троянський кінь	Демонстрації + практичні лабораторії	Аналіз контексту ситуації	Щоквартально
Підбирання	Фізичні симуляції + аудит середовища	Фізична безпека	Щорічно

Продовження таблиці 3.11

Атаки через соціальні мережі	Інтерактивні онлайн-симуляції	Управління цифровим слідом	Щомісячно
Зворотна соціальна інженерія	Поглиблені сценарні тренінги	Розпізнавання маніпуляцій	Раз на півроку

Розробка механізмів формування критичного мислення та скептицизму щодо нетипових комунікацій є ключовим елементом алгоритму навчання з протидії соціальній інженерії. Користувачів слід навчати розпізнавати ознаки маніпулятивного впливу, зокрема терміновість, апеляцію до авторитету, надмірно привабливі пропозиції або загрози. Важливо закріпити практику перевірки автентичності комунікацій як норму відповідальної поведінки. Для цього доцільно застосовувати практичні вправи з аналізу типових сценаріїв і розробки ефективних моделей реагування.

Включення елементів психологічної підготовки до протидії соціальному тиску та маніпуляціям значно підвищує ефективність захисту. Користувачів слід навчати розпізнавати та нейтралізувати техніки створення дискомфорту, провини чи страху не відповідати очікуванням. Ефективними засобами є рольові ігри для відпрацювання впевненої відмови та групові обговорення психологічних механізмів уразливості. Важливо також розвивати емоційну стійкість у стресових ситуаціях, коли критичне мислення ослаблене.

Кульмінацією навчального алгоритму є формування стійкої корпоративної культури кібербезпеки, де захист від соціальної інженерії інтегровано у всі процеси — від найму до оцінки ефективності. Важливою є активна підтримка з боку вищого керівництва, яке власним прикладом підтверджує прихильність до безпеки. Регулярні комунікації, визнання відповідальної поведінки та включення показників кібербезпеки у систему ключових показників ефективності сприяють становленню пильності як невід’ємної частини культури організації.

Висновки за розділом 3

Дослідження типових сценаріїв кібератак у третьому розділі підкреслює їхню зростаючу складність і багатогранність, що вимагає комплексного захисту інформаційних систем. Атаки, як-от фішинг, програми-вимагачі, розподілені атаки на відмову в обслуговуванні та компрометація ланцюгів постачання, поєднують технічні експлойти з методами соціальної інженерії. Особливо небезпечні цільові атаки, які використовують детальну розвідку та персоналізовані сценарії для обходу захисту. Це свідчить про необхідність не лише технічного вдосконалення безпеки, а й систематичного підвищення обізнаності користувачів та розвитку їхньої здатності розпізнавати маніпуляції.

Організаційні заходи, спрямовані на протидію соціальній інженерії, є ключовим елементом ефективної кібербезпеки, оскільки людський фактор залишається найвразливішою ланкою. Впровадження чітких процедур верифікації, сегментація доступу, регулярне навчання персоналу та створення культури відкритої комунікації щодо безпеки значно знижують ризики успішних атак. Особливу роль відіграють програми безперервного навчання, які включають симуляції фішингових атак і практичні вправи, що дозволяють співробітникам розвивати навички критичного мислення та швидкого реагування на підозрілі ситуації. Такий підхід забезпечує не лише підвищення індивідуальної стійкості, а й зміцнення загальної безпеки організації.

Розробка алгоритму навчання користувачів з протидії соціальній інженерії підкреслює важливість персоналізованого та практико-орієнтованого підходу. Інтеграція теоретичних знань про психологічні механізми маніпуляцій із регулярними симуляціями атак дозволяє формувати стійкі поведінкові патерни, які допомагають розпізнавати та нейтралізувати загрози. Використання гейміфікації, адаптивних навчальних систем та ментальних моделей, таких як "стоп-думай-дій", сприяє підвищенню залученості та ефективності засвоєння матеріалу. Це особливо важливо в умовах швидкої

еволюції методів атак, що вимагають від користувачів постійної пильності та готовності до нетипових сценаріїв.

Значна увага в розділі приділена формуванню корпоративної культури кібербезпеки, яка інтегрує принципи безпеки в усі аспекти діяльності організації. Створення такої культури передбачає активну участь керівництва, впровадження систем заохочення за відповідальну поведінку та регулярне оновлення політик безпеки відповідно до нових загроз. Важливим є також залучення амбасадорів кібербезпеки, які забезпечують децентралізовану підтримку та швидке поширення інформації про нові ризики. Такий підхід не лише підвищує стійкість до атак, а й сприяє формуванню довіри до внутрішніх процесів безпеки, що є основою для довгострокового захисту.

Нарешті, аналіз сучасних методів протидії кіберзагрозам вказує на необхідність поєднання організаційних, технічних і освітніх заходів для створення багаторівневої системи захисту. Аудит вразливостей, тестування стійкості до атак і регулярне оновлення навчальних програм дозволяють організаціям адаптуватися до динамічного ландшафту загроз. У контексті зростання ролі штучного інтелекту та автоматизованих атак особливого значення набуває розвиток психологічної стійкості користувачів і впровадження автоматизованих систем аналізу комунікацій. Комплексний підхід, що враховує як технологічні, так і людські аспекти, є єдиним шляхом до забезпечення безпеки в умовах сучасних кіберзагроз.

ВИСНОВКИ

Дослідження методів соціальної інженерії та їхнього зв’язку з поширенням шкідливого програмного забезпечення підтвердило їхню важливу роль у сфері кібербезпеки. Соціальна інженерія, як засіб впливу на людський фактор, ефективно обходить технічні засоби захисту, використовуючи психологічні вразливості — довіру, страх або неуважність. У поєднанні з технічними засобами поширення шкідливого програмного забезпечення це створює гібридні атаки, складні для виявлення. Така ситуація вимагає комплексного підходу до захисту, що охоплює як технологічні, так і поведінкові аспекти.

Проведений аналіз кіберзагроз свідчить про зростання складності та масштабів атак зі шкідливим програмним забезпеченням. Програми-вимагачі, банківські трояни та шпигунське програмне забезпечення дедалі частіше застосовують соціально-інженерні методи, як-от фішинг і цільовий фішинг, для початкового проникнення. Розвиток технологій, зокрема штучного інтелекту, ускладнює розпізнавання персоналізованих атак навіть технічно підкованим користувачам. Це підкреслює необхідність постійного вдосконалення захисту і підвищення цифрової грамотності.

Виконане дослідження типових сценаріїв атак соціальної інженерії демонструє їхню високу ефективність завдяки адаптації до психологічних і соціальних особливостей цільової аудиторії. Зловмисники використовують принципи впливу — авторитет, дефіцит, взаємність — для маніпуляції поведінкою, що забезпечує успіх атак навіть у захищених організаціях. Особливо небезпечні цільові атаки, які базуються на зборі інформації про жертву, підвищуючи ймовірність добровільних шкідливих дій. Це акцентує необхідність превентивних заходів для розвитку критичного мислення та обізнаності.

Огляд сучасних засобів захисту від соціальної інженерії свідчить про обмежену ефективність традиційних технічних рішень, таких як антивіруси та

системи виявлення вторгнень, проти психологічних маніпуляцій. Значний потенціал мають системи поведінкового аналізу, автоматизовані фільтри комунікацій і регулярні симуляції фішингових атак. Водночас ключову роль відіграє навчання користувачів, що підвищує стійкість до маніпуляцій і сприяє формуванню культури безпеки. Це вказує на необхідність інтеграції технічних і освітніх заходів для максимального ефекту.

Розроблені рекомендації для користувачів і організацій наголошують на важливості людиноцентричної моделі кібербезпеки. Регулярне навчання, практичні симуляції та впровадження ментальних моделей прийняття рішень, таких як «стоп-думай-дій», допомагають користувачам ефективно протидіяти соціальній інженерії. Для організацій ключовими є створення чітких процедур реагування на інциденти, впровадження політики верифікації запитів та підтримка культури відкритої комунікації з питань безпеки. Ці заходи сприяють зниженню ризиків і підвищенню стійкості до кіберзагроз.

Загалом, результати дослідження вказують на необхідність постійної адаптації до еволюції методів соціальної інженерії та шкідливого програмного забезпечення. У умовах швидкого технологічного прогресу та зростання цифровізації всіх сфер життя, кібербезпека має розглядатися як динамічний процес, що вимагає проактивного підходу. Формування глобальної культури кібергігієни, де кожен користувач усвідомлює свою роль у захисті інформації, є запорукою зниження ризиків і забезпечення безпеки в цифровому середовищі.

Виходячи із поставленої мети кваліфікаційної роботи, були виконані наступні завдання:

- проаналізовано поняття та класифікацію соціальної інженерії в контексті кібербезпеки;
- досліджено шкідливе програмне забезпечення, його цілі, види, механізми дії та способи розповсюдження;
- охарактеризовано методи та засоби соціальної інженерії, спрямовані на поширення шкідливого програмного забезпечення;

- визначено основні вектори розповсюдження шкідливого ПЗ із використанням соціальної інженерії;
- описано типові сценарії атак та проаналізовано їхню ефективність;
- розроблено рекомендації для користувачів та організацій щодо мінімізації ризиків зараження шкідливим програмним забезпеченням через соціально-інженерні впливи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Mitnick, K. D., & Simon, W. L. (2011). The art of deception: Controlling the human element of security. John Wiley & Sons. https://books.google.com.ua/books?hl=uk&lr=&id=9LpawpklYogC

2. Hadnagy, C., & Fincher, M. (2017). Understanding social engineering based attacks. Computers & Security, 70, 487–501. https://www.sciencedirect.com/science/article/abs/pii/S0167404817302249

3. National Institute of Standards and Technology. (n.d.). Social engineering. NIST Computer Security Resource Center Glossary. https://csrc.nist.gov/glossary/term/social_engineering

4. Verizon. (2024). 2024 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

5. В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. «Інформаційна та кібербезпека: соціотехнічний аспект». - 2015.

6. Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. Future Internet, 11(4), 89. https://www.mdpi.com/1999-5903/11/4/89

7. Grobler, M., Gaire, R., & Nepal, S. (2021). User, usage and usability: Redefining human-centric cyber security. Frontiers in Big Data, 4, Article 583723. https://doi.org/10.3389/fdata.2021.583723

8. Nobles, C. (2022). Stress, burnout, and security fatigue in cybersecurity: A human factors problem. Harvard Journal of Business and Public Administration. https://doi.org/10.2478/hjbpa-2022-0003

9. AV-TEST (2025). Malware Statistics & Trends Report. AV-TEST. https://www.av-test.org/en/statistics/malware/

10. Cybersecurity Ventures. (2025). Top 10 Cybersecurity Predictions and Statistics for 2024. Cybercrime Magazine. https://cybersecurityventures.com/research/

11. Ngafeeson, M. (2021). Cybercrime classification: A motivational model. https://www.researchgate.net/profile/Madison-Ngafeeson/publication/355840917_Cybercrime_Classification_A_Motivational_Model/links/6180a257a767a03c14e1bb3c/Cybercrime-Classification-A-Motivational-Model.pdf

12. ESET. (2013). Google identifies 10,000 phishing and malware sites every day. WeLiveSecurity. https://www.welivesecurity.com/2013/06/26/google-identifies-10000-phishing-and-malware-sites-every-day/

13. World Economic Forum. (2023). Global Cybersecurity Outlook 2023. https://www.weforum.org/publications/global-cybersecurity-outlook-2023/

14. Morgan, S. (2020). Cybercrime to cost the world $10.5 trillion annually by 2025. Cybercrime Magazine. https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

15. Kumar, J. N. Y. (2019). Behavioural based threat modelling to increase the efficiency in breach identification and notification (Магістерська робота). Національний коледж Ірландії. https://norma.ncirl.ie/4176/1/joshuanevilrajyuvakumar.pdf

16. VRI Technology. (2025). Protecting your small business: Essential cybersecurity tips to thwart phishing attacks. VRI Technology. https://www.vritechnology.com/post/protecting-your-small-business-essential-cybersecurity-tips-to-thwart-phishing-attacks

17. Symantec Internet Security Threat Report. https://docs.broadcom.com/docs/istr-03-jan-en

18. Microsoft. (2024). Microsoft Digital Defense Report 2024. https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

19. Stergiou, D. (2013). Social engineering and influence: A study that examines Kevin Mitnick’s attacks through Robert Cialdini’s influence principles (Магістерська робота). https://www.diva-portal.org/smash/get/diva2:1016104/FULLTEXT02.pdf

20. CCS Learning Academy. (2024). What is FOMO in cybersecurity? https://www.ccslearningacademy.com/what-is-fomo-in-cybersecurity/

21. Mandiant. (2013). APT1: Exposing One of China's Cyber Espionage Units. https://services.google.com/fh/files/misc/mandiant-apt1-report.pdf

22. News Hub Asia. (2022). Trend Micro reveals 82 per cent of Malaysian organisations concerned about growing attack surface. https://www.newshubasia.com/feature-report/trend-micro-reveals-82-per-cent-of-malaysian-organisations-concerned-about-growing-attack-surface/

23. Aldawood, H., & Skinner, G. (2020). An advanced taxonomy for social engineering attacks. International Journal of Computer Applications, https://doi.org/10.5120/ijca2020919744

24. Ivaturi, K., & Janczewski, L. (2011). A taxonomy for social engineering attacks. Proceedings of the International Conference on Information Resources Management (CONF-IRM). Association for Information Systems. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1015&context=confirm2011

25. Theocharidou, M., Lella, I., Naydenov, R., & Malatras, A. (2025). ENISA Threat Landscape: Finance Sector, January 2023 to June 2024. European Union Agency for Cybersecurity (ENISA). https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024_Final.pdf

26. Chapagain, D., Kshetri, N., Aryal, B., & Dhakal, B. (2024). SEAtech: Deception techniques in social engineering attacks: An analysis of emerging trends and countermeasures. https://arxiv.org/abs/2408.02092

27. Al-Musib, N. S., Al-Serhani, F. M., Humayun, M., & Jhanjhi, N. Z. (2023). Business email compromise (BEC) attacks. Materials Today: Proceedings, 81(Part 2), 497–503. https://doi.org/10.1016/j.matpr.2021.03.647

28. Dash, B., & Sharma, P. (2023). Are ChatGPT and Deepfake Algorithms Endangering the Cybersecurity Industry? A Review. International Journal of Engineering and Applied Sciences (IJEAS), 10(1). https://doi.org/10.31873/IJEAS.10.1.01

29. Calderaro, A., & Craig, A. J. S. (2020). Transnational governance of cybersecurity: Policy challenges and global inequalities in cyber capacity building. Third World Quarterly, 41(6), 917–938. https://www.tandfonline.com/doi/full/10.1080/01436597.2020.1729729

30. Uyheng, J., Moffitt, J. D., & Carley, K. M. (2022). The language and targets of online trolling: A psycholinguistic approach for social cybersecurity. Information Processing & Management, 59(5), 103012. https://doi.org/10.1016/j.ipm.2022.103012

31. Mitnick, K. D., & Simon, W. L. (2002). The art of deception: Controlling the human element of security. Foreword by S. Wozniak. Wiley. https://www.academia.edu/1396282/The_art_of_deception

32. Birthriya, S. K., Ahlawat, P., & Jain, A. K. (2025). Detection and prevention of spear phishing attacks: A comprehensive survey. Computers & Security, 151, 104317. https://doi.org/10.1016/j.cose.2025.104317

33. SlashNext. (2023). The State of Phishing Report 2023. https://slashnext.com/wp-content/uploads/2023/10/SlashNext-The-State-of-Phishing-Report-2023.pdf

34. Phishing.org. What is phishing? https://www.phishing.org/what-is-phishing

35. Rendina, F. (2019). A Social Engineering attack using Telegram. https://www.linkedin.com/pulse/social-engineering-attack-using-telegram-fabrizio-rendina/

36. Derella, M., Sharivker, S., & Aldana-Diaz, R. (n.d.). Integration of Social Engineering to Propagate the Spread of Malware Throughout Networks. https://samuelsharivker.com/papers/Social_Engineering_and_Malware_Propagation.pdf

37. Figueiredo, J., Carvalho, A., Castro, D., Gonçalves, D., & Santos, N. (2024). On the feasibility of fully AI-automated vishing attacks. arXiv. https://arxiv.org/abs/2409.13793

38. Stasiukonis, S. (2006). Social Engineering, the USB Way. Dark Reading. https://www.darkreading.com/perimeter/social-engineering-the-usb-way

39. Державна служба спеціального зв'язку та захисту інформації України. (2024). Система виявлення вразливостей і реагування на кіберінциденти та кібератаки: Річний звіт 2024. https://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006

40. Khan, N. A., Brohi, S. N., & Zaman, N. (2020). Ten deadly cyber security threats amid COVID-19 pandemic. TechRxiv. https://www.techrxiv.org/users/662470/articles/675719-ten-deadly-cyber-security-threats-amid-covid-19-pandemic

41. Pedersen, K. T., Pepke, L., Stærmose, T., Papaioannou, M., Choudhary, G., & Dragoni, N. (2025). Deepfake-driven social engineering: Threats, detection techniques, and defensive strategies in corporate environments. Journal of Cybersecurity and Privacy, 5(2), 18. https://doi.org/10.3390/jcp5020018

42. Falade, P. V. (2023). Decoding the threat landscape: ChatGPT, FraudGPT, and WormGPT in social engineering attacks. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 9(5), 185–198. https://doi.org/10.32628/CSEIT2390533

43. Mallik, A. (2018). Man-in-the-middle-attack: Understanding in simple words. Cyberspace: Jurnal Pendidikan Teknologi Informasi, 2(2), 109–134. https://jurnal.ar-raniry.ac.id/index.php/cyberspace/article/view/3453

44. Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. Future Internet, 12(10), 168. https://doi.org/10.3390/fi12100168

45. Fan, W., Lwakatare, K., & Rong, R. (2017). Social engineering: I-E based model of human weakness for attack and defense investigations. International Journal of Computer Network and Information Security (IJCNIS), 9(1), 1–11. https://doi.org/10.5815/ijcnis.2017.01.01

46. Shenderovitz, G., & Nissim, N. (2024). Bon-APT: Detection, attribution, and explainability of APT malware using temporal segmentation of API calls. Computers & Security. https://doi.org/10.1016/j.cose.2024.103862

47. Gal, S., & Bulgurcu, B. (2024). Exploring factors influencing internet users' susceptibility to deepfake phishing. AMCIS 2024 Proceedings, 21. https://aisel.aisnet.org/amcis2024/adoptdiff/adoptdiff/21

48. Smith, A., Papadaki, M., & Furnell, S. M. (2013). Improving awareness of social engineering attacks. In R. C. Dodge & L. Futcher (Eds.), Information assurance and security education and training. WISE WISE WISE 2013 2011 2009. IFIP Advances in Information and Communication Technology (Vol. 406). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-39377-8_29

49. BotPenguin. What is communication automation and how does it work? https://botpenguin.com/blogs/what-is-communication-automation-and-how-does-it-work

50. Salihu, A., & Berisha-Hoti, X. (2019). The effect of IT audit on security incidents. International Journal of Scientific & Technology Research. https://www.researchgate.net/profile/Armend-Salihu/publication/335570152_The_Effect_of_IT_Audit_on_Security_Incidents/links/5d6e044192851c8538889991/The-Effect-of-IT-Audit-on-Security-Incidents.pdf

51. Triplett, W. (2021). Establishing a cybersecurity culture organization. Acta Scientific Computer Sciences, 3(8), 44–49. https://www.researchgate.net/publication/361928960_Establishing_a_Cybersecurity_Culture_Organization

52. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікатної) програми підвищення кваліфікації: Практикум. – Київ: BAITE, 2021. – 106 с.

53. Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. Future Internet, 11(3), 73. https://doi.org/10.3390/fi11030073

54. Charles, H. (2023). Reducing cybersecurity risks in SMEs: Custom training programs to combat human-error vulnerabilities. International Journal of Cybersecurity Education, 5(2), 45–60. https://www.researchgate.net/publication/386400643_Reducing_Cybersecurity_Risks_in_SMEs_Custom_Training_Programs_to_Combat_Human-Error_Vulnerabilities

55. Malmquist, K. (2020). Information security ambassadors' perceptions of peer-led motivation in phishing detection (Doctoral dissertation, Walden University). ProQuest Dissertations & Theses. https://www.proquest.com/openview/4baeaf1751181fe923c5a074f92c11f6/1?pq-origsite=gscholar&cbl=18750&diss=y