МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ МЕТОДИКА ВИКОРИСТАННЯ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ В СУЧАСНИХ КІБЕРАТАКАХ: КЕЙС-ДОСЛІДЖЕННЯ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ”

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

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

_____ Степан КРАВЕЦЬ
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-42

Степан КРАВЕЦЬ
Ім’я, ПРІЗВИЩЕ

Керівник: Юрій ЯКИМЕНКО
к.в.н., доцент Ім’я, ПРІЗВИЩЕ

Рецензент:

Ім’я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Кравцю Степану Володимировичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “ Методика використання соціальної інженерії в сучасних кібератаках: кейс-дослідження та розробка рекомендацій щодо захисту ”,
керівник кваліфікаційної роботи ЯКИМЕНКО Юрій, к.в.н., доцент.
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологійвід “24“ лютого 2025 р. №56.

2. Строк подання кваліфікаційної роботи “20” травня 2025р.

3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека, методи та засоби соціальної інженерії, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
   4.1. Вивчити особливості соціальної інженерії в сучасному кіберпросторі.
   4.2. Дослідити соціально-інженерні кібератаки.
   4.3. Проаналізувати ефективності використання соціальної інженерії в сучасних кібератаках, розробити рекомендації щодо захисту від соціально-інженерних атак.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “11“ березня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2025	
2.	Збір та аналіз літератури.	29.03.2025	
3.	Вивчення особливостей соціальної інженерії в сучасному кіберпросторі.	08.04.2025	
4.	Дослідження соціально-інженерних кібератак.	22.04.2025	
5.	Аналіз ефективності використання соціальної інженерії в сучасних кібератаках та розробка рекомендацій щодо захисту від соціально-інженерних загроз.	08.05.2025	
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2025	
7.	Оформлення роботи.	22.05.2025	
8.	Оформлення презентації.	03.06.2025	
9.	Отримання рецензії на роботу.	03.06.2025	
10.	Захист в ЕК.	__.06.2025	

Здобувач вищої освіти _____ Степан КРАВЕЦЬ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Юрій ЯКИМЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

Направляється здобувач Кравець С.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Методика використання соціальної інженерії в сучасних кібератаках: кейс-дослідження та розробка рекомендацій щодо захисту"

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач КРАВЕЦЬ Степан у кваліфікаційній роботі вивчив особливості соціальної інженерії в сучасному кіберпросторі, дослідив соціально-інженерні кібератаки, проаналізував ефективності використання соціальної інженерії в сучасних кібератаках, розробив рекомендації за темою дослідження.

КРАВЕЦЬ Степан показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на конференції.

Все це дозволяє оцінити кваліфікаційну роботу здобувача КРАВЦЯ Степана на оцінку "добре" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Юрій ЯКИМЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Кравець С.В. допускається до захисту даної роботи в Екзаменаційній комісії.

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

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти КРАВЦЯ Степана
на тему “Методика використання соціальної інженерії в сучасних кібератаках: кейс-дослідження та розробка рекомендацій щодо захисту”

Актуальність. У сучасному цифровому світі, де кіберзагрози стають дедалі витонченішими, соціальна інженерія залишається одним із найбільш ефективних інструментів кібератак. Державні установи, корпорації та приватні особи дедалі частіше стають жертвами атак, що базуються не на технічних уразливостях, а на психологічних методах впливу. З огляду на постійне зростання обсягів кібератак із використанням соціальної інженерії, надзвичайно важливо розробити методи виявлення таких загроз і формувати навички протидії серед користувачів.

Дослідження методів соціальної інженерії та створення практичних рекомендацій щодо захисту є актуальним науково-прикладним завданням у сфері інформаційної безпеки.

Позитивні сторони.

1. У роботі проведено глибокий аналіз основних технік соціальної інженерії та особливостей їх використання у сучасних кібератаках.
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків.
3. Автор опрацював значну джерельну базу: близько 50 публікацій, в тому числі англомовних.
4. За результатами дослідження запропоновано рекомендації щодо підвищення стійкості організацій до атак соціальної інженерії.

Недоліки.

Доцільно було б приділити більше уваги аналізу та класифікації програмних засобів, що дозволяють оцінити ефективність впроваджених заходів із протидії атакам соціальної інженерії, зокрема програм для тестування обізнаності користувачів та проведення симульованих фішингових кампаній.

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

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “добре”, а здобувач КРАВЕЦЬ Степан заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____ _____
підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню методики використання соціальної інженерії в сучасних кібератаках. Робота складається зі вступу, трьох розділів, що містять 5 рисунків і 8 таблиць, висновків і списку використаних джерел із 48 найменувань. Загальний обсяг роботи становить 66 аркушів, з яких 6 аркуші займає список використаних джерел.

Метою роботи є дослідження методик використання соціальної інженерії в сучасних кібератаках, аналіз прикладів застосування та розробка практичних рекомендацій щодо захисту від подібних загроз.

Об'єктом дослідження є процеси реалізації атак соціальної інженерії в контексті інформаційної та кібербезпеки.

Предмет дослідження – особливості методів соціальної інженерії, їх застосування в сучасних кібератаках, а також підходи до протидії цим загрозам.

Методи дослідження. Для вирішення поставленого наукового завдання в роботі використано методи аналізу та синтезу інформації, порівняння, класифікації технік соціальної інженерії, експертного оцінювання ефективності захисних заходів, а також системний підхід до управління інформаційною та кібербезпекою.

Як результат у роботі вивчено особливості соціальної інженерії в сучасному кіберпросторі, досліджено соціально-інженерні кібератаки, проаналізовано ефективності використання соціальної інженерії в сучасних кібератаках, розробив рекомендації за темою дослідження.

Галузь застосування. Розроблені підходи можуть бути використані під час планування та впровадження систем управління інформаційною безпекою підприємств, а також при організації навчальних програм і тренінгів.

Ключові слова: СОЦІАЛЬНА ІНЖЕНЕРІЯ, ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА, УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, ПРОТИДІЯ СОЦІАЛЬНІЙ ІНЖЕНЕРІЇ, НАВЧАННЯ ПЕРСОНАЛУ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

ABSTRACT

The qualification work is devoted to the study of the methodology of using social engineering in modern cyberattacks. The work consists of an introduction, three chapters containing 5 figures and 8 tables, conclusions and the list of references containing 47 items. The total volume of the work is 65 pages, of which 6 pages are occupied by the the list of references.

The purpose of the study is to investigate the methods of using social engineering in modern cyber attacks, analyse examples of application and develop practical recommendations for protection against such threats.

The object the study is the processes of implementing social engineering attacks in the context of information and cybersecurity.

The subject of the study is the peculiarities of social engineering methods, their application in modern cyberattacks, as well as approaches to countering these threats.

Research methods. In order to solve the scientific task, the study uses methods of analysis and synthesis of information, comparison, classification of social engineering techniques, expert assessment of the effectiveness of protective measures, as well as a systematic approach to information and cybersecurity management.

As a result, the work examined the peculiarities of social engineering in modern cyberspace, investigated socially engineering cyberattacks, analysed the effectiveness of social engineering in modern cyberattacks, and developed recommendations on the topic of research.

Field of application. The developed approaches can be used in the planning and implementation of enterprise information security management systems, as well as in the organisation of educational programmes and trainings.

Keywords: SOCIAL ENGINEERING, INFORMATION SECURITY OF AN ENTERPRISE, INFORMATION SECURITY MANAGEMENT, COUNTERACTION TO SOCIAL ENGINEERING, TRAINING OF PERSONNEL IN INFORMATION SECURITY.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ІБ	Інформаційна безпека
КСЗІ	Комплексна система захисту інформації
ПЗ	Програмне забезпечення
ОС	Операційна система
АС	Автоматизована система
АІС	Автоматизована інформаційна система
БД	База даних
СКБД	Система керування базами даних
HTTPS	HyperText Transfer Protocol Secure (захищений протокол передачі гіпертексту)
IP	Internet Protocol (мережевий протокол)
MFA	Multi-Factor Authentication (багатофакторна автентифікація)
JWT	JSON Web Token (токен у форматі JSON)
SQL	Structured Query Language (структурована мова запитів)
SHA	Secure Hash Algorithm (алгоритм хешування)
SSL	Secure Sockets Layer (рівень захищених сокетів)
API	Application Programming Interface (інтерфейс прикладного програмування)
UI	User Interface (користувацький інтерфейс)
UX	User Experience (користувацький досвід)
DevOps	Development and Operations (інтеграція розробки та експлуатації)
DDoS	Distributed Denial of Service (розподілена атака на відмову в обслуговуванні)

ВСТУП

Актуальність теми. У сучасному світі, де державні установи, комерційні компанії та приватні особи стають об'єктами цілеспрямованих кібератак, питання забезпечення інформаційної безпеки є особливо актуальним. З огляду на стрімкий розвиток IT-сфери, інформаційні ризики та загрози також невпинно еволюціонують. Особливо небезпечним чинником стає соціальна інженерія — техніка впливу на користувачів з метою отримання несанкціонованого доступу до інформаційних ресурсів. У зв’язку з цим надзвичайно важливо формувати культуру безпеки серед персоналу підприємств, надаючи працівникам необхідні знання і навички для виявлення та запобігання атакам соціальної інженерії. Інноваційні методики навчання персоналу здатні підтримувати високий рівень обізнаності, враховувати актуальні тенденції розвитку загроз і, як наслідок, підвищувати загальний рівень інформаційної безпеки організації.

З огляду на зазначене дослідження методик використання соціальної інженерії в сучасних кібератаках є актуальним науковим завданням.

Мета роботи полягає у дослідженні методик використання соціальної інженерії в сучасних кібератаках, аналізі прикладів застосування та розробці практичних рекомендацій щодо захисту від подібних загроз.

Об’єкт дослідження – процеси реалізації атак соціальної інженерії в контексті інформаційної та кібербезпеки.

Предмет дослідження – особливості методів соціальної інженерії, їх застосування в сучасних кібератаках, а також підходи до протидії цим загрозам.

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

1. Вивчити особливості соціальної інженерії в сучасному кіберпросторі.

2. Дослідити соціально-інженерні кібератаки.

3. Проаналізувати ефективності використання соціальної інженерії в сучасних кібератаках, розробити рекомендації щодо захисту від соціально-інженерних атак.

Методи дослідження. Для вирішення поставленого наукового завдання в

роботі використано методи аналізу та синтезу інформації, порівняння, класифікації технік соціальної інженерії, експертного оцінювання ефективності захисних заходів, а також системний підхід до управління інформаційною та кібербезпекою.

Практичне значення одержаних результатів. Результати дослідження можуть бути використані для обґрунтованого вибору методів і засобів підвищення обізнаності персоналу щодо загроз соціальної інженерії. Застосування розроблених підходів дозволить інтегрувати програми навчання й тестування співробітників як невід'ємний елемент системи управління інформаційною безпекою, адаптуючи їх до цілей бізнесу, можливостей та ресурсів конкретного підприємства. Це сприятиме зниженню ризиків успішних атак соціальної інженерії та підвищенню загальної стійкості організації до інформаційних загроз.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції "Стратегії кіберстійкості: управління ризиками та безперервність бізнесу" 27 лютого 2025 року.

Розділ 1 СОЦІАЛЬНА ІНЖЕНЕРІЯ В СУЧАСНОМУ КІБЕРПРОСТОРІ

Методи атак на інформаційні системи стрімко еволюціонують. Однією з найнебезпечніших і водночас найефективніших загроз є соціальна інженерія — технологія впливу на людей з метою отримання доступу до конфіденційної інформації без застосування технічних засобів злому. Використання людського фактора як слабкої ланки в системі безпеки дозволяє зловмисникам обходити навіть найскладніші технічні захисти.

1.1 Поняття соціальної інженерії та її місце в інформаційній безпеці

Інформаційна безпека стає одним із найважливіших чинників захисту державних, корпоративних та особистих інтересів. Традиційні методи кібератак, що орієнтовані на технічні уразливості, дедалі частіше доповнюються або навіть замінюються методами соціальної інженерії. Використання людського фактора як найслабшої ланки у системах безпеки зумовлює високий рівень небезпеки таких атак.

Соціальна інженерія — це набір методів впливу на людей з метою отримання конфіденційної інформації, доступу до систем або ресурсів, обходу засобів захисту без застосування технічного злому. Вона базується на психологічних прийомах маніпулювання свідомістю та поведінкою людини.

Зловмисники використовують соціальну інженерію для того, щоб обійти захисні бар'єри, експлуатуючи довіру, страх, необізнаність або інші емоційні реакції своїх жертв. Серед найбільш поширених прикладів — фішинг, телефонне шахрайство (vishing), маніпулятивне спілкування в соціальних мережах та інші методи (див табл. 1.1).

Соціальна інженерія охоплює різноманітні техніки, кожна з яких має свої особливості, цілі та підходи до впливу на жертву [1].

Таблиця 1.1

Порівняльна характеристика методів соціальної інженерії

Критерій	Фішинг	Спірфішинг	Претекстинг	Бейтинг	Tailgating
Визначення	Масові розсилки для викрадення даних	Цільовий фішинг для конкретних осіб/організацій	Створення вигаданого сценарію для отримання інформації	Використання цікавої приманки (наприклад, заражені USB)	Фізичне проникнення разом із справжнім співробітником
Канал атаки	Email, месенджери, соцмережі	Персоналізовані email/SMS	Телефонні дзвінки, особиста комунікація	Фізичні носії, онлайн-приманки	Фізичний доступ
Ціль	Масові споживачі	Високопосадовці, фінансові служби	Адміністративний персонал, служби підтримки	Любопитні співробітники	Охорона, рецепція
Складність	Низька (автоматизація)	Висока (необхідність розвідки)	Середня (акторська майстерність)	Низька-середня	Залежить від рівня безпеки
Ефективність	3-5% (масові), до 30% (цільові)	До 45%	60-80% для кваліфікованих атакерів	30-40% (залежить від цікавості приманки)	50-70% у слабко захищених організацій
Типова тривалість	Хвилини-години	Дні-тижні (підготовка)	Години-дні	Хвилини-години	Секунди-хвилини
Приклад	Лист "Про терміновий скидання пароля"	Лист "Про зарплатні нарахування" від імені HR	Дзвінок "з техпідтримки" з проханням пароля	Підкинутий USB із написом "Зарплатні_2023"	Проходження через турнікет за співробітником
Захист	Фільтрація спаму, навчання співробітників	DMARC, двофакторна аутентифікація	Політика перевірки ідентичності	Блокування USB-портів, навчання	Системи контролю доступу, відеоспостереження
Вразливі групи	Недосвідчені користувачі	Фінансові служби, HR	Служби підтримки, адміністратори	Допитливі співробітники	Охорона, рецепціоністи

Фішинг є однією з найпоширеніших технік соціальної інженерії. Він полягає у надсиланні підроблених електронних листів, повідомлень у месенджерах або SMS, які імітують офіційні звернення від відомих організацій, банків або державних установ. Метою фішингу є переконати жертву надати конфіденційну інформацію, таку як логіни, паролі або дані банківських карт.

Фішингові кампанії можуть бути масовими або цілеспрямованими та часто супроводжуються використанням фальшивих вебсайтів, створених для збору введеної користувачем інформації.

Спірфішинг є більш витонченою формою фішингу, яка спрямована на конкретних осіб або організації. Нападники ретельно збирають інформацію про своїх цільових жертв, включаючи їхні професійні зв'язки, інтереси та звички. Це дозволяє створити персоналізовані повідомлення, які виглядають максимально правдоподібно. Спірфішинг часто використовується у промисловому шпигунстві та проти високопоставлених посадовців компаній.

Претекстинг передбачає створення вигаданого сценарію або історії для того, щоб переконати жертву розкрити конфіденційні дані або надати доступ до ресурсів. Наприклад, зловмисник може видавати себе за співробітника IT-відділу компанії, який потребує облікові дані для "проведення технічного обслуговування". Ефективність претекстингу залежить від здатності нападника бути переконливим та швидко реагувати на питання або підозри жертви.

Бейтинг базується на експлуатації цікавості або жадібності жертви. Зловмисник пропонує щось привабливе, наприклад безкоштовний подарунок, музику, фільми або іншу винагороду, в обмін на виконання певних дій, що відкривають доступ до системи. У фізичному варіанті бейтингу нападники можуть залишати заражені USB-накопичувачі у громадських місцях, сподіваючись, що хтось підключить їх до корпоративної мережі.

Tailgating (або "підсадка") передбачає фізичне проникнення до захищеної зони підприємства за допомогою обману або використання ввічливості співробітників. Наприклад, зловмисник може наблизитися до будівлі разом зі співробітником і ввічливо попросити його притримати двері, видаючи себе за забудькуватого колегу. Tailgating є серйозною загрозою для фізичної безпеки, оскільки дозволяє отримати прямий доступ до внутрішніх систем організації.

Кожна із цих технік демонструє, наскільки різноманітними можуть бути способи маніпуляції людьми задля досягнення злочинних цілей. Розуміння природи кожної з них є ключовим для розробки ефективних заходів захисту та

навчання персоналу правильно реагувати на підозрілі ситуації.

Методи соціальної інженерії постійно змінюються і вдосконалюються. З розвитком інформаційних технологій та соціальних мереж відкрилися нові можливості для атак. Зловмисники активно аналізують профілі користувачів у соціальних мережах, що дозволяє створювати більш переконливі сценарії атак.

Ефективність соціальної інженерії у великій мірі пояснюється кількома чинниками, які комплексно впливають на сприйняття користувачами інформаційних загроз. Однією з основних причин є низький рівень обізнаності користувачів щодо сучасних кіберзагроз. Багато співробітників не мають уявлення про сучасні методи атак, не розпізнають ознаки фішингу, не підозрюють про можливість маніпуляції через соціальні мережі або навіть через телефонні дзвінки. У результаті їхня необізнаність створює сприятливі умови для зловмисників, які можуть легко скористатися відсутністю настороженості та базових навичок інформаційної безпеки.

Іншою важливою причиною є психологічна вразливість людини. Довіра, страх, цікавість або бажання допомогти — це природні людські якості, які часто стають об'єктом експлуатації у процесі атак соціальної інженерії. Наприклад, повідомлення про "термінову проблему з обліковим записом" активує страх втрати доступу і змушує користувача діяти імпульсивно. Заклики до співчуття або надання допомоги можуть викликати бажання негайно реагувати без належної перевірки джерела інформації. Ці психологічні механізми активно використовуються в атаках для того, щоб змусити людину виконати певні дії всупереч здоровому глузду чи внутрішнім підозрам.

Відсутність належної культури інформаційної безпеки в організаціях також сприяє успіху соціальної інженерії. Якщо компанія не впроваджує регулярних тренінгів, не створює чітких інструкцій щодо обробки підозрілих запитів і не підтримує постійної обізнаності працівників, то навіть наявність сучасних технічних засобів захисту не гарантує безпеки. Культура безпеки повинна бути невід’ємною частиною корпоративної політики, яка передбачає не лише правила, але й активне залучення співробітників до процесу виявлення та

запобігання кіберзагрозам [2].

Недостатній контроль і моніторинг поведінки користувачів є ще одним фактором, що робить соціальну інженерію ефективною. Багато компаній обмежуються технічними рішеннями, не аналізуючи при цьому поведінкові аспекти використання інформаційних систем. Відсутність механізмів виявлення нетипової активності користувачів, наприклад, незвичайних запитів на доступ до певної інформації або зміни звичних моделей використання системи, дозволяє атакам залишатися непоміченими до моменту нанесення шкоди. Саме тому сучасні підходи до інформаційної безпеки повинні поєднувати технічний захист із ретельним аналізом поведінки користувачів.

Роль соціальної інженерії у сучасних кібератаках підкреслює необхідність комплексного підходу до забезпечення інформаційної безпеки. Необхідно поєднувати технологічні рішення із активною роботою з людським фактором, забезпечувати постійне підвищення рівня обізнаності та формувати правильні поведінкові стереотипи серед персоналу. Розуміння цих принципів дає змогу не лише знизити ризики атак соціальної інженерії, а й підвищити загальну стійкість організації до інформаційних загроз.

Інформаційна безпека традиційно спирається на три основні компоненти: технічні засоби захисту, організаційні заходи та людський фактор. Соціальна інженерія безпосередньо впливає на останній компонент, роблячи його критично важливим.

Організації повинні враховувати загрози соціальної інженерії під час розробки політик безпеки, навчання персоналу, створення процедур реагування на інциденти. Неврахування людського чинника суттєво знижує ефективність усієї системи захисту.

Ефективна протидія соціальній інженерії вимагає застосування комплексу заходів, спрямованих на попередження, виявлення та нейтралізацію спроб маніпулювання співробітниками. Одним із ключових напрямів є постійне навчання та підвищення обізнаності працівників. Безперервна освітня діяльність повинна включати тренінги, семінари, інформаційні кампанії, спрямовані на

ознайомлення співробітників з актуальними методами атак соціальної інженерії та способами їх розпізнавання. Працівники мають не лише теоретично знати про загрози, а й бути здатними миттєво розпізнавати спроби шахрайства у реальних умовах. Тренування повинні охоплювати моделювання реальних сценаріїв атак для розвитку практичних навичок реагування [3].

Іншим важливим заходом є регулярне проведення тестів на фішинг та інших симульованих атак. Проведення імітаційних фішингових кампаній дозволяє виявити рівень підготовленості персоналу, а також ідентифікувати співробітників, які потребують додаткового навчання. Такі тести мають бути частиною загальної програми забезпечення інформаційної безпеки та супроводжуватися зворотним зв'язком і аналізом допущених помилок.

Важливо також розробити чіткі політики і процедури інформаційної безпеки, які окреслюють правила поведінки у випадку виявлення підозрілих запитів або подій. Кожен співробітник має знати, до кого звернутися у разі виникнення підозри, як правильно зафіксувати інцидент і які дії потрібно вжити для запобігання поширенню загрози. Наявність зрозумілих і доступних інструкцій знижує ризик хаотичних дій і мінімізує наслідки успішних атак.

Запровадження багатофакторної автентифікації є ще одним критично важливим елементом протидії соціальній інженерії. Використання декількох рівнів перевірки особистості значно ускладнює завдання зловмисникам, навіть якщо їм вдається викрасти первинні облікові дані користувача. Багатофакторна автентифікація може включати комбінацію пароля, біометричних даних, одноразових кодів із мобільних додатків або токенів безпеки [4].

Моніторинг аномальної поведінки користувачів є ще одним ефективним інструментом виявлення спроб соціальної інженерії. Аналітика поведінки дозволяє виявити відхилення від нормального патерну дій співробітників, наприклад, незвичні запити на доступ до ресурсів, спроби завантаження великої кількості конфіденційних файлів або підключення до корпоративної мережі з незвичних геолокацій. Системи моніторингу повинні не лише фіксувати такі інциденти, але й оперативно інформувати відповідальних осіб для негайного

реагування.

Комплексна реалізація вищенаведених заходів дозволяє суттєво знизити ризики успішного застосування методів соціальної інженерії проти організації. Протидія повинна бути не одноразовою кампанією, а постійним процесом удосконалення культури інформаційної безпеки, який включає як технологічні інновації, так і розвиток навичок критичного мислення серед співробітників. Зрозуміло, що зловмисники також постійно вдосконалюють свої підходи, тому захист має розвиватися динамічно, із залученням сучасних засобів аналізу загроз та реагування на інциденти.

Одним із відомих прикладів реальної атаки із використанням методів соціальної інженерії є інцидент, що стався у 2011 році з компанією RSA Security. Атака розпочалася з фішингового листа, надісланого співробітникам компанії. Лист мав невинний вигляд і виглядав як повідомлення від внутрішнього відділу кадрів із темою "План роботи на поточний місяць" [5]. Декілька співробітників відкрили вкладений Excel-файл, що містив шкідливий код. Унаслідок цього зловмисники змогли отримати доступ до систем компанії та викрасти критично важливу інформацію про технології автентифікації SecurID, які широко використовувалися для захисту урядових та корпоративних мереж. Витік цієї інформації призвів до серйозних наслідків, включаючи масштабні атаки на оборонні підрядники уряду США. Цей випадок продемонстрував, наскільки серйозними можуть бути наслідки навіть однієї успішної атаки соціальної інженерії та підкреслив необхідність підвищення обізнаності співробітників про кіберзагрози.

Інший яскравий приклад стосується так званого "whaling" — таргетованих фішингових атак, спрямованих на керівників вищої ланки великих компаній. Ці атаки відрізняються високим рівнем персоналізації і вимагають ретельного збору інформації про цільову особу [6]. Нападники створюють спеціально розроблені листи, які можуть виглядати як офіційні запити від партнерів або внутрішні повідомлення від інших керівників. Часто такі листи містять прохання терміново переказати кошти на певний рахунок або надати доступ до конфіденційної

інформації. Відомі випадки, коли внаслідок таких атак компанії зазнавали збитків на десятки мільйонів доларів. Наприклад, компанія Ubiquiti Networks повідомила про втрату 46,7 мільйонів доларів унаслідок атаки, в якій зловмисники через підроблені листи від імені керівників виманили переказ коштів на сторонні рахунки. Інший приклад — атака на компанію Mattel, де внаслідок фальшивого запиту на переказ 3 мільйонів доларів гроші були переведені на рахунок у Китаї. Хоча компанії вдалося частково відновити кошти, цей випадок продемонстрував вразливість навіть добре захищених організацій перед соціально інженерними атаками [7].

Ці приклади подані у вигляді табл. 1.2 та ілюструють, що навіть великі корпорації, які інвестують значні ресурси в технічний захист, можуть стати жертвами атак через людський фактор. Зловмисники ретельно вивчають поведінку, стиль спілкування та бізнес-процеси компанії для створення максимально правдоподібних сценаріїв обману. Саме тому одним із ключових напрямів забезпечення інформаційної безпеки залишається розвиток культури кібербезпеки серед персоналу всіх рівнів. Без належної обізнаності навіть найсучасніші технічні засоби можуть бути обійдені шляхом маніпуляції людьми.

Таблиця 1.2

Аналіз реальних кейсів соціально-інженерних атак

Кейс	**Рік**	**Тип атаки**	**Метод**	**Деталі впровадження**	**Наслідки**	**Уроки/Запобіжні заходи**
Атака на RSA Security	2011	Цільовий фішинг	Фішинговий лист з Excel-вкладенням	Лист від імені відділу кадрів з темою "План роботи на поточний місяць"	Викрадено дані про SecurID, атаки на оборонних підрядникі в США	Необхідність: - Фільтрації вкладень - Сегментації мереж - Підвищення обізнаності
Ubiquiti Networks	2015	Whaling (BEC)	Підроблені листи від керівництва	Імітація офіційних запитів на переказ коштів	Втрата $46.7 млн	Впровадження: - Двофакторної верифікації платежів - Фізичного підтвердження транзакцій

Продовження таблиці 1.2

Mattel	2016	Whaling (BEC)	Фальшиві фінансові запити	Листи з проханням термінового переказу	Втрата $3 млн (частково відновлено)	Політики: - Верифікації великих транзакцій - Обмеження повноважень

Соціальна інженерія є однією з найсерйозніших загроз для інформаційної безпеки сучасних організацій. Її ефективність зумовлена тим, що вона експлуатує людські слабкості, які складно усунути технічними засобами. Розуміння сутності соціальної інженерії, її методів та шляхів протидії є необхідною умовою для забезпечення надійного захисту інформаційних ресурсів.

Формування культури інформаційної безпеки, регулярне навчання персоналу та інтеграція заходів з протидії соціальній інженерії в загальну систему безпеки є пріоритетними завданнями для всіх організацій, які прагнуть мінімізувати ризики в кіберпросторі.

1.2 Основні типи атак з використанням соціальної інженерії

Соціальна інженерія набуває дедалі більшої популярності серед зловмисників завдяки своїй ефективності та складності виявлення. На відміну від традиційних технічних атак, методи соціальної інженерії орієнтовані на експлуатацію людських слабкостей і психологічних особливостей. Атаки цього типу можуть відбуватися через різні канали комунікації та використовувати широкий спектр сценаріїв, залежно від мети і специфіки цільової аудиторії.

Для успішної протидії таким загрозам необхідно розуміти класифікацію атак соціальної інженерії, їх основні види та чинники, що сприяють їх успішному проведенню. Вивчення типових прикладів і моделей атак дозволяє краще оцінити ризики та розробити ефективні заходи захисту як на рівні окремих користувачів, так і на рівні організацій.

Атаки соціальної інженерії можуть здійснюватися через різні канали

комунікації, що відкриває перед зловмисниками широкі можливості для впливу на цільові аудиторії [8]. Класифікація атак за каналами взаємодії дозволяє краще розуміти механізми реалізації загроз та формувати відповідні заходи безпеки. Розглянемо основні канали, через які здійснюються атаки соціальної інженерії.

Електронна пошта є одним із найпопулярніших каналів для проведення атак соціальної інженерії. Основним видом загрози тут є фішинг — надсилання підроблених листів, які імітують офіційні повідомлення від банків, сервісів електронної комерції, державних установ тощо. Такі листи часто містять посилання на фальшиві вебсайти або вкладення з шкідливим програмним забезпеченням.

Фішингові листи можуть бути як масовими, спрямованими на широку аудиторію, так і таргетованими (спірфішинг), орієнтованими на конкретних осіб чи організації. Останні зазвичай містять персоналізовану інформацію, що підвищує ймовірність успішного обману. Електронна пошта також використовується для розповсюдження шкідливих програм (малварі), зокрема через прикріплені документи або архіви.

Ще одним розповсюдженим каналом для атак соціальної інженерії є телефонні дзвінки, що отримали назву "вішинг" (від англ. "voice phishing"). Зловмисники телефонують своїм жертвам, представляючись співробітниками банків, служб безпеки, державних органів або навіть колегами по роботі.

Під час таких дзвінків вони намагаються змусити людину розкрити конфіденційну інформацію, таку як номери платіжних карток, коди підтвердження з SMS, паролі або іншу важливу інформацію. Зловмисники часто використовують техніку нагнітання терміновості, створюючи відчуття небезпеки або необхідності негайної дії, щоб жертва не мала часу на обдумування.

Смішинг (від англ. "SMS phishing") є різновидом фішингу, який здійснюється через текстові повідомлення. Жертва отримує SMS-повідомлення із закликом здійснити певні дії: перейти за посиланням, оновити обліковий запис, верифікувати банківські дані тощо.

Посилання, що містяться в таких повідомленнях, зазвичай ведуть на фальшиві сайти, де жертву просять ввести особисті дані або завантажити шкідливі файли. У деяких випадках смішинг використовується для поширення мобільних троянів або шпигунських програм.

Соціальні мережі стають дедалі популярнішим середовищем для атак соціальної інженерії. Зловмисники створюють фальшиві профілі, імітують знайомих жертви або відомих осіб для встановлення довірчих відносин. Зібрана через соціальні мережі інформація про особисте життя, інтереси, звички або професійні зв'язки може бути використана для створення більш переконливих атак.

Через соціальні мережі також розповсюджуються шкідливі посилання, фальшиві конкурси, пропозиції роботи або інші схеми, що спонукають користувача до розкриття конфіденційної інформації або встановлення небезпечного програмного забезпечення.

Розглянемо основні канали, через які здійснюються атаки соціальної інженерії (див. табл.1.3).

Таблиця 1.3

Основні типи атак з використанням соціальної інженерії

Тип атаки	Канал атаки	Методика	Ціль	Приклад	Захист
Електронна пошта	Email	Масові розсилки з підробленими повідомленнями	Широке коло користувачів	Лист "Про термінове оновлення паролю" з підробленою адресою банку	Фільтрація спаму, перевірка домену, навчання співробітників
Фішингові листи	Email, месенджери	Персоналізовані листи з посиланнями на фальшиві сайти	Конкретні організації/особи	Лист від "служби підтримки" з проханням оновити дані кредитної картки	Двофакторна аутентифікація, перевірка SSL-сертифікатів

Продовження таблиці 1.3

Телефонні дзвінки	Телефон, VoIP	Претекстинг (імітація служби підтримки, банку тощо)	Співробітники, клієнти	Дзвінок "з техпідтримки" з проханням назвати пароль	Політика не розголошення інформації, кодові слова
Смішинг	SMS	Текстовиі повідомлення з посиланнями або підступними проханнями	Власники мобільних пристроїв	SMS "Ваша посилка зачекала на мито, перейдіть за посиланням для оплати"	Блокування підозрілих номерів, перевірка офіційних джерел
Соціальні мережі	Facebook, LinkedIn тощо	Створення фальшивих профілів, імітація знайомих, цікаві пропозиції	Користувачі соцмереж	Повідомлення від "друга" з проханням перейти на сайт або скачати файл	Уважність до незнайомих повідомлень, перевірка профілів

Соціальна інженерія не обмежується лише віртуальним простором. Зловмисники можуть використовувати фізичні методи проникнення до захищених приміщень підприємств. Tailgating (підсадка) передбачає фізичне входження в будівлю, слідуючи за співробітником, який відкриває двері з картковим доступом.

Baiting (підсадка через спокусу) у фізичному варіанті може включати залишення заражених USB-накопичувачів у громадських місцях, сподіваючись, що хтось із працівників підключить їх до корпоративного комп'ютера, відкривши доступ до мережі організації.

Зловмисники часто комбінують кілька каналів взаємодії для підвищення ефективності атак. Наприклад, після надсилання фішингового листа вони можуть зателефонувати жертві для підтвердження отримання листа, що збільшує рівень довіри. Такі багатоетапні атаки значно складніше виявити та нейтралізувати.

Сучасні атаки соціальної інженерії охоплюють широкий спектр методів, кожен з яких має свої особливості та цільові сценарії застосування. Розгляд найбільш поширених видів атак дозволяє краще розуміти природу загроз і розробляти відповідні заходи протидії.

Фішинг залишається одним із найпоширеніших і найефективніших видів атак соціальної інженерії. Його метою є викрадення конфіденційної інформації, такої як логіни, паролі, дані платіжних карток. Фішингові повідомлення зазвичай імітують офіційні листи від банків, служб технічної підтримки, поштових сервісів або інших авторитетних джерел. Вони містять посилання на фальшиві сайти, що візуально копіюють справжні портали, де користувачі вводять свої облікові дані.

Фішинг може бути як масовим (розсилка однакових листів великій кількості адресатів), так і цілеспрямованим (спірфішинг), де атака орієнтована на конкретних осіб або організації.

Спірфішинг (англ. spear phishing) є спеціалізованим видом фішингу, який націлений на окремих осіб або невеликі групи в межах організації. Зловмисники ретельно вивчають своїх жертв, використовуючи інформацію з відкритих джерел: профілі у соціальних мережах, корпоративні сайти, новини тощо.

Фішингові листи у спірфішингу є персоналізованими, що значно підвищує ймовірність довіри з боку отримувача. Часто такі листи містять інформацію, що стосується поточних проєктів, посадових обов’язків або особистих інтересів жертви.

Вішинг (англ. voice phishing) полягає у здійсненні телефонних дзвінків жертвам із метою викрадення конфіденційної інформації. Зловмисники часто видають себе за співробітників банків, правоохоронних органів або технічної підтримки.

Успіх вішингу базується на створенні ситуації стресу або терміновості. Наприклад, жертві повідомляють про "підозрілу активність" на банківському рахунку і пропонують "верифікувати" дані для захисту коштів.

Смішинг (англ. SMS phishing) — це атаки через текстові повідомлення. Зловмисники надсилають SMS із закликом терміново перейти за посиланням, перевірити рахунок, оновити пароль або отримати "виграш". Перехід за таким посиланням зазвичай веде на фальшивий сайт або активує завантаження шкідливого програмного забезпечення на мобільний пристрій.

Бейтинг полягає у використанні привабливих пропозицій або спокусливих обіцянок для того, щоб змусити жертву виконати певні дії. Це можуть бути оголошення про безкоштовні подарунки, фальшиві акції або залишені у публічних місцях USB-накопичувачі із шкідливим ПЗ [9].

Жертва, зацікавившись пропозицією або знахідкою, встановлює контакт із атакуючим середовищем, що призводить до компрометації пристрою або мережі.

Претекстинг — це створення фальшивого сценарію або передісторії для здобуття довіри жертви. Нападник вигадує обґрунтовану причину для отримання конфіденційної інформації або доступу до ресурсів. Наприклад, він може представитися співробітником служби підтримки, який "проводить технічне обслуговування" системи.

Претекстинг вимагає від зловмисника добре розробленого сценарію та вміння швидко реагувати на запитання жертви.

Тайлгейтинг (англ. tailgating) відноситься до фізичних атак соціальної інженерії. Зловмисник проникає на об'єкт, що охороняється, слідуючи за співробітником, який відкриває двері за допомогою перепустки. Нападники часто користуються ввічливістю або неуважністю людей, які несвідомо допомагають їм обійти фізичні системи контролю доступу.

Ефективність атак соціальної інженерії значною мірою визначається комплексом факторів, які сприяють їх успішному проведенню. Розуміння цих факторів є критично важливим для розробки заходів протидії та формування стійкої культури інформаційної безпеки в організаціях.

Одним із ключових чинників успішності атак є експлуатація базових психологічних механізмів поведінки людини. Зловмисники ретельно використовують такі тригери, як страх, терміновість, довіра до авторитету, цікавість, бажання допомогти або отримати вигоду.

Створення атмосфери терміновості (наприклад, загроза блокування рахунку або термінова необхідність підтвердження інформації) змушує людину діяти імпульсивно, без належного аналізу ситуації. Використання довіри до

відомих брендів або посадових осіб (наприклад, фальшиві листи від банків чи керівників) також значно підвищує ефективність атак [10].

Брак знань і розуміння сучасних кіберзагроз серед користувачів є ще одним важливим чинником, який сприяє успішності атак. Багато співробітників організацій не вміють розпізнавати ознаки фішингових листів, не знають правил безпечної роботи в Інтернеті або недостатньо уважні до процедур автентифікації.

Відсутність базових навичок кібергігієни робить користувачів легкою мішенню для соціальних інженерних атак. Саме тому постійне навчання і тренування персоналу має стати обов'язковим елементом політики інформаційної безпеки.

Люди, як правило, мають схильність довіряти іншим, особливо коли отримують повідомлення, що виглядають офіційно або відомо. Зловмисники активно експлуатують цю довіру, створюючи правдоподібні сценарії взаємодії.

Неуважність і звичка виконувати рутинні дії без обмірковування також грають на руку нападникам. Наприклад, співробітник може не звернути уваги на змінену адресу відправника листа або незвичайне посилання, якщо послання виглядає знайомо.

Організації, що не мають чітких правил поведінки у випадку підозрілих ситуацій, є більш вразливими до атак соціальної інженерії. Невизначеність у діях співробітників при отриманні незвичних запитів або листів призводить до того, що багато хто діє на власний розсуд, що часто грає на користь зловмисників.

Відсутність політик перевірки справжності запитів, недосконалі процедури обробки конфіденційної інформації або слабкі системи ідентифікації співрозмовників створюють додаткові вразливості.

Зловмисники активно використовують відкриті джерела для збору даних про своїх жертв. Соціальні мережі, корпоративні сайти, новини, бази даних – усе це дає нападникам детальне уявлення про життєві обставини, звички, професійні обов'язки й контакти цільової особи.

На основі зібраної інформації зловмисники створюють персоналізовані сценарії атак, що суттєво підвищує їхню успішність [11]. Знання специфіки

роботи компанії дозволяє, наприклад, підробити внутрішній службовий лист так, що навіть уважний співробітник не відразу запідозрить обман.

Одноетапна система входу за допомогою лише логіна і пароля значно підвищує ризик компрометації акаунтів у разі успішної атаки. Відсутність багатофакторної автентифікації дозволяє зловмисникам одразу отримати доступ до облікових записів після викрадення облікових даних.

Впровадження додаткових рівнів захисту, таких як підтвердження входу через SMS, біометрію або спеціальні токени, значно ускладнює використання вкрадених даних навіть у разі їх компрометації.

Атаки з використанням соціальної інженерії є одними з найбільш небезпечних і підступних методів кіберзлочинності, оскільки вони маніпулюють людським фактором для досягнення злочинних цілей. Основні типи таких атак, як фішинг, пре-текстинг, скамінг, та інші, показують, наскільки важливим є підвищення рівня обізнаності користувачів щодо ризиків, що виникають через людську наївність та довірливість. Враховуючи постійне вдосконалення методів соціальної інженерії, організації повинні активно працювати над розвитком культур кібербезпеки та регулярним навчанням своїх співробітників для мінімізації можливості успішних атак.

Висновки до розділу 1

Підкреслено важливість цього явища в контексті сучасної кібербезпеки. Соціальна інженерія, як метод маніпулювання людським фактором для отримання несанкціонованого доступу до інформації або ресурсів, займає ключове місце в стратегії забезпечення інформаційної безпеки. Атаки, що використовують соціальну інженерію, часто є більш ефективними, ніж технічні засоби зломів, оскільки вони експлуатують психологічні вразливості людей.

Визначено основні типи таких атак, зокрема фішинг, пре-текстинг, скамінг та інші, що демонструють різноманітність підходів до маніпуляцій з метою досягнення злочинних цілей. Оскільки ці атаки здатні обійти технічні

засоби захисту, зокрема через експлуатацію емоційної або психологічної вразливості користувачів, їхнє розуміння та протидія мають вирішальне значення для підвищення рівня безпеки організацій.

Отже, для ефективної боротьби з такими загрозами необхідно не лише вдосконалювати технічні засоби захисту, але й активно працювати над підвищенням обізнаності користувачів щодо ризиків, пов'язаних з соціальною інженерією, а також розробляти комплексні стратегії профілактики, що включають навчання і регулярні тренінги персоналу.

Розділ 2 КЕЙС-ДОСЛІДЖЕННЯ СОЦІАЛЬНО-ІНЖЕНЕРНИХ КІБЕРАТАК

Розвиток технологій та зростання рівня цифровізації в умовах глобалізованого світу значно ускладнили проблеми кібербезпеки. Незважаючи на значні досягнення у галузі технічного захисту, сучасні кібератаки все частіше спрямовані не лише на уразливості в програмному забезпеченні чи апаратних засобах, але й на людський фактор. Соціально-інженерні атаки, що базуються на маніпуляції поведінкою людей, здатні обійти навіть найсучасніші системи безпеки, адже їхня основна мета — експлуатація емоційних та психологічних вразливостей.

Зростаюча кількість успішних атак, що застосовують методи соціальної інженерії, вимагає глибокого аналізу практичних випадків і прикладів реальних інцидентів. Вивчення таких кейсів дозволяє не лише зрозуміти механізми дії цих атак, але й виявити найбільш ефективні способи їх профілактики та захисту. У цьому розділі будуть представлені детальні кейс-дослідження соціально-інженерних кібератак, що сталися в різних сферах діяльності, що дозволяє на конкретних прикладах розглянути типові стратегії нападників, а також фактори, що сприяють успіху або провалу таких атак.

Аналіз цих випадків допоможе визначити ключові уроки, які необхідно враховувати при розробці методик захисту від соціальної інженерії та підвищення рівня обізнаності користувачів щодо потенційних загроз.

2.1 Розробка методики використання соціальної інженерії в сучасних кібератаках

Соціальна інженерія є одним із найбільш поширених методів кіберзлочинів, оскільки вона експлуатує слабкі місця людської психології, а не технічні вразливості систем. У цьому розділі розглядається методика використання соціальної інженерії в сучасних кібератаках, включаючи аналіз

досвіду кейс-досліджень, огляд реальних інцидентів та практику застосування інструментів і технік.

Життєвий цикл соціально-інженерної атаки представлений на рис.2.1

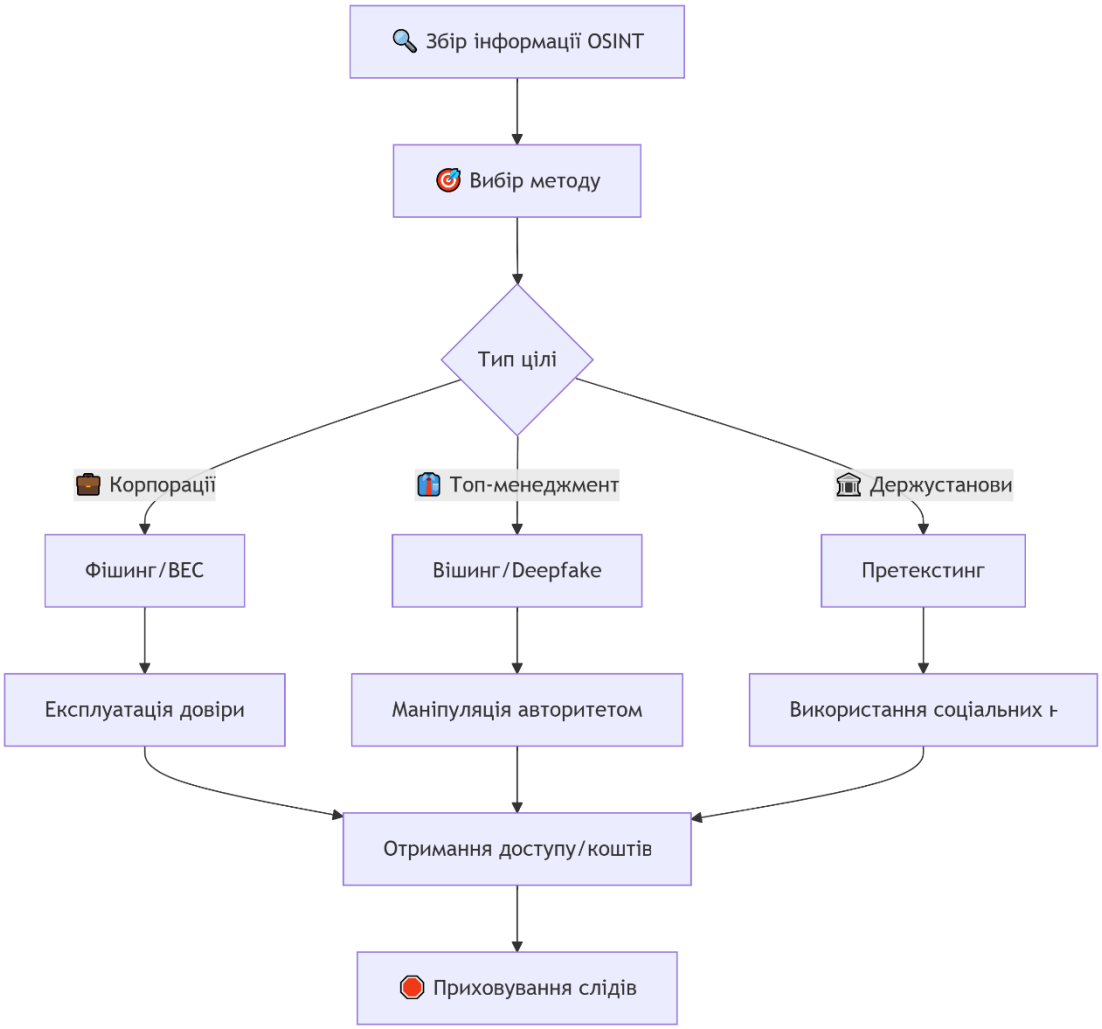

Рис. 2.1 Життєвий цикл соціально-інженерної атаки

Кейс-дослідження є важливим інструментом для вивчення соціально-інженерних атак, оскільки вони дозволяють проаналізувати реальні сценарії, методи злочинців та ефективність контрзаходів. Дослідження соціальної інженерії часто базуються на експериментах, таких як фішинг-тестування, претекстинг або візуальне соціальне інженерство.

Одним із ключових аспектів кейс-досліджень є визначення психологічних тригерів, які використовують зловмисники. Наприклад, у дослідженні, проведеному Verizon у 2023 році, було встановлено, що понад 90% успішних

фішинг-атак спиралися на почуття терміновості або авторитету [12]. Це підтверджує, що соціальні інженери ефективно маніпулюють емоціями жертв.

Крім того, важливим елементом кейс-досліджень є оцінка ефективності навчання співробітників. Дослідження компанії KnowBe4 показали, що регулярне тренування з кібербезпеки знижує ймовірність успішного фішингу на 60-70% [13]. Таким чином, аналіз кейсів дозволяє не лише вивчити тактики злочинців, але й розробити ефективні стратегії профілактики.

Соціально-інженерні кібератаки стають дедалі складнішими та різноманітнішими, що підтверджується численними реальними інцидентами. Аналіз таких кейсів дозволяє виявити ключові тенденції, методи злочинців та слабкі місця в системах безпеки організацій. У цьому підрозділі розглядаються найбільш показові випадки соціально-інженерних атак останніх років, їхній вплив на бізнес та суспільство, а також уроки, які можна з них винести.

Одним із найгучніших прикладів соціальної інженерії стала атака на Twitter у липні 2020 року [14]. Група злочинців, використовуючи техніку телефонного претекстингу, змогла обманом отримати доступ до внутрішньої системи адміністрування акаунтів. Вони подзвонили співробітникам Twitter, видаючи себе за IT-спеціалістів, і переконали їх розкрити дані для входу. В результаті зловмисники отримали контроль над акаунтами відомих осіб (Барака Обами, Ілона Маска, Білла Гейтса) та провели масштабний біткоїн-скам, опублікувавши повідомлення з проханням переказати кошти на вказані гаманці. Загальний збиток оцінюється в понад $120 тис., а інцидент серйозно підірвав довіру до платформи.

Цей випадок показав, що навіть компанії з високим рівнем технічного захисту можуть бути вразливими до соціальної інженерії, якщо не навчають співробітників протидії маніпуляціям.

У 2021 році сталася серія атак на компанію Ubiquiti Networks, де зловмисники використали складний фішинг із елементами претекстингу [15]. Вони надіслали співробітникам листи, що імітували офіційні повідомлення від HR-відділу, з проханням оновити облікові дані через підроблений портал. Після

отримання доступу злочинці змогли провести фінансові шахрайства на суму близько $50 млн.

Ще одним прикладом є атака на бельгійську фінансову установу Crelan Bank (2022), де зловмисники, видаючи себе за керівництво, змусили фінансового менеджера переказати €70 млн на підконтрольні рахунки [16]. Подібні інциденти демонструють, що BEC-атаки залишаються надзвичайно прибутковими для кіберзлочинців.

Інноваційні методи соціальної інженерії все частіше включають технології штучного інтелекту. У 2023 році в ОАЕ зафіксовано випадок, коли зловмисники за допомогою deepfake-аудіо імітували голос директора компанії, наказавши підлеглому переказати $35 млн [17]. Жертва не запідозрила обману, оскільки голос звучав ідентично.

Аналогічний інцидент стався у Великій Британії (2024), де штучний інтелект використовувався для створення відеозвернення "керівника", що сприяло успішному викраденню конфіденційних даних [18].

Соціальна інженерія активно застосовується в кібератаках на урядові організації. Наприклад, у 2022 році хакерська група APT29 (Cozy Bear) використала фішинг для проникнення в мережі європейських міністерств. Листи маскувалися під офіційні запити від дипломатичних відомств, що дозволило зловмисникам встановити шкідливе ПЗ [19].

Ще один показовий випадок — атака на американську систему водопостачання (2023), де інженера обманом змусили ввести свої дані на фішинговому сайті, що призвело до кіберпроникнення в SCADA-систему [20].

Всі кейси в загальному вигляді наведено в табл. 2.1.

Таблиця 2.1

Аналіз реальних кейсів соціально-інженерних атак

Кейс	Рік	Метод атаки	Техніка	Втрати/Наслідки	Уразливість	Запобіжні заходи
Twitter	2020	Телефонний претекстинг	Імітація IT-відділу	$120 тис., репутаційні збитки	Недостатня верифікація ідентичності	Введення багатофакторної аутентифікації для внутрішніх систем
Ubiquiti Networks	2021	Цільовий фішинг	Підробка HR-повідомлень	$50 млн	Відсутність тренувань з кібербезпеки	Впровадження регулярних фішинг-тестів
Crelan Bank	2022	BEC (Business Email Compromise)	Імітація керівництва	€70 млн	Слабкі механізми підтвердження платежів	Обов'язковий дзвінок для підтвердження великих транзакцій
Deepfake в ОАЕ	2023	AI-вішинг	Генерація голосу CEO	$35 млн	Відсутність голосових паролів	Введення кодового слова для фінансових операцій
Атака на європейські міністерства (APT29)	2022	Цільовий фішинг	Підробка дипломатичних листів	Викрадення конфіденційних даних	Відсутність перевірки доменів	Впровадження DMARC-аутентифікації
Система водопостачання США	2023	Фішинг	Підробка панелі управління SCADA	Кіберпроникнення в критичну інфраструктуру	Відсутність сегментації мережі	Ізоляція критичних систем
Deepfake у Великій Британії	2024	AI-вішинг	Відеоімітація керівника	Викрадення конфіденційних даних	Наївність співробітників	Тренування з розпізнавання deepfake

Для проведення соціально-інженерних атак зловмисники використовують різноманітні інструменти та техніки. Серед них:

- **Фішинг:** використання електронних листів, SMS або месенджерів для

обману жертв. Інструменти, такі як GoPhish або SET (Social-Engineer Toolkit), дозволяють автоматизувати розсилання шкідливих повідомлень.

- **Претекстинг:** створення вигаданих сценаріїв для отримання інформації. Наприклад, імітація служби підтримки для збору паролів.
- **Байт-інжиніринг:** використання USB-пристроїв із шкідливим ПЗ, які підкидаються жертвам у публічних місцях.
- **Вішинг (відеофішинг):** використання відеозвернень або deepfake для введення жертви в оману.

Дослідження показують, що комбінація цих методів підвищує ефективність атак. Наприклад, у кейсі з компанією SolarWinds зловмисники поєднали фішинг із соціальною інженерією для проникнення в мережу [21].

Також важливим аспектом є використання OSINT (Open Source Intelligence) для збору інформації про ціль. Інструменти, такі як Maltego або SpiderFoot, дозволяють зловмисникам отримувати дані з соціальних мереж, що значно підвищує успішність атак.

Аналіз кейс-досліджень, реальних інцидентів та інструментів соціальної інженерії дозволяє розробити ефективні методики протидії кібератакам. Враховуючи динамічний розвиток цієї сфери, необхідно постійно вдосконалювати підходи до навчання персоналу та впроваджувати технічні засоби захисту.

2.2 Аналіз результатів проведення соціально-інженерних кібератак

Соціально-інженерні атаки є одним із найпоширеніших методів кіберзлочинності, оскільки вони експлуатують не технічні вразливості систем, а психологічні слабкості людей. У цьому розділі досліджуються ключові фактори, що впливають на успішність таких атак, порівнюються різні типи соціальної інженерії за ефективністю, а також визначаються основні вразливості в поведінці користувачів, які роблять їх легкими цілями для зловмисників.

Соціальні інженери активно використовують емоційні маніпуляції для

досягнення своїх цілей [22]. Найчастіше експлуатуються такі психологічні чинники (табл. 2.2):

- **Терміновість** – повідомлення з формулюваннями на кшталт *"Ваш акаунт буде заблоковано через 24 години"* змушують користувачів діяти швидко, без критичного аналізу.
- **Авторитет** – імітація листів від керівництва, банків або держорганів підвищує рівень довіри.
- **Страх** – загрози фінансових втрат або розголошення конфіденційної інформації пригнічують раціональне мислення.
- **Допитливість** – пропозиції отримати винагороду або доступ до ексклюзивної інформації активізують бажання «клікнути» на посилання.

Таблиця 2.2

Порівняння психологічних чинників соціально-інженерної атаки

Психологічний чинник	Механізм впливу	Приклад використання в атаці	Ефективність
Терміновість	Активує імпульсивні реакції	"Ваш акаунт буде заблоковано за 24 години"	45-60% кліків
Авторитет	Викликає беззаперечну довіру	Листи від імені керівництва/банків	65-78% виконання інструкцій
Страх	Блокує критичне мислення	Загрози фінансових втрат/розголошення даних	50-70% успішних атак
Допитливість	Стимулює бажання дізнатись більше	"Ексклюзивна пропозиція тільки для вас"	30-40% кліків

Люди схильні до низки когнітивних упереджень, які полегшують роботу соціальних інженерів:

- ефект підтвердження – користувачі шукають інформацію, яка підтверджує їхні очікування, ігноруючи протилежні сигнали;
- ефект стаду – якщо повідомлення містить посилання на "популярність"

послуги ("Цим користуються мільйони!"), ймовірність кліку зростає;

- наївний реалізм – багато людей вважають, що "саме з ними нічого не станеться", що знижує обережність [23].

Техніки, засновані на соціальній взаємодії, такі як претекстинг (використання вигаданого сценарію) або квіпроксінг (підслуховування), ефективні через природню схильність людей допомагати іншим або уникати конфліктів.

Дослідження компанії Proofpoint (2023) показало, що:

- 45% користувачів клікають на фішингові посилання, якщо вони імітують внутрішню корпоративну комунікацію.
- 78% співробітників готові розкрити пароль під час телефонного дзвінка, якщо той подається як "техпідтримка" [24].

Соціально-інженерні атаки демонструють різний рівень ефективності залежно від використовуваного методу, цільової аудиторії та якості підготовки зловмисників. Фішинг, який включає розсилку електронних листів, SMS-повідомлень або повідомлень у месенджерах, залишається одним із найпоширеніших методів. Його ефективність коливається в межах 30-50% успішних кліків, що залежить від реалістичності підробки та вміння зловмисників створити відчуття терміновості. Основною перевагою цього методу є можливість масштабування – за допомогою спеціалізованих інструментів на кшталт GoPhish або Social-Engineer Toolkit можна одночасно атакувати тисячі цілей [25]. Однак для досягнення високої ефективності необхідно ретельно підготувати макети повідомлень, що імітують офіційні комунікації від відомих брендів або керівництва компанії.

Більш складні методи, такі як вішинг або використання deepfake-технологій, демонструють значно вищу ефективність при цільових атаках на окремих осіб, особливо коли мова йде про топ-менеджмент. Дослідження показують, що у випадках, коли зловмисники імітують голос або зовнішність керівника за допомогою штучного інтелекту, рівень успішності може досягати 70% [26]. Це пояснюється тим, що люди природно схильні довіряти візуальним

та аудіальним сигналам, особливо коли вони надходять від осіб з авторитетом. Проте такі атаки вимагають значно більших зусиль на підготовку, включаючи збір інформації про ціль, створення якісних імітацій, а також розробку правдоподібного сценарію взаємодії. Крім того, масштабування таких атак утруднене через їхню індивідуальну спрямованість.

Претекстинг, що передбачає телефонні дзвінки або особисту взаємодію під виглядом службових осіб, демонструє високий рівень ефективності – від 60 до 80% успішних спроб отримання конфіденційної інформації [27]. Цей метод ґрунтується на соціальних нормах поведінки, зокрема на бажанні людей бути корисними або уникнути конфлікту з "представниками влади". Перевагою претекстингу є можливість гнучко адаптувати сценарій під реакцію жертви, що значно підвищує ймовірність успіху. Однак такий підхід вимагає значних часових витрат і не підходить для масових атак, оскільки кожен випадок потребує індивідуального підходу.

Методи фізичної соціальної інженерії, такі як байт-інжинірінг з використанням підкинутих USB-пристроїв, показують помірну ефективність на рівні близько 40% [28]. Дослідження демонструють, що значна частина користувачів підключає знайдені носії до своїх комп'ютерів, не замислюючись про потенційні загрози. Хоча цей метод не дозволяє отримати доступ до віддалених систем, він може бути надзвичайно ефективним для проникнення в захищені мережі, де немає безпосереднього доступу до інтернету. Головним обмеженням є необхідність фізичного контакту з ціллю, що звужує коло потенційних жертв.

Порівняльний аналіз ефективності різних методів соціальної інженерії (табл. 2.3) дозволяє зробити висновок, що вибір конкретної техніки залежить від цілей зловмисників. Для масових атак найбільш підходящим є фішинг через баланс між ефективністю та масштабованістю. Коли мова йде про цільові атаки на конкретні організації або осіб, більш складні методи на кшталт вішингу або претекстингу демонструють значно вищу ефективність, незважаючи на трудомісткість їхньої підготовки. Важливим фактором залишається рівень

обізнаності цільової аудиторії – чим вищий рівень знань про методи соціальної інженерії, тим нижча ефективність будь-якого з описаних методів.

Таблиця 2.3

Порівняльний аналіз методів соціально-інженерних атак та впливу психологічних факторів

Критерій	Фішинг	Вішинг/Deepfake	Претекстинг	Байт-інжинірінг
Ефективність	30-50%	До 70%	60-80%	~40%
Масштабованість	Висока	Обмежена	Низька	Низька
Складність виконання	Низька	Висока	Середня	Низька
Використовувані психологічні фактори	Терміновість, авторитет	Довіра до авторитету, візуальні/аудіальні ілюзії	Соціальні норми, бажання допомогти	Допитливість, ігнорування безпеки
Цільова аудиторія	Масові співробітники	Топ-менеджмент, фінансові служби	Адміністративний персонал, служби підтримки	Персонал з фізичним доступом до систем
Інструменти	GoPhish, SET	Deepfake-ПЗ, AI-генератори голосу	Соціальні мережі, OSINT-інструменти	Підготовлені USB-пристрої

Визначення вразливостей у поведінці користувачів є ключовим аспектом у розумінні механізмів успішних соціально-інженерних атак. Дослідження показують, що певні шаблони поведінки значно підвищують ймовірність успіху кіберзлочинців. Однією з найпоширеніших вразливостей є надмірна довіра до офіційно виглядаючих джерел інформації. Користувачі часто не перевіряють справжність адрес електронної пошти, доменів вебсайтів або номерів телефонів, якщо повідомлення має професійне оформлення чи містить логотипи відомих організацій. Ця тенденція особливо виражена у випадках, коли повідомлення імітує комунікацію від керівництва компанії або служби підтримки.

Іншою суттєвою проблемою є ігнорування навіть очевидних сигналів безпеки. Статистика свідчить, що близько 40% користувачів натискають на потенційно небезпечні посилання, незважаючи на попередження браузерів або антивірусних програм. Така поведінка часто пояснюється поспіхом, перевантаженням інформацією або елементарною втомою, які пригнічують критичне мислення. Особливо небезпечним є звичка використовувати однакові паролі для різних сервісів, що робить користувачів вразливими до технік credential stuffing після одного успішного фішингу.

Важливим чинником є недостатній рівень кіберграмотності. Дослідження компанії KnowBe4 за 2024 рік демонструють, що лише 12% співробітників здатні правильно ідентифікувати складний фішинговий лист без спеціального навчання. Після проведення тренувань цей показник зростає до 75%, проте ефект від навчання поступово знижується вже через півроку, що вказує на необхідність регулярного оновлення знань [29]. Особливості організаційної культури також можуть підвищувати ризики – у компаніях з жорсткою ієрархією співробітники частіше виконують дивні прохання, якщо вони подаються від імені керівництва.

Психологічні особливості також відіграють значну роль. Багато користувачів схильні до ефекту "наївного реалізму", коли людина вважає, що саме з нею нічого поганого не станеться, навіть якщо вона знає про загрози. Це призводить до легковажного ставлення до правил кібербезпеки [30]. Соціальні інженери часто експлуатують природню допитливість людей – пропозиції отримати доступ до ексклюзивної інформації або обмежених пропозицій значно підвищують ймовірність успішної атаки. Водночас страх перед покаранням або фінансовими втратами може змусити користувачів швидше виконувати інструкції, не замислюючись про їхню легітимність. Порівняльний аналіз типів вразливості в соціально-інженерних атаках представлений в табл.2.4.

Таблиця 2.4

Порівняльний аналіз типів вразливості в соціально-інженерних атаках

Тип вразливості	Частота прояву	Наслідки	Способи експлуатації
Довіра до офіційного вигляду	68% користувачів (KnowBe4)	Кліки на фішингові посилання	Використання логотипів, офіційних шаблонів
Ігнорування сигналів безпеки	40% випадків	Підключення шкідливих пристроїв	Байт-інжинірінг, підроблені попередження
Використання однакових паролів	59% співробітників	Масові компрометації	Credential stuffing після одного успішного фішингу
Наївний реалізм	85% непрофільних працівників	Нехтування правилами безпеки	Атаки з розрахунком на "це точно не мене"

Для ефективного протидії цим вразливостям необхідний комплексний підхід. Впровадження регулярних тренувань з кібербезпеки дозволяє підвищити обізнаність персоналу, але ці навчальні програми повинні враховувати психологічні аспекти сприйняття інформації. Використання двофакторної аутентифікації значно знижує ризик навіть у випадку викрадення облікових даних. Симуляції реальних атак допомагають не лише виявити слабкі місця в обізнаності співробітників, але й сформувати практичні навички реагування на загрози. Важливо створити в організації культуру безпеки, де кожен співробітник відчуває особисту відповідальність за захист даних і має зрозумілі інструкції щодо дій у підозрілих ситуаціях.

Висновки до розділу 2

Проведений аналіз результатів соціально-інженерних кібератак дозволяє зробити низку важливих висновків щодо їхньої ефективності та механізмів впливу. Дослідження психологічних чинників показало, що успішність таких

атак ґрунтується на експлуатації природніх людських слабкостей - емоційних реакцій, когнітивних упереджень і соціальних норм поведінки. Терміновість, страх, довіра до авторитетів та бажання допомогти регулярно використовуються зловмисниками для маніпулювання жертвами.

Порівняльний аналіз різних типів атак виявив чітку залежність між складністю підготовки та ефективністю. Якщо масовий фішинг демонструє помірну успішність на рівні 30-50%, то цільові методи (вішинг, претекстинг) досягають 60-80% результативності, особливо при атаках на високопоставлених осіб. Однак саме поєднання різних технік у багатоетапних атаках становить найбільшу загрозу.

Вивчення поведінкових вразливостей підтвердило, що основною слабкою ланкою залишається людський фактор. Надмірна довіра, ігнорування сигналів безпеки, недостатня кіберграмотність і наївний реалізм створюють ідеальні умови для соціальних інженерів. При цьому традиційні технічні засоби захисту часто виявляються неефективними проти психологічно продуманих маніпуляцій.

Розділ 3 АНАЛІЗ ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ В СУЧАСНИХ КІБЕРАТАКАХ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ ВІД СОЦІАЛЬНО-ІНЖЕНЕРНИХ ЗАГРОЗ

3.1. Побудова ефективної системи захисту від соціально-інженерних загроз

Соціально-інженерні атаки базуються на маніпулюванні психологією людини. Зловмисники у сфері кібербезпеки часто застосовують ці методи для досягнення власних цілей. Одним із поширених інструментів є фішинг — обманні електронні листи, які імітують повідомлення від надійних джерел з метою змусити одержувача розкрити конфіденційну інформацію. Іншим прийомом є претекстинг, який передбачає створення вигаданих сценаріїв для збору чутливої інформації. Наприклад, зловмисники можуть видавати себе за представників банків або інших авторитетних організацій.

Кіберзлочинці також активно використовують психологічні механізми маніпуляції. Зокрема, часто застосовується техніка формування довіри до зловмисника через встановлення емоційного контакту. Цей підхід характерний для спрямованих фішингових атак. Інша стратегія полягає у викликанні почуття страху: зокрема, можуть використовуватись повідомлення про нібито виявлений вірус з вимогою негайних дій, що імітують попередження про зараження програмами-вимагачі. Крім того, уразливість жертв часто посилюється через збудження цікавості, наприклад шляхом поширення привабливих пропозицій, які спонукають користувачів здійснювати потенційно небезпечні дії [31].

Для побудови ефективної системи захисту від соціально-інженерних загроз треба розуміти етапи атаки, які зображені на рис. 3.1.

Рис. 3.1. Етапи кібератаки

Кіберзлочинець розпочинає атаку з фази рекогностування, збираючи дані про компанію, її працівників, постачальників і клієнтів через відкриті джерела, такі як вебсайти та LinkedIn. Використовуються також фальшиві дзвінки. Збирається інформація про IP-адреси, обладнання, ПЗ та дані з баз ICAAN [32]. На фазі озброєння створюються фішингові листи й підроблені сайти для викрадення облікових даних або поширення шкідливих файлів. Підбираються інструменти для подальшої експлуатації вразливостей.

Фаза «доставки» включає надсилання фішингових листів або публікацію фальшивих вебсторінок. Зловмисник очікує відкриття вкладень або переходу за посиланнями. У фазі експлуатації отримані облікові дані використовуються для входу в системи або віддаленого доступу до заражених пристроїв. Досліджується структура мережі.

На фазі інсталяції встановлюється бекдор, створюються адмін-акаунти, змінюються налаштування безпеки. Фаза командування і контролю дає повний доступ до мережі, дозволяє видавати себе за будь-якого користувача. На завершальній фазі реалізуються цілі атаки: крадіжка даних, порушення роботи або саботаж.

Ефективна система захисту від соціоінженерних загроз інтегрує особистісно-орієнтовані, організаційні та технічні компоненти для усунення вразливостей, що виникають внаслідок людської поведінки та мережевої динаміки.

Ключовим елементом є захист, орієнтований на людину, шляхом проведення інформаційних тренінгів. Оскільки соціальна інженерія націлена на

людську поведінку, навчання користувачів розпізнаванню маніпулятивних тактик має вирішальне значення. Навчальні програми зосереджені на розпізнаванні фішингу, спробах видачі себе за іншу особу та телефонних шахрайствах. Ефективне навчання має бути безперервним і регулярно оновлюватися, щоб відображати тактики, що розвиваються.

Особлива увага приділяється механізмам звітування, що сприяє ранньому виявленню та реагуванню.

Організаційні політики та процедури формують структурну основу захисту. Політики встановлюють ієрархічний контроль над процесами, забезпечуючи впровадження принципів безпеки в рутинні операції. Приклади включають протоколи верифікації, ідентифікацію абонента для телефонних розмов і принципи найменших привілеїв для прав доступу [33]. Політика класифікації даних та інструкції з безпеки посилюють поведінкові обмеження, мінімізуючи несанкціоноване розголошення даних. Розробка та підтримка цих політик вимагає детального планування та постійного аудиту для забезпечення їх дотримання.

З технічного боку, кілька механізмів безпосередньо підтримують захист. Пісочниця забезпечує ізольоване середовище виконання для стримування підозрілих програм або дій. Ця стратегія стримування запобігає поширенню шкідливого програмного забезпечення за межі контрольованих кордонів, захищаючи критичні системи та дані. Фреймворки авторизації, автентифікації та обліку (AAA) забезпечують контроль доступу, гарантуючи, що лише авторизовані користувачі взаємодіють з критично важливими системами. Багатофакторна автентифікація (MFA) посилює цей контроль, вимагаючи декількох форм перевірки особи. Ведення логів і моніторинг поведінки користувачів створюють аудиторські сліди, які допомагають проводити криміналістичні розслідування і виявляти аномалії [34].

Механізми перевірки цілісності підтверджують достовірність файлів, програмного забезпечення та переданих даних. Використовуючи цифрові

підписи або криптографічні хеші, системи можуть виявляти несанкціоновані зміни.

Технічні засоби захисту використовують алгоритми AI/ML для виявлення аномалій, що вказують на соціоінженерні атаки. Системи виявлення вторгнень (IDS) аналізують мережевий трафік на предмет відхилень від базових моделей довіри, таких як раптові сплески запитів на передачу повноважень або нерегулярні потоки даних між вузлами з низькою довірою [35]. Поведінкова біометрія, інтегрована з рольовим контролем доступу, автентифікує користувачів, зіставляючи послідовності дій з історичними профілями довіри.

Системи моніторингу доповнюють ці заходи, агрегуючи та аналізуючи активність системи в реальному часі. Сповіщення, що генеруються на основі виявлених аномалій, спонукають до дій з реагування на інциденти, мінімізуючи вплив успішних порушень. Адаптивні стратегії моніторингу необхідні для врахування зміни векторів атак і поведінки користувачів.

Разом ці компоненти - навчання, організаційна політика, технічні засоби захисту та адаптивне виявлення - утворюють багаторівневу систему захисту. Кожен рівень компенсує потенційні недоліки інших, створюючи стійку архітектуру, здатну протистояти складності та динамічності сучасних загроз соціальної інженерії.

3.2. Технічні рішення для виявлення і блокування спроб атак

Виявлення та запобігання вторгнень являє собою процес контролю інформаційних систем із використанням датчиків або агентів та подальшого аналізу отриманих даних з метою виявлення атак, вразливостей, порушень політик безпеки або стандартних безпекових практик, а також їхнього припинення в режимі реального часу. Система виявлення та запобігання вторгнень (IDPS) є засобом, який здійснює спостереження за інформаційними системами, виконує збір і аналіз інформації, а також ініціює дії у відповідь у разі виявлення вторгнення [36]. Системи виявлення вторгнень (IDS) функціонують

переважно як захисні інструменти, які лише повідомляють системних адміністраторів про настання інциденту. Системи запобігання вторгненням (IPS) здатні самостійно реалізовувати заходи для зупинення атаки, зокрема розривати з'єднання або змінювати конфігурації брендмауера з метою блокування доступу зловмисника до системи. У той час як реакція класичної IDS може затримуватись через зайнятість адміністратора, система IPS забезпечує автоматизовану відповідь. Найбільш ефективним варіантом глибокого захисту є архітектура, яка об'єднує технології IDS та IPS. Типова IDPS складається з модульних складових, зокрема системи моніторингу, сховища, аналізатора та модуля реагування [37].

Система моніторингу відстежує та реєструє події в комп'ютерній системі або мережі. Сховище зберігає інформацію про підозрілі дії або вторгнення, яка називається аудиторським записом; також у ньому зберігаються політики безпеки, використані при аналізі. Аналізатор застосовує різні методології аналізу для виявлення інцидентів. Реагування є механізмом відповіді на інциденти.

IDPS класифікують за кількома ознаками. За методологією виявлення виділяють: виявлення на основі зловживань, виявлення на основі аномалій, а також аналіз протоколів з урахуванням стану [38]. За активністю розрізняють: системи на основі мережі, на основі бездротових мереж, аналіз мережевої поведінки, а також системи на основі хостів. За поведінкою при виявленні IDPS можуть бути пасивними або активними. За частотою збору та аналізу інформації системи поділяють на безперервні та періодичні.

Першоджерелом системи виявлення та запобігання мережевим вторгненням (NIDPS) є мережевий трафік. У мережевому трафіку дані проходять через рівні від джерела до одержувача [39]. Чотири рівні TCP/IP: апаратний рівень, рівень інтернет-протоколу (IP), транспортний рівень, прикладний рівень. Модель TCP/IP зображена на рис. 3.2.

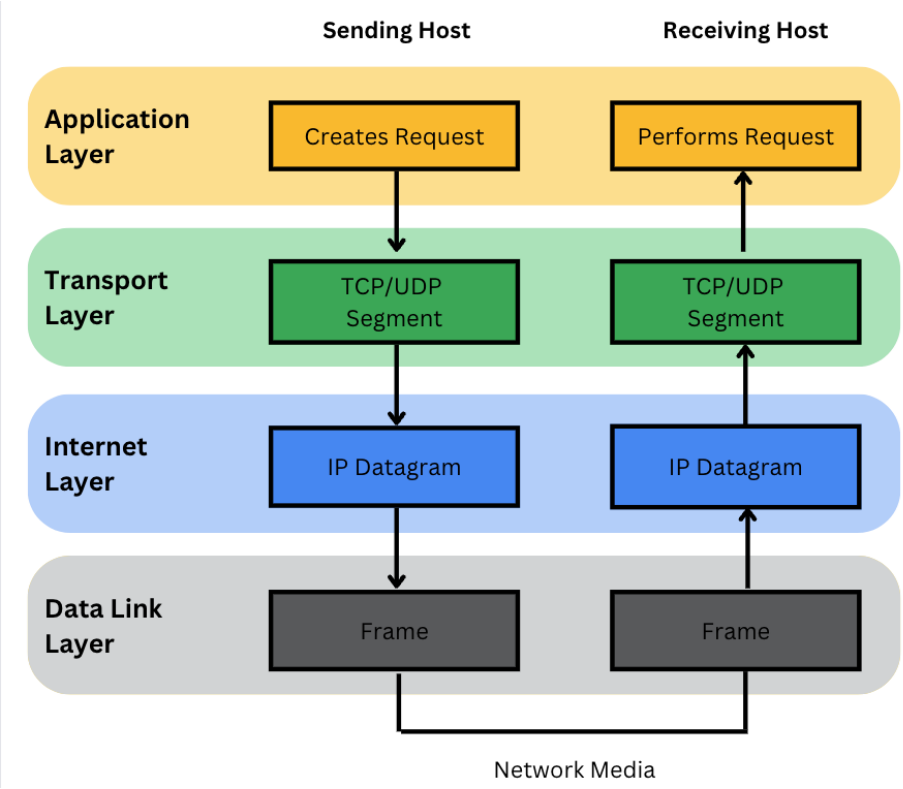

Рис. 3.2. Мережевий трафік в моделі TCP/IP

Типовий комплекс NIDPS складається з датчиків, одного або декількох серверів управління, декількох консолей і, за бажанням, одного або декількох серверів баз даних. Датчики - відстежують та аналізують активність. Датчики можуть бути апаратно-програмними - спеціалізованим апаратним забезпеченням і програмним забезпеченням датчика або тільки програмним забезпеченням [40]. До складу апаратного датчика входять спеціалізовані мережеві плати та драйвери для них, а також спеціалізовані процесори, які допомагають в аналізі.

Для виявлення аномалій у мережевому трафіку використовуються як статичні, так і динамічні методи аналізу протоколів. Статичний аналіз ґрунтується на перевірці заголовків пакетів та їхніх значень на відповідність стандартам протоколів. Наприклад, аномаліями вважаються TCP-пакети з одночасно встановленими прапорцями SYN та FIN, відсутність будь-яких прапорців у TCP-заголовку (значення 00), некоректна довжина заголовку IP (більше 20 байт для IPv4 без опцій) або спроби підключення з резервованих IP-адрес. Такі аномалії часто використовуються для проведення DoS-атак, сканування портів або спроб обходу систем безпеки [41]. Для виявлення

подібних загроз створюються сигнатури, які порівнюються з аудиторськими даними. Наприклад, сигнатура для виявлення невдалих спроб входу в Telnet може шукати рядок "Login failed" у корисному навантаженні пакетів (рис. 3.3).

```
     alert tcp $HOME_NET 23 ->
$EXTERNAL_NET any (msg:"TELNET Bad
Login";
     content: "Login failed"; nocase;
flow: from_server, established;
classtype:bad-unknown; sid:492; rev:5;)
```

Рис. 3.3. Приклад сигнатури Telnet

Динамічний аналіз протоколів передбачає повне декодування трафіку на всіх рівнях моделі TCP/IP. Це дозволяє аналізувати не лише заголовки, але й корисне навантаження, включаючи дані прикладного рівня (HTTP, FTP, SMTP). Наприклад, для виявлення експлойтів, що використовують переповнення буфера в команді FTP MKD, система перевіряє довжину аргументу команди та відсутність шкідливого коду. Динамічний підхід також дозволяє обробляти техніки ухилення, такі як Path Obfuscation, де зловмисники використовують екранування символів, надлишкові пробіли, Unicode-кодування або зміну формату шляху (наприклад, заміну "/" на "", використання послідовностей типу /./). Для цього NIDPS виконує нормалізацію шляхів, розпізнаючи еквівалентні варіанти та аналізуючи їх на предмет аномалій [42].

Важливу роль у протидії сучасним загрозам відіграє аналіз зашифрованого трафіку. Хоча традиційні NIDPS не здатні інспектувати дані всередині VPN, HTTPS або SSH-сесій, деякі системи використовують методи декодування трафіку до шифрування або після дешифрування. Наприклад, McAfee IntruShield може розпаковувати SSL-шар HTTPS-з’єднань для аналізу вмісту. Однак це вимагає інтеграції з ключовими інфраструктурами та може впливати на продуктивність.

Для виявлення поліморфних та метаморфних шкідливих програм застосовуються техніки емуляції та віртуалізації. Поліморфні віруси містять постійний компонент (наприклад, рутину дешифрування), який може бути

ідентифікований за сигнатурою, тоді як метаморфні віруси повністю змінюють код, що вимагає використання евристичного аналізу, статистичних методів або машинного навчання.

Аналіз мережевих потоків (NetFlow, IPFIX) дозволяє виявляти аномалії на основі агрегованих даних, таких як джерельні та цільові IP-адреси, порти, обсяги трафіку, тривалість сесій. Наприклад, підхід subspace method використовує вибіркові дані з маршрутизаторів (1% пакетів) для виявлення аномалій на рівні OD-потоків. Кожен потік розкладається на нормальну та аномальну компоненти, а порушення визначаються через перевищення порогових значень [43]. Комбіновані методи, такі як timeslot-based та flow-based аналіз, дозволяють зменшити навантаження на систему: перший етап використовує часові інтервали для попередньої класифікації трафіку, а другий застосовує детальний аналіз до підозрілих потоків.

Нормалізація трафіку є критичною для уникнення технік обходу, пов’язаних з фрагментацією пакетів або неоднозначною інтерпретацією даних. Нормалізатори видаляють надлишкові дані, відновлюють правильний порядок фрагментів та усувають можливі конфлікти під час їхньої реасемблерації. Це дозволяє NIDPS аналізувати трафік у стандартизованому форматі, знижуючи ймовірність пропуску атак, замаскованих через некоректну фрагментацію або перекриття офсетів.

Сучасні системи також інтегрують машинне навчання для статистичного аналізу параметрів трафіку, таких затримки між пакетами, розподіл розмірів пакетів, частота запитів. Це дозволяє відрізняти легальну активність (наприклад, веб-серфінг) від аномальної (DDoS-атаки, сканування). Використання нейронних мереж або дерев прийняття рішень покращує точність виявлення нових типів атак, для яких відсутні сигнатури.

3.3. Розробка та впровадження рекомендацій на основі досліджених кейсів

Технічні рішення є першою лінією захисту від соціальної інженерії, застосовуючи автоматизовані системи для виявлення та нейтралізації загроз до моменту їх контакту з потенційною жертвою. Вони особливо ефективні проти масштабних фішингових кампаній, які покладаються на обсяг і повторюваність. Використовуючи передові алгоритми, штучний інтелект та інші технології, такі інструменти блокують шкідливі дії на випередження. До найпоширеніших відносяться антифішингове програмне забезпечення, фільтри безпеки електронної пошти, багатофакторна автентифікація (MFA) та системи виявлення, керовані ШІ.

Антифішингове програмне забезпечення аналізує вхідну пошту на підозрілі URL, аномальні адреси відправників і типовий фішинговий контент. Воно також перевіряє метадані електронних листів та використовує репутаційні бази доменів. Гібридні моделі машинного навчання дозволяють адаптуватися до змінних тактик атак. Фільтри безпеки електронної пошти доповнюють ці інструменти через контентну і поведінкову фільтрацію, використовуючи евристику та середовище «пісочниці» для аналізу вкладень. Вони блокують загрози на мережевому рівні, зменшуючи ризик для співробітників.

MFA вимагає додаткових рівнів автентифікації, таких як OTP, біометрія або апаратні токени. Це ускладнює використання викрадених облікових даних, однак зловмисники іноді переконують користувачів самостійно обходити захист, наприклад, надаючи одноразовий код. Системи на базі ШІ виявляють аномалії, аналізуючи великі обсяги даних, зокрема стилістику мови в електронних листах за допомогою NLP, що дозволяє розпізнавати фішингові повідомлення навіть у разі імітації легітимного контенту.

Антифішингові інструменти та поштові фільтри щодня блокують мільйони спроб фішингу. Емпіричні дослідження демонструють, що організації, які впроваджують ці технології, відзначають помітне зменшення успішних

фішингових атак. Встановлення багатофакторної автентифікації значно знижує кількість компрометацій облікових записів, особливо з підвищеним рівнем ризику. MFA, доповнюючи рівні перевірки, ефективно протидіє викраденню облікових даних. Її інтеграція з програмами з підвищення обізнаності демонструє додатковий позитивний ефект. Системи, що працюють на базі штучного інтелекту, незважаючи на новизну, вже відіграють важливу роль у боротьбі зі складними загрозами. На відміну від традиційних методів, ШІ здатен оперативно адаптуватися до нових даних, наприклад, виявляючи новостворені фішингові сайти протягом кількох секунд після їх появи.

Однак технічні рішення мають і певні обмеження. Поширеною проблемою є хибні спрацювання, коли легітимні повідомлення визначаються як зловмисні. Це порушує робочі процеси та знижує довіру користувачів до автоматизації. Висока вартість помилок є критичною, зокрема для організацій із залежністю від безперервного зв’язку [44]. Інша проблема — ухильна тактика зловмисників, які адаптують фішинговий контент під внутрішню комунікацію або актуальні події, обходячи захист. Такі дії вимагають постійної актуалізації алгоритмів. Запровадження технічного захисту потребує значних ресурсів. Малим і середнім підприємствам може бракувати необхідної інфраструктури або експертизи, що підвищує їхню вразливість. Жодне технічне рішення не усуває повністю пов’язані з поведінкою людини фактори, що підкреслює потребу в комплексному підході.

Технічні рішення є важливими, однак людська поведінка часто обмежує їхню ефективність, оскільки соціальні інженери експлуатують психологічні вразливості, довіру та когнітивні упередження. Підходи, орієнтовані на людину, надають користувачам знання та навички для розпізнавання маніпуляцій. Навчання з питань безпеки є поширеним методом зниження ризиків. Програми навчають розпізнавати фішинг і телефонні шахрайства, а також відповідні реакції. Ефективність підвищується за умови постійного, інтерактивного навчання, адаптованого до конкретних загроз. Імерсивні методи, такі як фішингові симуляції та гейміфікація, демонструють кращу результативність.

Такі вправи створюють контрольоване середовище, де користувачі вчаться на помилках без реальних наслідків, що підвищує пильність.

Людиноцентричні підходи також спрямовані на поведінкові втручання, що протидіють упередженням, зокрема терміновості, авторитету і соціальному підтвердженню. Методи праймінгу стимулюють обережність при взаємодії з листами або посиланнями. Формування культури «безпека понад усе» сприяє зниженню імпульсивних дій. Вбудовані навчальні моделі інтегрують короткі підказки безпеки в робочі процеси, наприклад банери із попередженням у листах, що зменшує ризики без втрати продуктивності.

Успішність таких підходів залежить від організаційного контексту: культури компанії, участі керівництва та комунікаційної практики. Ієрархічні структури можуть сприяти виконанню шахрайських запитів, якщо вони сприймаються як авторитетні. Необхідна адаптація заходів до конкретного сектору та вразливостей, з урахуванням міжкультурних особливостей стилів комунікації та довіри.

Організації, що впровадили регулярні симуляції фішингу в рамках програм підвищення обізнаності, зафіксували поступове зниження кількості переходів за шкідливими посиланнями. Компанії, які проводили гейміфіковані тренінги, за рік зменшили успішні фішингові атаки на 30%. Поведінкові втручання, зокрема механізми зворотного зв’язку в режимі реального часу, як-от негайні сповіщення при взаємодії з імітацією фішингового листа, підвищили рівень обізнаності користувачів і сприяли формуванню культури колективної відповідальності за безпеку. Однак залишаються проблеми, пов’язані з помилковою природою людської поведінки. Когнітивні упередження, втома й соціальна динаміка можуть знижувати ефективність навіть ретельно розроблених навчальних програм. Довгостроковий ефект втручань потребує постійного підкріплення.

Серед головних труднощів у впровадженні таких заходів є опір змінам поведінки. Працівники можуть вважати навчання незручним або неусвідомлювати його важливості, особливо в умовах відсутності підтримки з боку керівництва. Подолання опору потребує ефективної комунікації та

вбудовування безпеки в культуру організації. Іншою проблемою є втома від навчання: багаторазові тренінги та інформаційні кампанії можуть викликати десенсибілізацію і зниження ефективності. Організації мають збалансувати частоту проведення з різноманітністю формату, щоб підтримувати актуальність і зацікавленість. Крім того, соціальні інженери постійно змінюють тактики, що ускладнює збереження ефективності статичних програм і вимагає регулярного оновлення матеріалів та вправ з урахуванням нових загроз.

Ефективна протидія атакам соціальної інженерії потребує збалансованої оцінки технічних рішень і підходів, орієнтованих на людину. Технічні заходи забезпечують автоматизацію, масштабованість і точність виявлення загроз. Вони особливо ефективні проти масових фішингових кампаній. Фільтри електронної пошти, антифішингові інструменти та системи на основі ШІ працюють за визначеними правилами, дозволяючи нейтралізувати загрози до їх досягнення користувача. Гібридні системи машинного навчання адаптуються до нових атак, зокрема шкідливих URL [45]. Багатофакторна автентифікація знижує ризик несанкціонованого доступу. Поєднання MFA з навчанням підсилює захист від компрометації облікових записів. Проте технічні засоби демонструють обмеження при складних персоналізованих атаках, таких як spear-фішинг, які базуються на соціальному контексті та стилізації під внутрішнє листування.

Підходи, орієнтовані на людину, розвивають здатність користувачів розпізнавати та протидіяти атакам. Вони ефективні при контекстно залежних загрозах, враховуючи поведінкові та психологічні фактори. Адаптивні навчальні програми, симуляції та вправи підвищують готовність до реальних атак. Поведінкові втручання, як-от попереджувальні банери, сприяють безпечній поведінці. Такі заходи ефективні проти динамічних загроз, що обходять автоматизований захист. Підходи сприяють створенню культури безпеки, де працівники виступають першою лінією оборони. Водночас виклики включають труднощі масштабування, помилки у сприйнятті, опір змінам і втому від навчання, що потребує постійного оновлення та підтримки.

Розглянемо різницю між підходами в табл. 3.1.

Таблиця 3.1.

Порівняння технічних рішень і підходів, орієнтовані на людину

Аспекти	Технічні рішення	Людино-орієнтовані підходи
Основний фокус	Автоматизація, виявлення та запобігання за допомогою алгоритмів та інструментів	Вплив на психологічні та поведінкові фактори
Ефективність	Висока ефективність у боротьбі з великомасштабними, повторюваними атаками (наприклад, фішинговими кампаніями)	Висока ефективність у боротьбі з цільовими або адаптивними атаками (наприклад, spear-фішинг, претекст)
Сильні сторони	Масштабованість, виявлення в реальному часі та узгодженість	Адаптивність, розуміння контексту та розширення індивідуальних можливостей
Обмеження	Боротьба з персоналізованими атаками, хибними спрацьовуваннями та вимогами до ресурсів	Втома, проблеми з масштабуванням та залежність від суджень користувачів
Приклади інструментів	Антифішингове програмне забезпечення, фільтри електронної пошти, MFA, система виявлення на основі штучного інтелекту	Тренінги з підвищення обізнаності про безпеку, симуляції фішингу, поведінкові підказки
Залежність	Потребує потужної інфраструктури та постійних оновлень для збереження ефективності	Потребує постійного підкріплення та зміни організаційної культури
Ідеальний сценарій	Велика організація з великим обсягом електронної пошти; боротьба з однотипними шаблонами атак	Контекстно-чутливі галузі (наприклад, фінанси, охорона здоров'я); високопоставлені особи

Таблиця ілюструє, що технічні рішення і підходи, орієнтовані на людину, не є взаємовиключними, а доповнюють один одного. У той час як технічні рішення чудово підходять для боротьби з масовими, повторюваними загрозами, людино-орієнтовані підходи блищать у боротьбі з адаптивними, цілеспрямованими атаками. Інтегруючи ці стратегії, організації можуть розробити гібридні моделі, які використовують сильні сторони обох парадигм.

На рис. 3.4. показано сильні сторони та взаємодоповнюваність технічних рішень і підходів, орієнтованих на людину, у боротьбі з атаками соціальної інженерії.

Рис. 3.4. Збіг технічних і людино-орієнтованих підходів

Технічні рішення, такі як антифішингові інструменти та системи на основі штучного інтелекту, чудово забезпечують масштабованість, узгодженість та автоматизацію для боротьби з повторюваними загрозами, такими як фішингові кампанії. З іншого боку, людино-орієнтовані підходи враховують поведінкові та психологічні фактори, які лежать в основі успішних спроб соціальної інженерії, що робить їх особливо ефективними у протидії адаптивним і цілеспрямованим атакам, таким як spear-фішинг [46]. Перетин цих двох парадигм підкреслює потенціал гібридних моделей, які інтегрують обидві стратегії. Моделювання фішингу та системи виявлення в режимі реального часу створюють безперервний цикл зворотного зв'язку, в якому поведінка користувачів інформує про оновлення алгоритмів, а інструменти виявлення допомагають визначити пріоритети в навчанні співробітників. Аналогічно, вбудовування підказок безпеки в автоматизовані системи підвищує обізнаність користувачів, водночас зменшуючи залежність від ручного втручання. Ці гібридні засоби захисту усувають обмеження обох підходів, створюючи стійку і динамічну систему безпеки організації.

Постійна еволюція тактик соціальної інженерії створює виклики для технічних рішень і підходів, орієнтованих на людину, що вимагає безперервної адаптації. Технічні рішення мають обмеження, зокрема хибні спрацьовування,

коли легітимні повідомлення помилково позначаються як загрози або зловмисні листи не розпізнаються. Це особливо характерно для інструментів на базі ШІ, яким складно виявити складні лінгвістичні патерни. Зловмисники використовують електронні листи, що імітують внутрішню комунікацію, або приховують шкідливий контент у нетипових форматах. Такі дії знижують ефективність статичних або правил-орієнтованих систем. Розгортання технічних засобів вимагає значних фінансових і технічних ресурсів, що часто є недоступним для малих і середніх підприємств. Крім того, технічні інструменти не впливають на людські фактори, які активно використовуються в соціальній інженерії.

Людиноцентричні підходи також мають обмеження. Втома від навчання через повторювані тренінги може знижувати чутливість і залученість працівників, що зменшує ефективність програм. Зміна поведінки потребує часу, постійного підкріплення та ресурсів. Поведінка людей залишається вразливою до стресу, когнітивних викривлень і тиску авторитетів. Зловмисники використовують ці фактори, щоб обійти протоколи безпеки. Масштабування таких підходів є складним у великих або багатонаціональних організаціях, де культурні та мовні відмінності ускладнюють стандартизацію навчальних втручань.

Майбутній напрям — гібридні моделі, які об'єднують технічні рішення з людським фактором. Інструменти ШІ можуть визначати пріоритетність загроз на основі поведінкових даних, дозволяючи фахівцям зосередитися на складних випадках [47]. Дані з симуляцій фішингових атак використовуються для покращення алгоритмів і навчальних матеріалів, створюючи зворотний зв'язок у реальному часі. Така взаємодія сприяє адаптивності систем і стійкості користувачів. Розробляються інтегровані системи, де технічні засоби співпрацюють з людським наглядом для ідентифікації складних загроз.

Нові технології, зокрема штучний інтелект і машинне навчання, мають високий потенціал у виявленні складних атак, прогнозуванні загроз і адаптації до нових тактик. Обробка природної мови дозволяє системам розпізнавати тонкі

мовні сигнали, які важко підробити. Інтеграція поведінкової аналітики дозволяє ідентифікувати працівників з високим ризиком і застосовувати до них цільові заходи підвищення безпеки.

Застосування поведінкової економіки та психології відкриває нові шляхи для покращення навчальних стратегій [48]. Вивчення когнітивних упереджень, які використовують зловмисники, дозволяє створити ефективніші програми, зокрема з використанням методів поведінкового підкріплення. Гейміфікація у навчанні, наприклад через винагороди або змагання, підвищує мотивацію та залученість, сприяючи формуванню культури безпеки.

Регуляторні ініціативи також відіграють роль. Уряди та галузеві структури можуть встановлювати стандарти мінімальних вимог до навчання, сприяти впровадженню MFA, ШІ-інструментів і стимулювати інвестиції в кібербезпеку. Це сприятиме міжгалузевій уніфікації протидії загрозам соціальної інженерії.

Висновки до розділу 3

Соціальна інженерія залишається одним із найпоширеніших та найнебезпечніших інструментів у арсеналі кіберзлочинців, що підтверджується численними кейсами сучасних кібератак. Аналіз ефективності використання соціальної інженерії показав, що її успіх багато в чому залежить від людського фактору, а не лише від технічних вразливостей систем. Тому побудова ефективної системи захисту від таких загроз потребує комплексного підходу, що поєднує технічні, організаційні та психологічні аспекти. Перш за все, необхідно розвивати культуру кібербезпеки серед користувачів, оскільки саме їхня несвідомість або необізнаність часто стає причиною успішних атак. Регулярні тренінги, симуляції фішингових атак та інформування про актуальні загрози допомагають зменшити ризик вразливості персоналу. Крім того, важливо створити чіткі протоколи реагування на підозрілі події, щоб мінімізувати час між виявленням загрози та її усуненням.

Технічні рішення для виявлення та блокування соціально-інженерних атак також грають ключову роль у захисті. Використання сучасних антифішингових систем, аналізу поведінки користувачів (UEBA), а також штучного інтелекту для виявлення аномалій дозволяє автоматизувати процес виявлення підозрілих дій. Наприклад, системи, що аналізують електронні листи на наявність фішингових ознак, можуть блокувати шкідливі повідомлення до того, як вони потраплять до одержувача. Також ефективними є рішення для двофакторної аутентифікації та обмеження доступу до конфіденційних даних на основі принципу найменших привілеїв. Однак технічні засоби не є панацеєю, оскільки злочинці постійно вдосконалюють свої методи, тому важливо регулярно оновлювати захист і адаптувати його до нових загроз.

Розробка рекомендацій на основі досліджених кейсів показала, що найефективніший захист досягається за рахунок поєднання проактивних і реактивних заходів. До проактивних належать постійний моніторинг загроз, аналіз тенденцій у сфері соціальної інженерії та попереднє тестування систем на вразливості. Реактивні заходи включають швидке реагування на інциденти, розслідування причин успішних атак та вдосконалення захисту на основі отриманого досвіду. Важливо також враховувати специфіку кожної організації, оскільки універсальних рішень не існує. Наприклад, фінансові установи потребують більш жорстких заходів безпеки порівняно з іншими галузями через високий ризик фінансових втрат.

Таким чином, ефективний захист від соціально-інженерних загроз вимагає не лише технічних інновацій, але й постійної роботи з персоналом, адаптації до нових методів атак та комплексного підходу до управління ризиками. Лише поєднання усіх цих елементів дозволить мінімізувати ймовірність успішних кібератак і забезпечити надійний захист конфіденційної інформації. Впровадження рекомендацій, розроблених на основі реальних кейсів, дозволить організаціям не лише протистояти існуючим загрозам, але й бути готовими до нових викликів у майбутньому.

ВИСНОВКИ

Соціальна інженерія залишається одним із найнебезпечніших інструментів у кіберзлочинності, оскільки експлуатує не технічні вразливості систем, а психологічні особливості людей.

У кваліфікаційній роботі було досліджено сутність соціальної інженерії, її роль у сучасному кіберпросторі та основні методи атак, такі як фішинг, претекстинг, вішинґ та інші. Аналіз показав, що, попри розвиток технологій захисту, злочинці постійно вдосконалюють свої схеми, роблячи їх більш складними для виявлення.

У розділі, присвяченому кейс-дослідженню, було розглянуто реальні приклади соціально-інженерних атак, що підтвердили їх високу ефективність. Дослідження виявило, що навіть обізнані користувачі можуть стати жертвами через вміння злочинців маніпулювати емоціями, створювати відчуття терміновості чи використовувати довірені джерела. Було розроблено методику аналізу таких атак, яка дозволяє визначати ключові фактори успіху зловмисників і слабкі місця в системах захисту.

Третій розділ роботи присвячений розробці комплексних заходів протидії соціально-інженерним загрозам. Запропоновано підхід, що поєднує технічні, організаційні та освітні компоненти. До технічних рішень належать системи антифішингу, аналізу поведінки, двофакторна аутентифікація та автоматизоване виявлення аномалій. Однак технології самі по собі не є достатніми – необхідно формувати культуру кібербезпеки через регулярні тренінги, тестування на вразливість та розробку чітких протоколів реагування.

На основі досліджених кейсів було розроблено рекомендації щодо підвищення стійкості організацій до соціально-інженерних атак. Вони включають:

- постійне оновлення засобів захисту з урахуванням нових тактик злочинців;
- симуляцію атак для перевірки готовності персоналу;
- обмеження доступу до конфіденційних даних за принципом найменших привілеїв;

- створення механізмів швидкого виявлення та усунення наслідків успішних атак.

Підсумовуючи, ефективний захист від соціальної інженерії вимагає не лише технічних інновацій, але й постійної роботи з людським фактором. Лише комплексний підхід, що враховує як технологічні, так і психологічні аспекти, дозволить суттєво знизити ризик успішних кібератак. Запропоновані в роботі рекомендації можуть бути використані організаціями для побудови надійної системи безпеки, здатної протистояти сучасним соціально-інженерним загрозам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. A contradistinction study of physical vs. cyberspace social engineering attacks and defense / A. Sobur et al. SSRN electronic journal. 2024. URL: https://doi.org/10.2139/ssrn.487811

2. A contradistinction study of physical vs. cyberspace social engineering attacks and defense / A. Sobur et al. SSRN electronic journal. 2024. URL: https://doi.org/10.2139/ssrn.4878111

3. Aldawood H., Skinner G. Educating and raising awareness on cyber security social engineering: a literature review. 2018 IEEE international conference on teaching, assessment, and learning for engineering (TALE), Wollongong, NSW, 4–7 December 2018. 2018. URL: https://doi.org/10.1109/tale.2018.8615162

4. Choi Y. Social engineering cyber threats. Journal of global awareness. 2023. Vol. 4, no. 2. P. 1–12. URL: https://doi.org/10.24073/jga/4/02/08

5. Deák V. Social engineering alapú információszerzés a kibertérben megvalósuló lélektani műveletek során. Hadtudományi szemle. 2019. Vol. 12, no. 3. P. 95–111. URL: https://doi.org/10.32563/hsz.2019.3.6

6. Femi-Oyewole F., Osamor V., Okunbor D. A systematic review of social engineering attacks & techniques: the past, present, and future. 2024 international conference on science, engineering and business for driving sustainable development goals (SEB4SDG), Omu-Aran, Nigeria, 2–4 April 2024. 2024. P. 1–12. URL: https://doi.org/10.1109/seb4sdg60871.2024.10629836

7. Guaña-Moya J., Ávila-Pesantez D. Social engineering as the art of deception in cyber-attacks: a mapping review. Information systems and technologies. Cham, 2024. P. 155–163. URL: https://doi.org/10.1007/978-3-031-45642-8_15

8. Karpova N. E., Voskanyan I. I. Threat of social engineering and phishing in modern information security. Digital technology security. 2024. No. 2. P. 69–78. URL: https://doi.org/10.17212/2782-2230-2024-2-69-78

9. Montañez R., Atyabi A., Xu S. Social engineering attacks and defenses in the physical world vs. cyberspace: a contrast study. Cybersecurity and cognitive science. 2022. P. 3–41. URL: https://doi.org/10.1016/b978-0-323-90570-1.00012-7

10. Olchowik M. Analysis and classification of chosen social engineering methods in cybersecurity. Przegląd teleinformatyczny. 2022. Vol. 9 (27), no. 1-4. P. 17–29. URL: https://doi.org/10.5604/01.3001.0016.2880

11. Social engineering / X. Luo et al. Information resources management journal. 2011. Vol. 24, no. 3. P. 1–8. URL: https://doi.org/10.4018/irmj.2011070101

12. Stopochkina I., Ilyin M., Ponomarenko O. Social engineering in modern messengers: applications for offensive security. Information technology: computer science, software engineering and cyber security. 2023. No. 2. P. 84–89. URL: https://doi.org/10.32782/it/2023-2-10

13. That's not a good idea: a robot changes your behavior against social engineering / D. Pasquali et al. HAI '23: international conference on human-agent interaction, Gothenburg Sweden. New York, NY, USA, 2023. URL: https://doi.org/10.1145/3623809.3623879

14. Wang Z., Sun L., Zhu H. Defining social engineering in cybersecurity. IEEE access. 2020. Vol. 8. P. 85094–85115. URL: https://doi.org/10.1109/access.2020.2992807

15. Wang Z., Sun L., Zhu H. Defining social engineering in cybersecurity. IEEE access. 2020. Vol. 8. P. 85094–85115. URL: https://doi.org/10.1109/access.2020.2992807

16. Zhmurko O. Social engineering as a threat to cybersecurity: methods of prevention and protection. Health and safety pedagogy. 2024. Vol. 9, no. 1. P. 37–42. URL: https://doi.org/10.31649/2524-1079-2024-9-1-037-042

17. Akyeşilmen N., Alhosban A. Non-Technical cyber-attacks and international cybersecurity: the case of social engineering. *Gaziantep university*

journal of social sciences. 2024. Vol. 23, no. 1. P. 342–360. URL: https://doi.org/10.21547/jss.1346291

18. Almutairi B. S., Alghamdi A. The role of social engineering in cybersecurity and its impact. *Journal of information security*. 2022. Vol. 13, no. 04. P. 363–379. URL: https://doi.org/10.4236/jis.2022.134020

19. Choi Y. Social engineering cyber threats. *Journal of global awareness*. 2023. Vol. 4, no. 2. P. 1–12. URL: https://doi.org/10.24073/jga/4/02/08

20. Exploring social engineering attacks involving insights from case studies / S. Kakarla et al. *Advances in information security, privacy, and ethics*. 2024. P. 13–60. URL: https://doi.org/10.4018/979-8-3693-6665-3.ch002

21. Kulkarni A. V., Nath S. Human Susceptibility to Social Engineering Attacks: an innovative approach to social change. *2024 IEEE international conference on interdisciplinary approaches in technology and management for social innovation (IATMSI)*, Gwalior, India, 14–16 March 2024. 2024. URL: https://doi.org/10.1109/iatmsi60426.2024.10502492

22. Montañez R., Golob E., Xu S. Human cognition through the lens of social engineering cyberattacks. *Frontiers in psychology*. 2020. Vol. 11. URL: https://doi.org/10.3389/fpsyg.2020.01755

23. Montañez R., Golob E., Xu S. Human cognition through the lens of social engineering cyberattacks. *Frontiers in psychology*. 2020. Vol. 11. URL: https://doi.org/10.3389/fpsyg.2020.01755

24. Outcomes of social engineering: understanding cybercriminals' exploitation of human psychology / D. K. K. M et al. *Interantional journal of scientific research in engineering and management*. 2024. Vol. 08, no. 11. P. 1–7. URL: https://doi.org/10.55041/ijsrem39133

25. Pallivalappil A. S., S. N. J., K. K. P. Social engineering attacks on facebook – A case study. *International journal of case studies in business, IT, and education*. 2021. P. 299–313. URL: https://doi.org/10.47992/ijcsbe.2581.6942.0135

26. Siddiqi M. A., Pak W., Siddiqi M. A. A study on the psychology of social engineering-based cyberattacks and existing countermeasures. *Applied sciences*. 2022. Vol. 12, no. 12. P. 6042. URL: https://doi.org/10.3390/app12126042

27. Sillanpää M., Hautamäki J. Social engineering intrusion. *IAIT2020: the 11th international conference on advances in information technology*, Bangkok Thailand. New York, NY, USA, 2020. URL: https://doi.org/10.1145/3406601.3406631

28. Social engineering attacks prevention: a systematic literature review / W. Syafitri et al. *IEEE access*. 2022. Vol. 10. P. 39325–39343. URL: https://doi.org/10.1109/access.2022.3162594

29. Social engineering in social media and online interactions / T. K. Vashishth et al. *Advances in information security, privacy, and ethics*. 2024. P. 257–292. URL: https://doi.org/10.4018/979-8-3693-6665-3.ch012

30. Son S. Social engineering in the digital age of social media : master's thesis. URL: https://ruj.uj.edu.pl/xmlui/handle/item/238917

31. Wibowo B. Social engineering as a major cybersecurity threat: analysis of challenges and solutions for organizations. *International journal of science education and cultural studies*. 2024. Vol. 3, no. 2. P. 57–65. URL: https://doi.org/10.58291/ijsecs.v3i2.306

32. Wulandari N., Adnan M. S., Wicaksono C. B. Are you a soft target for cyber attack? Drivers of susceptibility to social engineering-based cyber attack (SECA): a case study of mobile messaging application. *Human behavior and emerging technologies*. 2022. Vol. 2022. P. 1–10. URL: https://doi.org/10.1155/2022/5738969

33. Zhmurko O. Social engineering as a threat to cybersecurity: methods of prevention and protection. *Health and safety pedagogy*. 2024. Vol. 9, no. 1. P. 37–42. URL: https://doi.org/10.31649/2524-1079-2024-9-1-037-042

34. Половенко Л. П., Мерінова С. В. Виявлення ознак соціальної інженерії та технологія протидії соціальним хакерам на підприємстві. *Підприємництво та інновації*. 2019. № 10. С. 183–187. URL: https://doi.org/10.37320/2415-3583/10.28

35. A comprehensive analysis of social engineering attacks: from phishing to prevention - tools, techniques and strategies / S. Gupta et al. *2024 second international conference on intelligent cyber physical systems and internet of things (icoici)*, Coimbatore, India, 28–30 August 2024. 2024. P. 1–8. URL: https://doi.org/10.1109/icoici62503.2024.10696444

36. A comprehensive survey on social engineering-based attacks on social networks / A. Naz et al. *International Journal of ADVANCED AND APPLIED SCIENCES*. 2024. Vol. 11, no. 4. P. 139–154. URL: https://doi.org/10.21833/ijaas.2024.04.016

37. Birthriya S. K., Ahlawat P., Jain A. K. A comprehensive survey of social engineering attacks: taxonomy of attacks, prevention, and mitigation strategies. *Journal of applied security research*. 2024. P. 1–49. URL: https://doi.org/10.1080/19361610.2024.2372986

38. Exploring social engineering attacks involving insights from case studies / S. Kakarla et al. *Advances in information security, privacy, and ethics*. 2024. P. 13–60. URL: https://doi.org/10.4018/979-8-3693-6665-3.ch002

39. Flack J. C., D'Souza R. M. The digital age and the future of social network science and engineering. *Proceedings of the IEEE*. 2014. Vol. 102, no. 12. P. 1873–1877. URL: https://doi.org/10.1109/jproc.2014.2368790

40. Haggag M. H. Social engineering attacks detection techniques: survey study. *International journal of engineering and computer science*. 2017. URL: https://doi.org/10.18535/ijecs/v6i1.09

41. Kotkova B., Blahova M. Cyberterrorism and social engineering - methods and countermeasures. *23rd SGEM international multidisciplinary scientific geoconference 2023*, Albena, Bulgaria, 3–9 July 2023. 2023. URL: https://doi.org/10.5593/sgem2023/2.1/s07.08

42. Masinde N., Graffi K. Peer-to-Peer-Based social networks: a comprehensive survey. *SN computer science*. 2020. Vol. 1, no. 5. URL: https://doi.org/10.1007/s42979-020-00315-8

43. Mitigating social engineering for improved cybersecurity / E. U. Osuagwu et al. *2015 international conference on cyberspace (cyber-abuja)*, Abuja, Nigeria, 4–7 November 2015. 2015. URL: https://doi.org/10.1109/cyber-abuja.2015.7360515

44. Mr S. M. A. s., Mr A. A., Mr M. A. A. Social Engineering threats and Countermeasures in SHCT. *International journal of business intelligent*. 2019. Vol. 8, no. 2. URL: https://doi.org/10.20894/ijbi.105.008.002.004

45. Salahdine F., Kaabouch N. Social engineering attacks: a survey. *Future internet*. 2019. Vol. 11, no. 4. P. 89. URL: https://doi.org/10.3390/fi11040089

46. Samojlova A. A. Social engineering methods. *Scientific development trends and education*. 2019. URL: https://doi.org/10.18411/lj-11-2019-48

47. Sokolov V., Korzhenko O. Analysis of recent attacks based on social engineering techniques. *SSRN electronic journal*. 2018. URL: https://doi.org/10.2139/ssrn.3455471

48. Кравець С.В. Використання соціальної інженерії в сучасних кібератаках: кейс-дослідження та розробка рекомендацій щодо захисту. *Стратегії кіберстійкості: управління ризиками та безперервність бізнесу*: матеріали всеукр. наук.-практ. конф., м. Київ, 27 лютого 2025 р. С. 232-235. URL: https://duikt.edu.ua/uploads/p_2779_46212583.pdf