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 ІНТЕГРАЦІЇ СОЦІОІНЖЕНЕРНИХ СЦЕНАРІЇВ У ПРОЦЕС ТЕСТУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ”

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

_____ Максим КАРПЕНКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-42

Максим КАРПЕНКО
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

Карпенку Максиму Анатолійовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Методика інтеграції соціоінженерних сценаріїв у процес тестування інформаційної безпеки”,
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, соціоінженерні сценарії, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
4.1. Вивчити особливості соціальної інженерії як інструменту впливу на інформаційну безпеку.
4.2. Проаналізувати соціоінженерні сценарії в процесі тестування інформаційної безпеки.
4.3.Дослідити та розробити рекомендації щодо впровадження соціоінженерних сценаріїв у процес тестування інформаційної безпеки.

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 як інструменту впливу на інформаційну безпеку.	08.04.2025	
4.	Аналіз соціоінженерних сценаріїв у процесі тестування інформаційної безпеки	22.04.2025	
5.	Дослідження та розробка рекомендацій щодо впровадження соціоінженерних сценаріїв у процес тестування інформаційної безпеки.	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 _____ Максим КАРПЕНКО
(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 Карпенко М.А. 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 інтеграції соціоінженерних сценаріїв у процес тестування інформаційної безпеки"

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач КАРПЕНКО Максим у кваліфікаційній роботі вивчив особливості соціальної інженерії як інструменту впливу на інформаційну безпеку, проаналізував соціоінженерні сценарії в процесі тестування інформаційної безпеки, дослідив та розробив рекомендації щодо впровадження соціоінженерних сценаріїв у процес тестування інформаційної безпеки.

КАРПЕНКО Максим 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 КАРПЕНКА Максима 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 Карпенко М.А. 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 КАРПЕНКА Максима
на тему “Методика інтеграції соціоінженерних сценаріїв у процес тестування інформаційної безпеки”

Актуальність. У сучасному цифровому середовищі, де загрози інформаційній безпеці стають дедалі складнішими, соціальна інженерія залишається одним із найнебезпечніших і водночас найменш контрольованих методів реалізації кібератак. Зловмисники дедалі частіше використовують психологічні маніпуляції, щоб обійти технічні засоби захисту й отримати несанкціонований доступ до інформації. Це створює нагальну потребу у впровадженні комплексних методик, що дозволяють не лише виявляти подібні загрози, але й інтегрувати соціоінженерні сценарії до системного процесу тестування інформаційної безпеки. Формування таких підходів сприятиме виявленню вразливостей у людському факторі та підвищенню загальної кіберстійкості організацій. Розробка й апробація методики інтеграції соціоінженерних сценаріїв у процес безпекового тестування є актуальним і важливим науково-прикладним завданням.

Позитивні сторони.

1. У роботі проведено детальний аналіз соціоінженерних атак та їхнього впливу на інформаційну безпеку, із виокремленням типових сценаріїв та векторів впливу.
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 широкий спектр джерел: близько 50 публікацій, в тому числі англомовних.
4. За результатами дослідження запропоновано рекомендації щодо впровадження соціоінженерного тестування в корпоративне середовище.

Недоліки.

Робота могла б бути доповнена глибшим аналізом програмних засобів, що застосовуються для реалізації соціоінженерного тестування — зокрема платформ для симульованого фішингу, навчання персоналу та оцінки результатів тестування.

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 КАРПЕНКО Максим 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 інтеграції соціоінженерних сценаріїв у процес тестування інформаційної безпеки. Робота складається зі вступу, трьох розділів, що містять 6 рисунків та 7 таблиць, висновків і списку використаних джерел із 49 найменувань. Загальний обсяг роботи становить 75 аркушів, з яких 6 аркушів займає список використаних джерел.

Метою роботи є обґрунтування методики інтеграції соціоінженерних сценаріїв у процес тестування інформаційної безпеки, а також аналіз практик їхнього застосування для виявлення вразливостей, зумовлених людським фактором.

Об'єктом дослідження є процеси забезпечення інформаційної та кібербезпеки в організаціях з урахуванням людського чинника як складової системи захисту.

Предмет дослідження – методи моделювання соціоінженерних атак, принципи їх інтеграції в тестування безпеки, а також підходи до підвищення ефективності виявлення та нейтралізації подібних загроз.

Методи дослідження. У процесі дослідження застосовано методи аналізу й синтезу інформації, порівняльний аналіз технік соціальної інженерії, класифікацію сценаріїв атак, експертне оцінювання ефективності тестування та системний підхід до розробки і впровадження заходів інформаційної безпеки.

Як результат у роботі вивчено особливості соціальної інженерії як інструменту впливу на інформаційну безпеку, проаналізовано соціоінженерні сценарії в процесі тестування інформаційної безпеки, досліджено та розроблено рекомендації щодо впровадження соціоінженерних сценаріїв у процес тестування інформаційної безпеки.

Галузь застосування. Запропонована методика може бути використана у практиці тестування інформаційної безпеки підприємств, установ і організацій, а також у розробці навчальних програм з підвищення обізнаності персоналу

щодо соціоінженерних загроз.

Ключові слова: СОЦІАЛЬНА ІНЖЕНЕРІЯ, ТЕСТУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, СОЦІОІНЖЕНЕРНІ СЦЕНАРІЇ, ВРАЗЛИВОСТІ ЛЮДСЬКОГО ФАКТОРУ, ПРОТИДІЯ КІБЕРАТАКАМ, НАВЧАННЯ КОРИСТУВАЧІВ.

ABSTRACT

The qualification work is devoted to the study of the methodology for integrating socio-engineering scenarios into the information security testing process. The work consists of an introduction, three chapters containing 6 figures and 7 tables, conclusions and the list of references containing 49 items. The total volume of the work is 75 pages, of which 6 pages are occupied by the the list of references.

The purpose of the study is to substantiate the methodology for integrating socio-engineering scenarios into the information security testing process, as well as to analyse the practices of their application to identify vulnerabilities caused by the human factor.

The object the study is the processes of ensuring information and cybersecurity in organisations, taking into account the human factor as a component of the protection system.

The subject of the study is methods of modelling socio-engineering attacks, principles of their integration into security testing, as well as approaches to improving the efficiency of detecting and neutralising such threats.

Research methods. In the course of the study, the methods of information analysis and synthesis, comparative analysis of social engineering techniques, classification of attack scenarios, expert evaluation of testing efficiency and a systematic approach to the development and implementation of information security measures were applied.

As a result, the paper examines the features of social engineering as a tool for influencing information security, analyses social engineering scenarios in the process of information security testing, and studies and develops recommendations for implementing social engineering scenarios in the process of information security testing.

Field of application. The proposed methodology can be used in the practice of testing the information security of enterprises, institutions and organisations, as well as in the development of training programmes to raise staff awareness of socio-

engineering threats.

Keywords: SOCIAL ENGINEERING, INFORMATION SECURITY TESTING, SOCIO-ENGINEERING SCENARIOS, HUMAN FACTOR VULNERABILITIES, COUNTERING CYBERATTACKS, USER TRAINING.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ІБ	Інформаційна безпека
КСЗІ	Комплексна система захисту інформації
ПЗ	Програмне забезпечення
ОС	Операційна система
АС	Автоматизована система
БД	База даних
СОІ	Соціальна інженерія
СІС	Соціоінженерний сценарій
ФІ	Фішинг
BEC	Business Email Compromise (компрометація ділової пошти)
MFA	Multi-Factor Authentication (багатофакторна автентифікація)
IDS	Intrusion Detection System (система виявлення вторгнень)
SIEM	Security Information and Event Management (система управління подіями та інформацією безпеки)
CISO	Chief Information Security Officer (керівник служби інформаційної безпеки)
DLP	Data Loss Prevention (запобігання витоку даних)
OSINT	Open-Source Intelligence (розвідка на основі відкритих джерел)
GDPR	General Data Protection Regulation (Загальний регламент захисту даних ЄС)
CVE	Common Vulnerabilities and Exposures (загальновідомі вразливості)
UI	User Interface (користувацький інтерфейс)
HR	Human Resources (відділ кадрів/персоналу)

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 – обґрунтування методики інтеграції соціоінженерних сценаріїв у процес тестування інформаційної безпеки, а також аналіз практик їхнього застосування для виявлення вразливостей, зумовлених людським фактором.

Об’єкт дослідження – процеси забезпечення інформаційної та кібербезпеки в організаціях з урахуванням людського чинника як складової системи захисту.

Предмет дослідження – методи моделювання соціоінженерних атак, принципи їх інтеграції в тестування безпеки, а також підходи до підвищення ефективності виявлення та нейтралізації подібних загроз.

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

1. Вивчити особливості соціальної інженерії як інструменту впливу на інформаційну безпеку.

2. Проаналізувати соціоінженерні сценарії в процесі тестування

інформаційної безпеки.

3. Дослідити та розробити рекомендації щодо впровадження соціоінженерних сценаріїв у процес тестування інформаційної безпеки.

Методи дослідження. У процесі дослідження застосовано методи аналізу й синтезу інформації, порівняльний аналіз технік соціальної інженерії, класифікацію сценаріїв атак, експертне оцінювання ефективності тестування та системний підхід до розробки і впровадження заходів інформаційної безпеки.

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 ЯК ІНСТРУМЕНТ ВПЛИВУ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ

У сучасних умовах розвитку інформаційного суспільства дедалі важливішого значення набуває людський фактор як один із ключових елементів системи інформаційної безпеки. Технічні засоби захисту поступово вдосконалюються, однак при цьому саме користувачі залишаються найбільш вразливою ланкою. Соціальна інженерія, як сукупність методів психологічного впливу з метою отримання конфіденційної інформації або доступу до інформаційних систем, стала потужним інструментом для кібератак.

1.1 Теоретичні та методологічні основи соціальної інженерії

Соціальна інженерія в контексті інформаційної безпеки розглядається як сукупність методів психологічного впливу, спрямованих на отримання несанкціонованого доступу до конфіденційної інформації або ресурсів шляхом маніпуляції поведінкою користувачів. Цей підхід базується на використанні людських слабкостей, таких як довіра, страх, бажання допомогти або уникнути конфлікту, що робить його особливо ефективним у сучасному цифровому середовищі.

Теоретичні підходи до вивчення соціальної інженерії включають міждисциплінарні дослідження, що поєднують психологію, соціологію, кібербезпеку та поведінкову економіку. Одним із ключових аспектів є розуміння того, як зловмисники використовують психологічні принципи для маніпуляції поведінкою жертв. Наприклад, Роберт Чалдіні у своїй теорії впливу виділяє шість основних принципів: взаємність, зобов'язання та послідовність, соціальне підтвердження, авторитет, симпатія та дефіцит [1]. Ці принципи широко застосовуються в соціоінженерних атаках для створення ситуацій, у яких жертва відчуває себе зобов'язаною виконати певну дію або надати інформацію.

Теорія запланованої поведінки, розроблена Айзеном та Фішбейном,

пояснює, як наміри особи впливають на її поведінку. Згідно з цією теорією, поведінка визначається намірами, які, у свою чергу, залежать від ставлення до поведінки, суб'єктивних норм та сприйняття контролю над поведінкою. Зловмисники можуть впливати на ці фактори, створюючи ситуації, в яких жертва відчуває соціальний тиск або вважає, що має обмежений контроль над ситуацією, що спонукає її до небажаних дій [2].

У сфері інформаційної безпеки соціальна інженерія розглядається як одна з найсерйозніших загроз, оскільки вона обходить технічні засоби захисту, спрямовуючи атаки безпосередньо на користувачів. Це підкреслює важливість розуміння психологічних механізмів, що лежать в основі соціоінженерних атак, для розробки ефективних стратегій захисту.

Одним із підходів до вивчення соціальної інженерії є створення онтологій, які описують основні поняття та взаємозв'язки в цій галузі. Наприклад, дослідники розробили онтологію соціальної інженерії в кібербезпеці, яка включає 11 основних концепцій та 22 типи взаємозв'язків між ними [3]. Ця онтологія дозволяє формалізувати знання про соціоінженерні атаки та використовувати їх для аналізу інцидентів, виявлення вразливостей та розробки заходів протидії.

Наступним підходом є вивчення когнітивних упереджень, які зловмисники використовують для маніпуляції поведінкою жертв. Серед них можна виділити ефект прив'язки, коли особа надає надмірне значення першій отриманій інформації; ефект підтвердження, коли людина шукає інформацію, що підтверджує її переконання; та ефект авторитету, коли особа підкоряється вказівкам авторитетної фігури. Розуміння цих упереджень дозволяє розробляти ефективні стратегії навчання та підвищення обізнаності користувачів.

Важливо також враховувати роль емоцій у прийнятті рішень. Зловмисники часто використовують емоційні тригери, такі як страх, терміновість або співчуття, щоб змусити жертву діяти імпульсивно. Наприклад, фішингові листи можуть містити повідомлення про термінову необхідність змінити пароль або підтвердити особисті дані, що спонукає користувача до негайних дій без

належної перевірки.

Теоретичні підходи до вивчення соціальної інженерії в інформаційній безпеці включають аналіз психологічних механізмів впливу, когнітивних упереджень, емоційних тригерів та соціальних норм. Розуміння цих аспектів є ключовим для розробки ефективних заходів протидії соціоінженерним атакам, включаючи навчання персоналу, впровадження політик безпеки та використання технічних засобів захисту.

Класифікація технік та методів соціальної інженерії є ключовим етапом у розумінні механізмів, які використовують зловмисники для отримання несанкціонованого доступу до інформації або систем. Ці методи базуються на психологічних маніпуляціях і експлуатації людських слабкостей, що робить їх особливо небезпечними [4]. Розглянемо основні категорії та приклади таких технік (табл. 1.1).

Фішинг — одна з найпоширеніших форм соціальної інженерії. Зловмисники надсилають електронні листи, які імітують повідомлення від відомих організацій, з метою змусити користувача перейти за шкідливим посиланням або надати конфіденційну інформацію. Цей метод часто використовується для збору облікових даних або встановлення шкідливого програмного забезпечення на пристрої жертви. Існують різновиди фішингу, такі як **вішинг** (використання телефонних дзвінків для отримання інформації) та **смішинг** (надсилання шкідливих SMS-повідомлень).

Претекстинг полягає у створенні вигаданого сценарію або особи, щоб змусити жертву розкрити конфіденційну інформацію. Зловмисник може видавати себе за співробітника служби безпеки або технічної підтримки, щоб отримати доступ до систем або даних. Цей метод вимагає ретельної підготовки та збору інформації про жертву для створення правдоподібного претексту.

Бейтинг (від англ. bait — приманка) передбачає використання фізичних або цифрових приманок для заманювання жертви. Наприклад, зловмисник може залишити заражений USB-накопичувач у громадському місці з надією, що хтось підключить його до комп'ютера, що призведе до встановлення шкідливого ПЗ.

Цей метод експлуатує людську цікавість та необережність.

Плечовий серфінг (англ. shoulder surfing) — спостереження за жертвою під час введення нею конфіденційної інформації, наприклад, паролів або PIN-кодів. Це може відбуватися в громадських місцях, таких як кафе або транспорт. Зловмисник використовує візуальні підказки для збору інформації без прямого контакту з жертвою.

Обратна соціальна інженерія передбачає створення ситуації, в якій жертва сама звертається до зловмисника за допомогою. Наприклад, зловмисник може викликати проблему в системі жертви, а потім запропонувати свою допомогу у її вирішенні, отримуючи при цьому доступ до конфіденційної інформації. Цей метод базується на довірі та бажанні жертви швидко вирішити проблему.

Спрямований фішинг (спірфішинг) — атака, спрямована на конкретну особу або організацію. Зловмисники збирають детальну інформацію про жертву для створення персоналізованих повідомлень, що підвищує ймовірність успішної атаки. Цей метод часто використовується проти керівників компаній або осіб з доступом до важливої інформації.

Фармінг — перенаправлення користувачів на фальшиві веб-сайти, які імітують легітимні ресурси. Це досягається шляхом зміни налаштувань DNS або використання шкідливого ПЗ. Користувач, не підозрюючи нічого, вводить свої облікові дані на підробленому сайті, що призводить до їх компрометації.

Соціальні мережі також є платформою для соціальної інженерії. Зловмисники можуть створювати фальшиві профілі або використовувати зібрану з відкритих джерел інформацію для встановлення довіри з жертвою. Це може призвести до розголошення конфіденційної інформації або встановлення шкідливих програм.

Інсайдерські загрози виникають, коли співробітники організації свідомо або несвідомо сприяють зловмисникам. Це може бути результатом маніпуляцій, шантажу або просто необережності. Інсайдери мають доступ до внутрішніх систем і можуть завдати значної шкоди без необхідності зовнішнього втручання.

Таблиця 1.1

Порівняльна таблиця методів соціальної інженерії

Метод / Техніка	Опис	Ціль	Приклади	Рівень складності	Ефективність
Фішинг	Масові розсилки підроблених повідомлень (емейли, SMS) з метою виманювання даних або завантаження шкідливого ПЗ.	Отримання логінів, паролів, банківських даних.	Листи від "банку" з посиланням на фішинговий сайт.	Низький	Висока (через масштабність)
Спрямований фішинг (Spear Phishing)	Персоналізовані атаки на конкретних осіб/організації з використанням детальної інформації про жертву.	Викрадення конфіденційних даних, доступів.	Лист від "керівника" з проханням переказати кошти.	Середній/Високий	Дуже висока
Претекстинг	Використання вигаданого сценарію (легенди) для отримання інформації.	Отримання даних через довіру (наприклад, під виглядом техпідтримки).	Дзвінок "з IT-відділу" з проханням надати пароль.	Середній	Висока
Бейтинг	Заманювання жертви на заражений носій (флешка, сайт) через цікаву пропозицію.	Зараження ПЗ або викрадення даних.	Підкинута флешка з позначкою "Зарплатна відомість".	Низький/Середній	Середня
Плечовий серфінг	Візуальне підглядання паролів, PIN-кодів у громадських місцях.	Отримання доступу до акаунтів, платіжних систем.	Підгляд пароля в кафе або транспорті.	Низький	Залежить від обережності жертви

Продовження табл. 1.1

Зворотна соціальна інженерія	Жертву спонукають самостійно звернутися до зловмисника (наприклад, під виглядом допомоги).	Викрадення даних через "довіру" після звернення жертви.	Підроблений сайт техпідтримки з кнопкою "Допомога".	Високий	Висока
Фармінг	Перенаправлення жертви на фальшиві сайти через підміну DNS або шкідливі скрипти.	Крадіжка даних через підроблені вебсторінки.	Автоматичне перенаправлення на фішинговий сайт банку.	Високий	Дуже висока

Розуміння та класифікація методів соціальної інженерії є важливим кроком у розробці ефективних стратегій захисту. Освіта користувачів, впровадження політик безпеки та використання технологічних рішень можуть значно знизити ризик успішних атак. Організації повинні постійно оновлювати свої знання про нові методи соціальної інженерії та адаптувати свої заходи безпеки відповідно до змін у загрозах.

Соціальна інженерія залишається однією з найнебезпечніших загроз у сфері інформаційної безпеки, оскільки вона спрямована на експлуатацію людського фактора. Зловмисники використовують психологічні методи впливу для отримання несанкціонованого доступу до конфіденційної інформації, що робить такі атаки особливо ефективними. Розгляд реальних прикладів використання соціальної інженерії дозволяє краще зрозуміти механізми цих атак та розробити ефективні стратегії захисту (табл. 1.2.).

Одним із найвідоміших випадків є кібератака на роздрібну мережу Target у 2013 році [5]. Хакери отримали доступ до системи компанії через фірму-підрядника з обслуговування кондиціонерів, використовуючи фішинговий лист для встановлення шкідливого програмного забезпечення. Це дозволило їм викрасти дані понад 40 мільйонів кредитних і дебетових карток клієнтів.

У 2016 році відбулася одна з наймасштабніших кібератак на банківську систему — пограбування Центрального банку Бангладеш [6]. Хакери надіслали

фішингові листи співробітникам банку, встановили шкідливе ПЗ та отримали доступ до системи SWIFT. Вони намагалися перевести майже 1 мільярд доларів, з яких 81 мільйон було успішно виведено.

У 2020 році відбулася масштабна атака на Twitter, коли хакери отримали доступ до облікових записів відомих осіб і компаній [7]. Вони використали методи соціальної інженерії для обману співробітників Twitter, отримали доступ до внутрішніх інструментів і розмістили шахрайські повідомлення з проханням переказати біткоїни. Ця атака продемонструвала вразливість навіть великих технологічних компаній до соціоінженерних методів.

У 2014 році група "Guardians of Peace" здійснила атаку на Sony Pictures Entertainment, використовуючи фішингові листи для отримання доступу до внутрішніх систем компанії [8]. Хакери викрали та оприлюднили конфіденційні дані, включаючи електронні листи, фінансові звіти та невипущені фільми. Ця атака підкреслила важливість захисту від соціальної інженерії навіть для великих корпорацій.

У 2023 році британська інженерна компанія Arup стала жертвою шахрайства із використанням відео, згенерованого штучним інтелектом. Співробітник компанії був обманутий і перевів 20 мільйонів фунтів стерлінгів на рахунки шахраїв, які видавали себе за керівництво компанії під час відеодзвінка. Цей випадок демонструє, як новітні технології можуть бути використані для соціоінженерних атак [9].

У 2016 році хакери, пов'язані з російською військовою розвідкою, здійснили фішингову атаку на членів передвиборчої кампанії Гілларі Клінтон. Вони надіслали фішингові листи, замасковані під повідомлення від Google, що дозволило їм отримати доступ до електронної пошти та викрасти тисячі конфіденційних документів [10].

Таблиця 1.2

Відомі кібератаки із використанням соціальної інженерії

Рік	Компанія / Організація	Метод атаки	Наслідки	Сума збитків / Обсяг витоку
2013	Target (роздрібна мережа)	Фішинг (через підрядника HVAC)	Викрадення даних 40+ млн кредитних карток	Понад $200 млн (штрафи, компенсації)
2014	Sony Pictures Entertainment	Фішинг (внутрішні системи)	Витік конфіденційних даних, фільмів, листів	~$100 млн (втрати, репутаційні збитки)
2016	Центральний банк Бангладеш	Фішинг + шкідливе ПЗ (SWIFT)	Крадіжка через міжбанківські перекази	81млн(зпланованих81млн(зпланованих1 млрд)
2016	Передвиборча кампанія Гілларі Клінтон	Фішинг (листи "від Google")	Викрадення електронної пошти, тисяч документів	Політичні наслідки, втручання у вибори США
2020	Twitter	Соціальна інженерія (обман співробітників)	Доступ до акаунтів знаменитостей, шахрайські твіти	~$118 тис. (в біткоїнах), репутаційні збитки
2023	Arup (інженерна компанія)	Deepfake-відео (штучний інтелект)	Обман співробітника, переказ коштів	£20 млн (25 млн доларів)

Ці приклади свідчать про те, що соціальна інженерія є потужним інструментом у руках зловмисників. Вони використовують довіру, необізнаність та психологічні особливості людей для досягнення своїх цілей. Для ефективного захисту необхідно не лише впроваджувати технічні засоби безпеки, але й проводити навчання персоналу, підвищувати обізнаність про методи соціальної інженерії та розробляти політики безпеки, що враховують людський фактор.

Соціоінженерні атаки — це форма кібератак, яка орієнтована на маніпулювання людським фактором для отримання несанкціонованого доступу до систем або інформації. Вони ґрунтуються на використанні психологічних методів впливу на жертву, що дозволяють атакувальнику обманним шляхом здобути необхідні ресурси. Методологічні принципи і етапи реалізації соціоінженерних атак є ключовими для розуміння механізмів, що лежать в основі цих загроз.

Збір інформації є першим етапом реалізації соціоінженерної атаки. Він полягає в акумуляції відомостей про ціль, зокрема про її організаційну структуру, технологічне забезпечення, зв'язки між працівниками та специфіку діяльності. Основною метою цього етапу є отримання достатньої кількості даних, щоб побудувати правдоподібний сценарій для подальших маніпуляцій. Інформація може бути зібрана з різних джерел, таких як соціальні мережі, відкриті бази даних, публічні документи або навіть через особисте спостереження за жертвами.

На основі зібраної інформації атакувальник створює сценарій для подальшої атаки [11]. Це другий етап, в рамках якого визначається, як саме будуть реалізовані маніпуляції з жертвою. Сценарій повинен бути не тільки переконливим, але й таким, щоб не викликати у підсвідомості жертви сумнівів. Атакувальники можуть вибирати різні методи впливу, від фальшивих електронних листів до створення фальшивих веб-сайтів або телефонних дзвінків, що видають себе за представників довірених осіб чи організацій. Важливим аспектом є вибір інструментів і тактик, що дозволяють максимально сховати справжній намір, не привертаючи увагу до несправжності ситуації.

Наступний етап — це встановлення довіри. Для того, щоб атака була успішною, атакувальник повинен створити умови, за яких жертва буде готова довіряти йому. Це може включати використання соціальних навичок, таких як симпатія, авторитет або співпереживання, що дозволяє переконати жертву виконати необхідні дії, не підозрюючи про небезпеку. Установлення довіри може проходити як через особисті зустрічі, так і через онлайн-комунікацію, де

атакувальник маніпулює поведінкою жертви за допомогою психологічних прийомів, таких як апеляція до емоцій або переконання у вигоді від співпраці.

Після встановлення довіри наступає етап маніпуляції. Тут атакувальник безпосередньо здійснює вплив на рішення жертви, спрямовуючи її до виконання певних дій, що вигідні для нього. Це можуть бути дії на кшталт надання конфіденційної інформації, доступу до систем або виконання інших небезпечних для безпеки організації або особистості вчинків. Маніпуляція може включати техніки підвищення тиску або використання часу як фактору для досягнення бажаного результату. Водночас, атакувальник може створювати враження невідкладності або загрози, що спонукає жертву швидко реагувати, не усвідомлюючи реальних наслідків своїх дій.

Завершальним етапом є реалізація мети атаки. На цьому етапі атакувальник досягає своєї мети — чи то отримання доступу до системи, крадіжка конфіденційної інформації, чи завдання іншої шкоди. Важливою особливістю цього етапу є те, що жертва, зазвичай, не усвідомлює, що стала частиною атаки, і, отже, не має можливості заблокувати подальші кроки атакувальника. Після реалізації мети атакувальник може залишити жертву з її проблемами або використовувати отриману інформацію для подальших маніпуляцій. Однак варто зазначити, що успішна реалізація мети може бути лише тимчасовим результатом. Якщо жертва або організація виявить факт атаки, це може призвести до розкриття схеми соціоінженера, а також до вжиття заходів безпеки для уникнення подібних інцидентів у майбутньому.

Успіх соціоінженерної атаки багато в чому залежить від ефективності виконання кожного етапу та здатності атакувальника використовувати найкращі методи для маніпулювання жертвою. Цей процес не є випадковим, а є результатом детальної підготовки, вивчення слабких місць та психології людей. Тому підприємствам і організаціям важливо постійно навчати своїх співробітників, підвищувати їх обізнаність про соціоінженерні загрози і розвивати навички, які дозволяють відрізняти реальні запити від потенційно небезпечних [12].

Технологічний розвиток та використання сучасних інструментів дозволяють атакувальникам використовувати нові методи для обміну інформацією, що ускладнює виявлення атак. Саме тому важливо, щоб організації не лише навчали своїх співробітників, а й постійно вдосконалювали систему безпеки, інтегруючи новітні технології для виявлення і блокування соціоінженерних атак на всіх етапах їх виконання.

1.2 Досвід використання соціальної інженерії в аспекті забезпечення інформаційної безпеки

Соціальна інженерія стала однією з найбільш розповсюджених і небезпечних загроз для організацій усіх рівнів. З кожним роком зловмисники вдосконалюють свої методи, використовуючи психологічний вплив, маніпуляції та інші техніки для досягнення своїх цілей — крадіжки конфіденційної інформації, доступу до корпоративних систем або завдання шкоди репутації організацій [13]. Тому важливо ретельно вивчати досвід використання соціальної інженерії, щоб створити ефективні стратегії для протидії цим загрозам і забезпечення належного рівня захисту інформаційних ресурсів.

Соціоінженерія, як метод атаки, здобуває все більшу популярність через свою здатність маніпулювати людьми і обхід традиційних засобів безпеки. Атаки такого типу здійснюються через психологічні маніпуляції, де зловмисники використовують людські слабкості, соціальні навички та недосконалість систем для досягнення своїх цілей. Успішні соціоінженерні атаки на організації часто призводять до серйозних наслідків, таких як крадіжка фінансових засобів, витік конфіденційної інформації, або навіть серйозні порушення в роботі компанії. Для розуміння масштабів загрози та способів протидії важливо розглядати конкретні приклади таких атак.

Фішинг є одним із найбільш розповсюджених видів соціоінженерних атак, що спрямовані на обман жертв через електронну пошту або інші засоби комунікації. Зловмисники створюють фальшиві електронні листи, які

виглядають як офіційні повідомлення від надійних джерел, таких як банки, корпоративні служби підтримки, або навіть державні установи. Вони часто використовують логотипи, фірмові шрифти та інші візуальні елементи, щоб листи виглядали як справжні.

Прикладом такого типу атаки є фішинг-кампанія, яка вразила компанії, що здійснюють електронні платежі, у 2016 році. Зловмисник, маскуючись під одного з постачальників, відправив електронний лист, в якому був запит на перерахування значної суми грошей. Оскільки цей лист виглядав абсолютно легітимно і містив всю необхідну інформацію, співробітники компаній виконали запит без додаткових перевірок. В результаті зловмисник зміг отримати понад 100 мільйонів доларів [14]. Це був один із найбільших відомих випадків фішингових атак, що демонструє, як просте введення помилкової інформації може призвести до серйозних фінансових втрат.

Іншим популярним методом соціоінженерії є створення фальшивих вебсайтів, що імітують легітимні платформи для збору чутливої інформації [15]. Цей метод часто використовується в поєднанні з фішингом або іншими атаками. Зловмисники створюють вебсайти, що виглядають схожими на офіційні ресурси банків, онлайн-магазинів або інтернет-платежних систем, і запрошують жертву ввести свої особисті дані, такі як логіни, паролі та номери кредитних карток.

У 2017 році було зафіксовано кілька випадків використання такого методу для атаки на банківські установи [16]. Зловмисники створили фальшиві вебсайти, які імітували банківські платіжні платформи. Після того як користувачі вводили свої платіжні дані, ці дані одразу потрапляли до рук кіберзлочинців. В результаті таких атак було вкрадено мільйони доларів, і кілька банків були змушені вжити надзвичайних заходів для захисту своїх клієнтів і відновлення репутації.

Атаки через злам корпоративної електронної пошти або бізнес-емейл компрамайз (BEC) є ще однією потужною формою соціоінженерії, яка не передбачає використання традиційних технічних вразливостей у програмному забезпеченні чи апаратних засобах [17]. Зловмисники у цих випадках

використовують фальшиві електронні листи або змінюють адресу електронної пошти, щоб здаватися представниками високого рівня компанії, такими як генеральний директор або фінансовий директор.

Одним із найбільш відомих випадків BEC-атаки був інцидент, що стався з компанією "Ubiquiti Networks" у 2015 році [18]. Зловмисники надіслали співробітникам фальшиві запити на здійснення переказу великих сум грошей, які були підписані, начебто, генеральним директором компанії. Через брак перевірок в компанії жертви здійснили платіж, що в результаті призвело до втрати понад 40 мільйонів доларів. Цей випадок став сигналом для багатьох організацій, що почали інвестувати в посилення своїх внутрішніх процедур і навчання співробітників для запобігання подібним атакам.

В останні роки соціальні мережі стали потужним інструментом для здійснення соціоінженерних атак. Зловмисники використовують профілі в соціальних мережах для збору особистої інформації про цільових осіб, що дозволяє створювати більш правдоподібні обманки. Наприклад, за допомогою таких платформ, як Facebook, LinkedIn або Instagram, зловмисники можуть дізнатися про зв'язки жертви, її інтереси, робочі досягнення та інші деталі, які потім використовуються для маніпуляції [19].

У 2019 році стало відомо про серію атак, що були проведені з використанням LinkedIn [20]. Зловмисники створювали фальшиві профілі, які виглядали як представники компаній-партнерів або постачальників, і зв’язувалися з працівниками великих організацій. Після того як вони завоювали довіру, починали задавати питання або просити доступ до конфіденційної інформації. Оскільки ці профілі виглядали абсолютно правдоподібно, багато співробітників, не підозрюючи про небезпеку, надавали зловмисникам необхідні дані, що в результаті призводило до компрометації даних компанії.

Мобільні пристрої є ще одним вразливим елементом в екосистемі інформаційної безпеки, і соціоінженери активно використовують їх для атак. СМС-фішинг (smishing) — це метод, за допомогою якого зловмисники відправляють фальшиві текстові повідомлення, що містять посилання на

шкідливі вебсайти або інструкції для надання конфіденційної інформації. Такі повідомлення можуть виглядати як запити від банків, урядових служб або компаній, з якими користувач регулярно має справу.

В одному з випадків, що стався в 2020 році, атакувальники використовували smishing для того, щоб заманити жертв на фальшиві сторінки для перевірки особистих даних під виглядом урядових ініціатив у зв'язку з пандемією COVID-19 [21]. Люди, не перевіряючи достовірність повідомлень, вводили свої особисті дані на фальшивих сайтах, що дозволяло зловмисникам викрасти ці дані і використати їх для фінансових злочинів.

Соціоінженерія, як форма атаки, часто має за мету виявлення й використання слабких місць в системах безпеки організацій. Це не завжди стосується технологічних вразливостей — програмних помилок чи неполадок в апаратному забезпеченні. Натомість соціоінженери націлюються на людський фактор, який часто є найслабшою ланкою в системі безпеки. Відсутність належної обізнаності співробітників, недоліки у політиках безпеки або навіть відсутність строгих процедур підтвердження можуть призвести до серйозних витоків інформації або порушень безпеки. Соціоінженерні атаки, орієнтуючись на ці вразливості, здатні обійти навіть найсучасніші технологічні засоби захисту.

Людський фактор є однією з основних причин успіху соціоінженерних атак. Навіть найсучасніші засоби захисту, такі як брандмауери, системи виявлення вторгнень (IDS) або антивірусні програми, можуть бути неефективними, якщо працівники організації не дотримуються основних правил безпеки. Недостатня підготовка співробітників щодо виявлення потенційних загроз або навіть елементарні помилки, як от слабкі паролі або відсутність двофакторної автентифікації, можуть стати причиною витоку даних.

Відсутність регулярних тренінгів з інформаційної безпеки, невиконання корпоративних політик, або банальна нездатність співробітників перевірити достовірність запитів може призвести до серйозних наслідків. Наприклад, один із найбільш гучних випадків соціоінженерної атаки стався з компанією Sony Pictures у 2014 році, коли хакери змогли отримати доступ до великої кількості

конфіденційних документів, включаючи фінансові звіти, листування з партнерами та інші чутливі матеріали [22]. За словами експертів, частину цього доступу забезпечили саме соціоінженерні атаки на співробітників компанії, коли зловмисники маскувались під технічну підтримку.

Ще одна велика уразливість, яку використовують соціоінженери, — це неадекватна або надмірно відкрита обробка інформації. Зловмисники можуть використовувати інформацію, яку компанія неадекватно зберігає чи публікує у відкритих джерелах. Наприклад, відкриті соціальні мережі, вебсайти компаній, публікації в блогах, а також корпоративні презентації можуть містити важливі деталі, які можуть стати ціллю для соціоінженерних атак.

Атакувальники, маючи в розпорядженні інформацію про структуру організації, її співробітників, керівників і навіть внутрішні проекти, можуть створювати фальшиві запити або обманювати співробітників, щоб отримати доступ до систем або ресурсів. Один із класичних прикладів — це "телефонні атаки" або атаки за допомогою фальшивих листів, де зловмисники маскуються під співробітників технічної підтримки або інших важливих осіб і просять надіслати паролі чи інші чутливі дані.

Уразливість в обробці інформації часто виникає через недотримання стандартів безпеки при роботі з даними. Наприклад, у 2018 році стала відома історія про те, як одна з великих компаній виявила, що через недостатню політику захисту даних співробітники надавали вільний доступ до важливої корпоративної інформації стороннім особам, що використовували її для атаки. Внаслідок цього дані про важливі фінансові угоди були скомпрометовані, що призвело до значних фінансових збитків [23].

Ще одна вразливість, яку можуть використовувати соціоінженери, полягає в недостатньо чітких або застарілих політиках безпеки та відсутності єдиних протоколів щодо управління доступом до інформації. Багато організацій не мають належних процедур для перевірки ідентичності або авторизації запитів, що може сприяти успішному проведенню соціоінженерних атак.

Наприклад, один із найбільших інцидентів в історії кібератак стався з

компанією Target у 2013 році [24]. Хакери змогли проникнути в корпоративну мережу через компрометацію облікового запису третьої сторони — компанії-постачальника, що мала доступ до системи Target. Завдяки слабким процедурам безпеки і недостатньо строгому моніторингу активностей сторонніх постачальників, зловмисники змогли отримати доступ до даних 40 мільйонів карток клієнтів і здійснити їхнє незаконне використання. Це стало результатом недоліків у політиках безпеки, а саме в процедурі надання доступу стороннім постачальникам і перевірці їхніх дій.

Протоколи безпеки, які включають підтвердження запитів через кілька каналів зв'язку (наприклад, телефонний дзвінок або додаткову перевірку через SMS або електронну пошту), можуть значно знизити ймовірність того, що зловмисник здобуде доступ до конфіденційної інформації [25].

Мобільні пристрої — ще один вектор, через який зловмисники можуть атакувати організації, використовуючи соціоінженерні методи. Мобільні телефони, планшети і навіть персональні пристрої можуть бути легко скомпрометовані через фішинг або інші техніки. Низька обізнаність співробітників про безпеку мобільних пристроїв, відсутність належного захисту або слабкі паролі на таких пристроях можуть стати причиною витоку інформації або введення зловмисників у систему.

Соціоінженери використовують фішингові атаки через мобільні пристрої для збору конфіденційних даних або навіть для проникнення в корпоративні мережі. У 2020 році стало відомо, що зловмисники за допомогою фальшивих SMS-повідомлень намагалися отримати від співробітників компаній дані для доступу до систем внутрішнього фінансування [26]. Вони створювали фальшиві послання, в яких йшлося про термінову перевірку фінансових транзакцій, примушуючи співробітників вводити свої облікові дані на шкідливих сайтах.

Соціальні мережі стали потужним інструментом для збору інформації, яку соціоінженери можуть використовувати для виявлення вразливих місць в системах безпеки організацій. Через соціальні платформи хакери можуть отримати відомості про працівників, їхні ролі в компанії, інтереси, зв'язки з

іншими підприємствами, а також інші деталі, що можуть бути використані для персоналізованих атак.

Це дозволяє створювати фальшиві запити, що мають велику ймовірність успіху через високу ступінь довіри між жертвою і зловмисником. Наприклад, у 2018 році група хакерів використовувала LinkedIn для створення фальшивих профілів і відправлення персоналізованих запитів на доступ до корпоративної інформації [27]. Вони знаходили співробітників, які працювали в певних відділах компаній, і на основі їхніх інтересів або професійних зв'язків створювали обманливі запити на доступ до конфіденційних матеріалів.

Протидія соціоінженерним атакам потребує комплексного підходу, що охоплює технічні, організаційні та освітні заходи. Системи безпеки, що базуються лише на технологічних засобах, часто не можуть протистояти соціоінженерним атакам, оскільки ці атаки орієнтовані на людський фактор. Це означає, що організаціям необхідно розробляти не лише технічні рішення для захисту від кіберзагроз, а й активно працювати з персоналом, щоб підвищити обізнаність і навички виявлення таких атак.

Одним із найефективніших методів боротьби з соціоінженерними атаками є навчання співробітників основам інформаційної безпеки, а також специфічним технікам виявлення та реагування на можливі загрози. Створення культури безпеки в організації починається з підвищення обізнаності персоналу. Це включає регулярні тренінги, курси та практичні заняття, що дозволяють співробітникам навчитися виявляти підозрілі дії, а також знати, як правильно реагувати на фішинг, смішинг, візит зловмисників під виглядом технічної підтримки чи інші соціоінженерні методи.

Один з прикладів ефективної програми навчання був в компанії Google, де співробітники проходять обов'язкові тренінги з інформаційної безпеки. Програма включає імітаційні фішинг-атаки, які допомагають працівникам практично відпрацьовувати навички виявлення таких атак і правильно на них реагувати. Завдяки цьому рівень успішних фішинг-атак на співробітників Google значно зменшився, а персонал став більш обізнаним і готовим до таких загроз.

Насправді, навіть проста зміна звичок — таких як перевірка домену у веб-адресах або налаштування двофакторної автентифікації — може значно підвищити рівень безпеки компанії. Крім того, дуже важливо проводити регулярні перевірки, щоб переконатися, що всі співробітники залишаються обізнаними про нові загрози.

Технічні засоби захисту є важливими, але вони повинні доповнюватися навчанням співробітників та чіткими політиками безпеки. Системи моніторингу, брандмауери та фільтри для електронної пошти можуть виявляти і блокувати багато фішингових листів, шкідливих програм та спроб доступу до мережі. Водночас, не менш важливим є налаштування захисту для мобільних пристроїв, оскільки багато атак проводяться через мобільні телефони та планшети. Встановлення антивірусних програм, шифрування даних і регулярні оновлення програмного забезпечення також є критично важливими компонентами технічної безпеки.

Одним із ефективних технічних рішень є використання фільтрів спаму і антифішингових механізмів для електронної пошти [28]. Вони допомагають автоматично виявляти та блокувати підозрілі повідомлення ще до того, як вони потраплять до поштової скриньки співробітника. Проте важливо пам'ятати, що технічні засоби захисту мають свої обмеження, і вони не завжди можуть виявити найскладніші, добре скоординовані фішингові атаки. Тому їх слід комбінувати з іншими методами захисту.

Також варто розглянути впровадження механізмів для моніторингу та аналізу дій співробітників у корпоративних системах. Наприклад, можна використовувати програмне забезпечення для виявлення аномальної поведінки (Security Information and Event Management, SIEM), яке дозволяє оперативно виявляти і реагувати на потенційно небезпечні дії [29]. Такий моніторинг дозволяє швидко виявляти несанкціоновані спроби доступу або порушення безпеки в системах.

Для зменшення ризику соціоінженерних атак важливо забезпечити багатоетапну перевірку особи, перш ніж надавати доступ до чутливих даних або

систем. Це включає впровадження системи багаторівневої аутентифікації, що може включати паролі, біометричні дані, а також одноразові коди, що надсилаються на мобільний телефон або електронну пошту.

Протоколи багаторівневої аутентифікації дозволяють значно знизити ймовірність успішної атаки на облікові записи співробітників навіть у разі компрометації паролів або іншої інформації. Це особливо важливо для доступу до критичних внутрішніх систем, фінансових платформ або баз даних, де захист даних має високий пріоритет.

Впровадження політик, що обмежують доступ до конфіденційної інформації тільки за потребою (principle of least privilege), є ще одним важливим заходом захисту. Тільки співробітники, що мають прямий доступ до необхідних ресурсів для виконання своїх робочих завдань, повинні мати можливість доступу до чутливих даних [30]. Це зменшує ризик витоку інформації через соціоінженерні атаки, оскільки зловмисники не зможуть отримати доступ до ресурсів, які їм не надаються.

Налаштування жорстких політик безпеки є важливим кроком для протидії соціоінженерії. Однак для досягнення успіху важливо не лише визначити ці політики, але й забезпечити їх правильне виконання. Це включає визначення правил для співробітників щодо доступу до даних, паролів, використання мобільних пристроїв, а також обов'язкових перевірок та підтверджень для будь-яких запитів на зміну доступу або фінансові операції.

Один з популярних заходів — це вимога, щоб будь-яка зміна в інтерфейсі користувача або у фінансових транзакціях підтверджувалася через два або більше канали комунікації, що дозволяє знизити ймовірність успіху фальшивих запитів. Наприклад, запити на зміну банківських реквізитів можуть бути підтверджені через телефонний дзвінок або відеоконференцію, щоб упевнитись у справжності запиту.

Також важливим є забезпечення зберігання даних в зашифрованому вигляді. Шифрування є ефективним заходом захисту даних на випадок, якщо інформація буде вкрадена або зловмисники отримають доступ до серверів

організації. Шифрування даних навіть у разі витоку допомагає зберегти їх конфіденційність.

Захист від соціоінженерії не обмежується лише впровадженням політик і технологій. Важливо регулярно проводити перевірки на проникнення та тестування вразливостей, які можуть виявити слабкі місця в системах безпеки і процесах організації. Проведення регулярних тестів, включаючи "чорні" та "білих" хакерів, дозволяє виявити уразливості, до яких можуть призвести соціоінженерні атаки.

Тестування на проникнення включає в себе імітацію реальних атак з боку зовнішніх або внутрішніх зловмисників. Це дозволяє не тільки оцінити ефективність політик безпеки, але й оцінити готовність співробітників до подібних загроз, даючи можливість провести додаткове навчання.

Висновки до розділу 1

Розглянуто основні аспекти, що стосуються теоретичних і практичних підходів до соціальної інженерії як складової частини забезпечення інформаційної безпеки.

Проаналізовано сутність соціальної інженерії, її роль у сучасному контексті інформаційної безпеки та методи її використання. Визначено, що соціальна інженерія передбачає використання людських слабкостей для досягнення несанкціонованого доступу до чутливої інформації або систем. Акцентовано увагу на основних етапах соціоінженерних атак, таких як збір інформації, маніпуляція та реалізація мети. Зокрема, методологічні підходи до проведення соціоінженерних атак ґрунтуються на психологічному впливі, що дозволяє здійснювати атаки на базі людських взаємодій, а не на технічних вразливостях.

Проаналізовано реальні приклади соціоінженерних атак, а також їх вплив на інформаційну безпеку організацій. Було продемонстровано, як соціоінженери активно використовують людський фактор, недоліки в політиках безпеки та

відсутність навчання для здійснення своїх атак. Розглянуто успішні приклади атак, а також заходи, які допомагають знизити ризики, зокрема через підвищення обізнаності співробітників і впровадження комплексних технологічних і організаційних заходів.

Соціальна інженерія залишається одним з найефективніших інструментів для порушення інформаційної безпеки, і її вплив на організації значно зростає. Врахування соціоінженерних аспектів при формуванні стратегій захисту є необхідним для ефективного протистояння сучасним кіберзагрозам.

Розділ 2 СОЦІОІНЖЕНЕРНІ СЦЕНАРІЇ В ПРОЦЕСІ ТЕСТУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У сучасних умовах стрімкого розвитку інформаційних технологій значної уваги потребує не лише технічний захист систем, а й соціальний фактор, який часто стає найслабшою ланкою в безпеці. Соціоінженерні атаки, спрямовані на маніпулювання людьми з метою отримання конфіденційної інформації або несанкціонованого доступу, залишаються одними з найпоширеніших та найнебезпечніших загроз.

Тестування інформаційної безпеки не може бути повноцінним без оцінки рівня вразливості персоналу до соціоінженерних впливів. Моделювання реальних сценаріїв атак дозволяє виявити слабкі місця в усій системі безпеки, включаючи людський фактор, та вжити превентивних заходів.

У цьому розділі розглядаються основні соціоінженерні сценарії, які використовуються під час тестування на проникнення (pentesting), методи їх реалізації та способи протидії. Також аналізуються ефективні підходи до навчання співробітників, спрямовані на мінімізацію ризиків, пов’язаних із соціальним інжинірингом.

2.1 Основні підходи атаки за допомогою методів соціальної інженерії

Соціальна інженерія як метод маніпуляції людською поведінкою з метою отримання конфіденційної інформації або несанкціонованого доступу до систем і даних охоплює широкий спектр технік, які постійно вдосконалюються злочинцями. В основі цих методів лежить використання психологічних слабкостей людини, таких як довіра, люб'язність, страх або жадібність, а не технічних вразливостей програмного забезпечення. Методи соціальної інженерії представлені на рис. 2.1.

Однією з найпоширеніших і найнебезпечніших категорій соціоінженерних атак є фішинг. Він полягає у масовій розсилці електронних листів, SMS-

повідомлень або повідомлень у соціальних мережах, які імітують офіційні комунікації від відомих організацій, таких як банки, поштові служби або соціальні мережі. Ці повідомлення зазвичай містять підступні посилання на фальшиві вебсайти, що точно копіюють легальні, або вкладення зі шкідливим програмним забезпеченням [31]. Жертву під різними приводами просять ввести свої облікові дані, дані кредитних карток або завантажити файл, що призводить до витоку інформації або зараження системи.

Більш цільовою та небезпечною різновидністю фішингу є спір-фішинг (spear phishing), де атака проводиться не масово, а цілеспрямовано проти конкретної особи або організації. Зловмисники ретельно вивчають інформацію про жертву, використовуючи відкриті джерела, такі як соціальні мережі або корпоративні сайти, щоб створити максимально персоналізоване та правдоподібне повідомлення. Наприклад, лист може бути оформлений як офіційний запит від керівництва компанії або партнера по бізнесу, що значно підвищує ймовірність успіху атаки.

Ще однією поширеною технікою є вішинг (vishing), який передбачає використання голосового зв'язку для отримання конфіденційної інформації. Зазвичай зловмисники представляються співробітниками банків, служби підтримки або правоохоронних органів і під різними приводами вимагають від жертви надати особисті дані, паролі або іншу конфіденційну інформацію. Високий рівень організації таких атак, включаючи підроблені номери телефонів і сценарії розмов, робить їх особливо небезпечними.

Претекстинг – це інший метод соціальної інженерії, який базується на створенні вигаданого, але правдоподібного сценарію для отримання довіри жертви. Наприклад, зловмисник може представитись технічним спеціалістом, якому потрібен доступ до системи для вирішення нібито термінової проблеми, або кур'єром, який потребує пропуску у приміщення. Успіх претекстингу залежить від здатності злочинця переконливо грати свою роль і використовувати соціальні норми, такі як бажання допомогти або уникнути конфлікту.

Особливу небезпеку становить кві проїтінг (tailgating), коли зловмисник

отримує фізичний доступ до захищеної зони, наприклад офісної будівлі або серверної кімнати, шляхом обходу систем контролю доступу. Це може бути реалізовано через пропускання зловмисника співробітником, який піддається на прохання "тримати двері", або через використання підроблених бейджів.

Також варто згадати про байтінґ (baiting), який ґрунтується на зацікавленості жертви отримати безкоштовний або привабливий продукт. Наприклад, зловмисники можуть залишати заражені USB-накопичувачі у громадських місцях з написом "Зарплатна відомість" або "Конфіденційно", сподіваючись, що знахідка буде підключена до корпоративного комп'ютера.

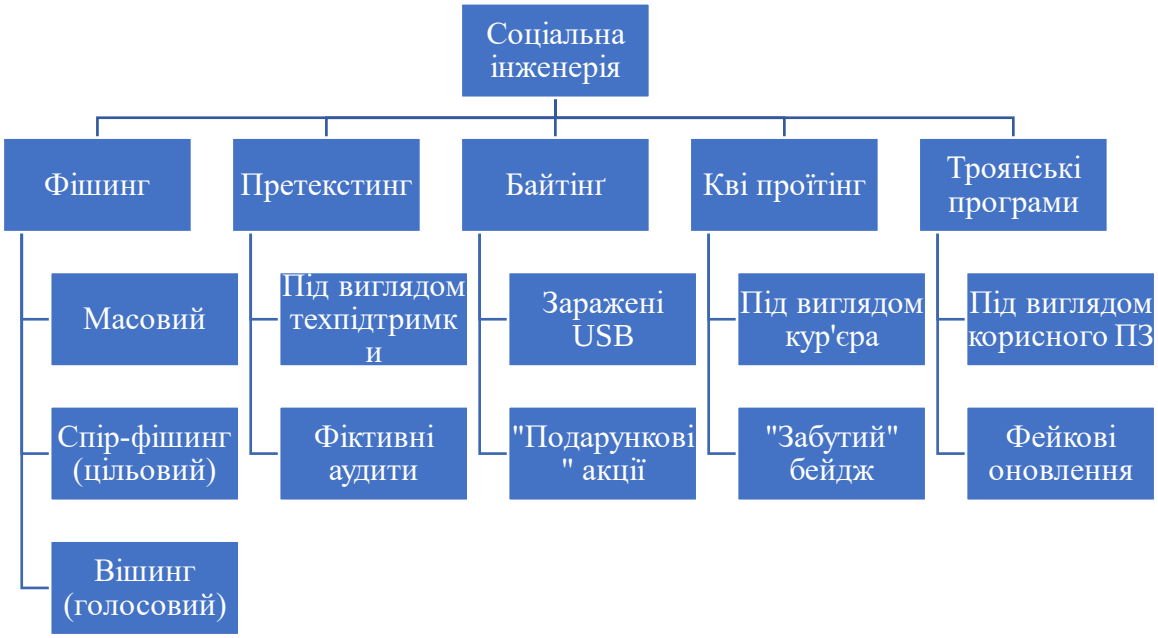

Рис. 2.1 Класифікація методів соціальної інженерії

Кожен із цих методів має свої особливості реалізації та ступінь ефективності, що залежить від рівня підготовки жертви та наявності в організації ефективних заходів захисту [32]. Розуміння цих технік є першим кроком до побудови надійної системи протидії соціоінженерним атакам.

Сучасний ландшафт кіберзагроз демонструє невпинне зростання складності та витонченості соціоінженерних атак, які все частіше поєднують у собі психологічні методи впливу з передовими технічними засобами. Ця симбіотична взаємодія значно підвищує ефективність атакуючих, роблячи соціальну інженерію одним з найнебезпечніших векторів кібератак. Основна

небезпека полягає в тому, що ці методи експлуатують не стільки технічні вразливості систем, скільки природні психологічні особливості людини, такі як довіра, бажання допомогти або страх перед негативними наслідками.

Техніко-психологічний симбіоз сучасних атак досяг такого рівня розвитку, коли традиційні методи соціальної інженерії тісно інтегруються з складними технічними експлойтами. Наприклад, цільовий фішинг вже давно перестав бути простою розсилкою підроблених листів [33]. Сучасні атаки такого типу передбачають використання цілих інфраструктур, що включають підроблені вебсайти з сертифікатами SSL, системи відстеження кліків жертв, а навіть механізми автоматичного адаптування контенту під конкретного одержувача. Особливо небезпечним є поєднання соціальної інженерії з атаками типу "людина посередині", коли зловмисник не просто виманює дані, але й активно втручається в процес комунікації, модифікуючи передану інформацію в реальному часі.

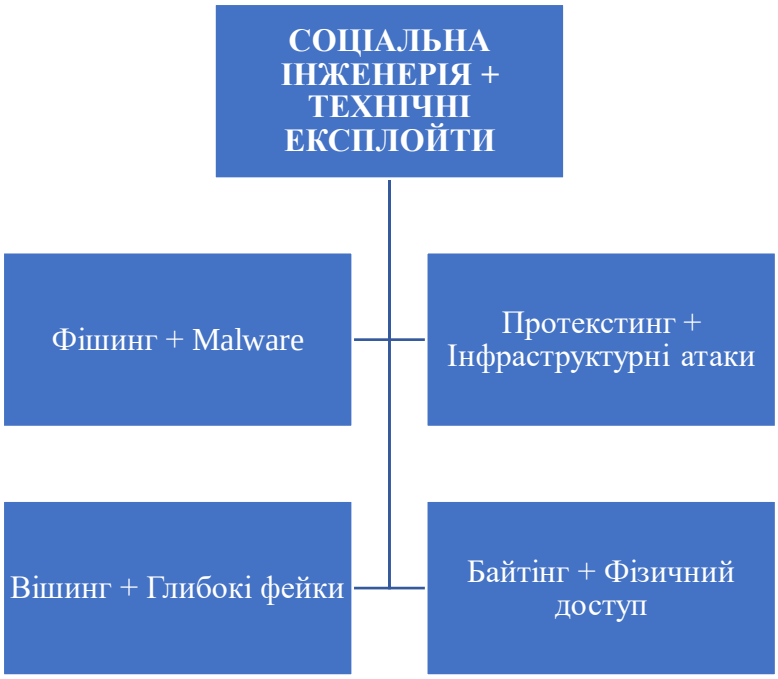

Рис. 2.2 Співвідношення соціоінженерних методів і технічних векторів атак

Окремо варто відзначити зростаючу популярність атак, що поєднують соціальну інженерію з експлуатацією нуль-денних вразливостей. У таких

випадках жертва не просто передає зловмисникам свої облікові дані, але й непомітно для себе завантажує й запускає шкідливий код, який надалі дозволяє атакуючим отримати повний контроль над системою [34]. Особливо небезпечними є документи з вбудованими макросами або PDF-файли з експлойтами, які активуються при спробі перегляду вмісту.

Сучасні соціоінженерні атаки все частіше використовують методи обходу багатофакторної аутентифікації. Наприклад, техніка "сеансового викрадення" дозволяє зловмисникам отримувати доступ до систем навіть при наявності MFA. Це досягається за рахунок комбінації фішингу для отримання логіну та паролю з подальшим викраденням сеансових cookie або токенів через шкідливі скрипти.

Однією з найбільш тривожних тенденцій останніх років стало активне застосування технологій штучного інтелекту в соціальній інженерії. Генеративні нейромережі дозволяють створювати надзвичайно правдоподібні фішингові листи, адаптовані під стиль спілкування конкретної організації або навіть окремого співробітника. Розвиток технологій глибокого фейку відкрив нову сторінку в вішингових атаках - тепер зловмисники можуть імітувати не тільки голос, але й зовнішність керівників під час відеодзвінків.

Аналіз статистики останніх років показує, що соціальна інженерія залишається основним вектором початку більшості успішних кібератак. Згідно з даними Verizon DBIR, понад 80% інцидентів із витоком даних починаються саме з соціоінженерних методик [35]. При цьому середній час відкриття фішингового листа становить менше двох хвилин, що свідчить про високу ефективність цих методів. Особливо варто відзначити, що більше половини співробітників клікають на підозрілі посилання, якщо вони досить вправно оформлені.

Регіональні особливості соціоінженерних атак також заслуговують на увагу. В українському сегменті інтернету переважають атаки, що імітують комунікацію з банківськими установами або правоохоронними органами. Останнім часом спостерігається зростання кількості цільових атак на IT-компанії, де зловмисники вдають із себе потенційних клієнтів або партнерів по бізнесу.

Психологічні аспекти успішних соціоінженерних атак засновані на глибокому розумінні механізмів прийняття рішень. Найбільш ефективними тригерами виявляються відчуття терміновості (87% успішних кліків), авторитетність джерела (65%) та соціальний доказ (58%). Цікаво, що періоди підвищеної ефективності атак часто збігаються з передсвятковими тижнями, кінцем фінансового кварталу або нічним часом для топ-менеджменту, коли рівень критичності сприйняття інформації знижується [36].

Сучасні соціоінженерні атаки перетворилися на високотехнологічні комплексні операції, що вимагають від організацій впровадження адекватних багаторівневих заходів захисту. Традиційні підходи до інформаційної безпеки, орієнтовані виключно на технічні засоби захисту, виявляються неефективними проти складних комбінованих атак, що використовують як технічні вразливості, так і слабкості людської психіки. Це вимагає принципово нового підходу до побудови систем безпеки, який би поєднував технічні засоби захисту з постійним навчанням персоналу та розробкою ефективних механізмів виявлення соціоінженерних атак на ранніх стадіях.

Аналіз реальних випадків успішних соціоінженерних атак дозволяє не лише зрозуміти сучасні тенденції в кіберзлочинності, але й виявити типові помилки організацій, що призводять до серйозних наслідків. Одним із найрезонансніших інцидентів останніх років стала атака на компанію Ubiquiti Networks у 2015 році [37]. В цьому випадку зловмисникам вдалося викрасти 40 мільйонів доларів за допомогою складного поєднання цільового фішингу та технічних експлойтів. Атака почалася з ретельно підготовлених електронних листів, адресованих фінансовим службовцям компанії, які імітували легальні запити від керівництва. Використовуючи методи соціальної інженерії, злочинці змогли переконати співробітників виконати низку транзакцій на підставних рахунки, при цьому кожен етап операції супроводжувався психологічним тиском через терміновість виконання.

Ще одним показовим прикладом є масштабний інцидент із Twitter у липні 2020 року, коли зловмисникам вдалося отримати доступ до акаунтів численних

відомих осіб, включаючи Барака Обаму, Джо Байдена та Ілона Маска. В цьому випадку атака базувалася на складному поєднанні соціальної інженерії та технічних методів [38]. Зловмисники вивчили внутрішні процеси Twitter, після чого через телефонні дзвінки змогли переконати співробітників служби підтримки надати доступ до адміністративних панелей. Особливістю цього інциденту стало використання так званого "вішингу" - голосових дзвінків з підробленими номерами, що імітували внутрішні лінії компанії. В результаті атаки зловмисники отримали можливість публікувати повідомлення від імені високопоставлених осіб, що призвело до значного фінансового збитку та репутаційних втрат.

Окремо варто розглянути кейс із атакою на австрійський виробник компонентів для літаків FACC у 2016 році. В цьому випадку зловмисники, видаючи себе за керівництво компанії, змогли виманити у фінансового директора 42 мільйони євро [39]. Атака була настільки добре підготовлена, що включала створення цілого фіктивного проекту з відповідною документацією та навіть організацію конференц-дзвінків з використанням технологій глибокого фейку для імітації голосів керівників. Цей інцидент наочно демонструє, наскільки складними та багатоетапними можуть бути сучасні соціоінженерні атаки.

Український бізнес також неодноразово ставав жертвою соціальної інженерії. Яскравим прикладом є атака на одну з великих українських банківських установ у 2018 році, коли зловмисникам вдалося викрасти близько 10 мільйонів гривень [40]. В цьому випадку атака почалася з фішингового листа, адресованого співробітнику відділу кадрів, який містив інфекційний файл. Після зараження системи зловмисники отримали доступ до внутрішньої мережі, де протягом кількох місяців вивчали бізнес-процеси, перш ніж провести фінансову операцію. Особливістю цього випадку стало те, що зловмисники використовували знання про внутрішні корпоративні традиції та особливості спілкування між співробітниками для маскування своєї діяльності.

Аналіз цих та подібних інцидентів дозволяє виділити кілька ключових

закономірностей. По-перше, більшість успішних атак ґрунтуються на ретельній підготовці, яка включає збір інформації про цільову організацію та її співробітників. По-друге, зловмисники все частіше використовують багатоетапні сценарії, де соціальна інженерія поєднується з технічними методами проникнення. По-третє, критичним фактором успіху атак часто стає недостатня обізнаність співробітників про методи соціальної інженерії та їхні прояви.

Ці реальні випадки наочно демонструють, що сучасні соціоінженерні атки перетворилися на складні багаторівневі операції, що вимагають від організацій комплексного підходу до захисту, який би поєднував технічні засоби безпеки з постійним навчанням персоналу та вдосконаленням внутрішніх процедур перевірки. Відсутність будь-якого з цих елементів значно підвищує ризик успішного проведення атаки з серйозними фінансовими та репутаційними наслідками для організації.

Ефективна протидія соціоінженерним атакам вимагає комплексного підходу, що поєднує технічні, організаційні та психологічні аспекти. Сучасні дослідження демонструють, що традиційні методи захисту, орієнтовані виключно на технічні рішення, виявляються недостатньо ефективними проти складних багаторівневих атак, що експлуатують людський фактор. Тому розробка стратегії протидії повинна враховувати всі можливі вектори атак та включати низку взаємопов'язаних заходів.

Одним із найважливіших елементів захисту є регулярне навчання персоналу з розпізнавання соціоінженерних атак. Такі тренінги повинні бути практико-орієнтованими та включати не лише теоретичні основи, а й симуляцію реальних атак. Найефективнішими виявляються програми, що передбачають періодичне тестування співробітників за допомогою контрольованих фішингових кампаній. Такі тести дозволяють не лише оцінити рівень обізнаності персоналу, а й виявити найбільш вразливі ланки в організації. Важливо, щоб навчання не було формальним, а враховувало специфіку діяльності конкретної організації та актуальні тенденції в соціальній інженерії.

Технічні засоби захисту відіграють ключову роль у протидії соціоінженерним атакам. Впровадження багатофакторної аутентифікації (MFA) значно ускладнює зловмисникам доступ до систем навіть у разі компрометації облікових даних. Системи фільтрації електронної пошти, здатні виявляти фішингові повідомлення на основі аналізу контенту, метаданих та поведінкових характеристик, є обов'язковим елементом захисту. Особливу увагу слід приділити системам моніторингу та аналізу діяльності користувачів (UEBA), які дозволяють виявляти незвичайну поведінку, що може свідчити про успішну соціоінженерну атаку.

Розробка чітких протоколів перевірки ідентичності є критично важливою для запобігання претекстингу та вішинговим атакам. Такі протоколи повинні включати кілька незалежних каналів підтвердження, особливо коли йдеться про конфіденційні операції або зміну критичних параметрів системи. Наприклад, запит на зміну реквізитів оплати повинен підтверджуватися не лише електронним листом, а й телефонним дзвінком на заздалегідь відомий номер, або особистою зустріччю.

Організація фізичного захисту також відіграє важливу роль у протидії соціальній інженерії. Заходи повинні включати сувору систему контролю доступу, супровід відвідувачів, захист від "підхоплення" дверей (tailgating), а також чіткі процедури видалення доступу для колишніх співробітників. Особливу увагу слід приділити захисту інформації, що може бути використана для соціоінженерних атак, таких як організаційні структури, контактні дані співробітників або внутрішні процедури.

Створення культури кібербезпеки в організації є не менш важливим, ніж технічні засоби захисту. Це передбачає не лише регулярне навчання, а й формування серед співробітників розуміння важливості їхньої ролі в забезпеченні безпеки [41]. Система заохочення за виявлення підозрілих дій або повідомлень, а також створення зручних каналів для такого повідомлення значно підвищують ефективність протидії.

Розробка плану реагування на інциденти, пов'язані з соціальною

інженерією, дозволяє мінімізувати наслідки у разі успішної атаки. Такий план повинен включати чіткі інструкції щодо блокування компрометованих облікових записів, відновлення даних, повідомлення клієнтів та регуляторних органів, а також проведення розслідування для виявлення причин інциденту.

Використання спеціалізованих платформ для тестування на проникнення (pentesting), що включають соціоінженерні сценарії, дозволяє регулярно оцінювати рівень захищеності організації та виявляти слабкі місця до того, як ними скористаються зловмисники. Такі тестування повинні охоплювати всі можливі вектори атак, включаючи електронну пошту, телефонні дзвінки, фізичний доступ та соціальні мережі.

Важливим аспектом протидії є моніторинг зовнішніх джерел інформації, таких як paste-сайти, dark web або соціальні мережі, на предмет витоку конфіденційної інформації про організацію або її співробітників. Така інформація часто використовується для підготовки цільових соціоінженерних атак.

Сучасні підходи до протидії соціальній інженерії все частіше використовують технології штучного інтелекту та машинного навчання для аналізу поведінки користувачів, виявлення аномалій у комунікації та автоматичного блокування підозрілих дій. Такі системи здатні виявляти навіть раніше невідомі методи атак на основі аналізу шаблонів поведінки.

Ефективна стратегія протидії соціоінженерним атакам повинна бути динамічною та постійно адаптуватися до нових загроз. Це вимагає регулярного оновлення політик безпеки, навчальних програм та технічних засобів захисту з урахуванням змін у тактиці зловмисників і появи нових технологій. Тільки комплексний підхід, що враховує технічні, організаційні та людські аспекти, може забезпечити ефективний захист від постійно еволюціонуючих соціоінженерних атак.

Щоб підсумувати вищесказане, створено табл. 2.1.

Таблиця 2.1

Порівняльний аналіз соціоінженерних атак та методів протидії

Критерій	**Приклади атак (2.1.3)**	**Методи протидії (2.1.4)**	**Ефективність заходів**
Цільовість	Атака на Ubiquiti (2015), Twitter (2020)	Персоналізовані тренінги, симуляція атак	Високоя (зниження ризику на 60-80%)
Технічний вектор	Використання макросів у документах, фармінг	MFA, системи фільтрації пошти, UEBA	Середня-висока (блокують 70-90% атак)
Психологічний вплив	Вішинг з імітацією керівництва	Протоколи перевірки ідентичності (2+ канали)	Високоя для цільових атак
Фізичний доступ	Кві проїтінг (FACC, 2016)	Контроль доступу, супровід відвідувачів	Високоя при суворому дотриманні
Автоматизація атак	Генеративний AI для фішингу	AI-системи аналізу поведінки	Середня (вимагає постійного оновлення)
Реагування на інциденти	Багатоетапні атаки з вивченням інфраструктури	Плани реагування, моніторинг dark web	Критично важливий елемент

2.2 Розробка методики інтеграції соціоінженерних сценаріїв у процес тестування інформаційної безпеки

Інтеграція соціоінженерних сценаріїв у процес тестування інформаційної безпеки є критично важливим етапом для виявлення слабких ланок у системі захисту, пов'язаних із людським фактором. Цей розділ детально висвітлює методичні підходи до розробки та впровадження таких сценаріїв, аналізує ключові етапи тестування, можливості автоматизації та пропонує комплексну методику інтеграції соціоінженерних технік у стандартні процеси перевірки

безпеки.

Розробка ефективних соціоінженерних сценаріїв для тестування інформаційної безпеки вимагає ретельного планування та глибокого розуміння як технічних аспектів, так і психологічних механізмів, які лежать в основі маніпуляційної діяльності зловмисників. Цей процес починається з комплексного аналізу цільової організації, який охоплює вивчення організаційної структури, корпоративної культури, бізнес-процесів та існуючих процедур інформаційної безпеки. Особливу увагу приділяють аналізу соціальних взаємодій між співробітниками, ієрархії підпорядкування та каналам внутрішньої комунікації, оскільки саме ці фактори часто стають об'єктом експлуатації при реальних атаках (див. рис. 2.3.).

На основі проведеного аналізу формується детальний профіль потенційних "жертв", який включає соціально-демографічні характеристики співробітників, їхні цифрові звички, рівень технічної обізнаності та психологічні особливості поведінки. Цей профіль дозволяє максимально адаптувати тестові сценарії під реальні умови функціонування організації. Наприклад, для кол-центрів актуальними будуть сценарії, що імітують клієнтські дзвінки з вимаганням конфіденційної інформації, тоді як для бухгалтерії більш ефективними виявляться листи з підробленими фінансовими документами.

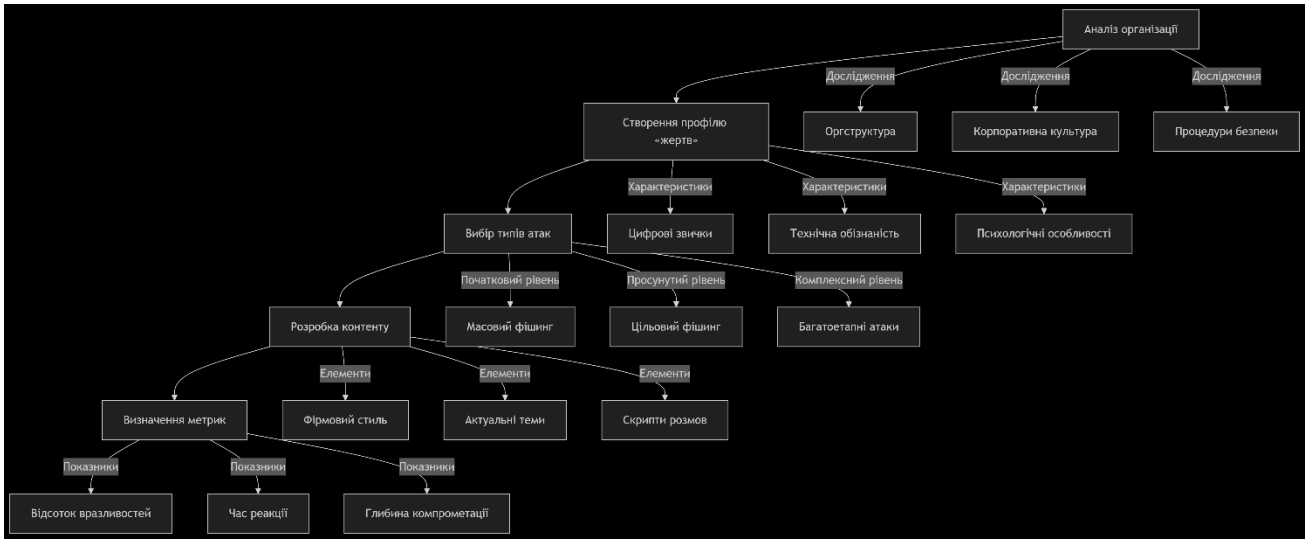

Рис. 2.3 Процес розробки соціоінженерних сценаріїв

Вибір конкретних типів соціоінженерних атак для тестування базується на

принципі поступового ускладнення. На початкових етапах рекомендовано використовувати стандартні сценарії, такі як масові фішингові розсилки з загальними темами (наприклад, оновлення корпоративних політик або зміни у графіку роботи). По мірі підвищення обізнаності співробітників сценарії ускладнюються, включаючи цільовий фішинг (spear phishing) з персоналізованими зверненнями, претекстинг із складними легендами або навіть багатоетапні комбіновані атаки, що поєднують електронні комунікації з телефонними дзвінками [42].

Створення правдоподібного контенту для тестових атак є критично важливим етапом розробки сценаріїв. Для фішингових листів це передбачає не тільки точне копіювання корпоративного стилю (логотипи, шаблони, підписи), але й використання актуальних внутрішніх тем, імен реальних керівників та відомостей про поточні події в організації. Особливу складність становить розробка підроблених вебсторінок, які повинні точно відтворювати офіційні інтерфейси корпоративних сервісів, включаючи всі елементи дизайну, систему входу та навіть повідомлення про помилки.

Для телефонних сценаріїв (вішингу) розробляються детальні скрипти розмов, що враховують специфіку бізнес-процесів організації. Ці скрипти включають не тільки основні повідомлення, а й варіанти відповідей на можливі запитання співробітників, техніки подолання сумнівів та алгоритми дій у разі виявлення атаки. Сучасні підходи передбачають використання технологій синтезу мовлення або навіть глибокого фейку для імітації голосів керівників.

Важливим аспектом розробки є визначення системи метрик для оцінки ефективності тестування. До базових показників відносять відсоток співробітників, які відкрили тестові листи, перейшли за посиланнями, ввели свої облікові дані на підроблених сторінках або надали конфіденційну інформацію по телефону. Для більш глибокого аналізу використовують такі показники, як час відкриття листа до переходу за посиланням, тривалість взаємодії з підробленим ресурсом, кількість спроб перевірки автентичності повідомлення.

Сучасні підходи до розробки соціоінженерних сценаріїв все частіше

використовують методики з області поведінкової психології та аналізу даних. Наприклад, застосовуються алгоритми машинного навчання для прогнозування найбільш вразливих груп співробітників або автоматичного генерування персоналізованих фішингових повідомлень на основі аналізу їхньої цифрової активності. Це дозволяє максимально наблизити тестові сценарії до реальних умов атаки, підвищуючи їх ефективність як інструменту оцінки рівня безпеки.

Процес тестування інформаційної безпеки з використанням соціоінженерних сценаріїв є багатоетапною процедурою, яка вимагає ретельної підготовки та системного підходу. Кожен етап має свої особливості та критично важливі моменти, які необхідно враховувати для отримання об'єктивних результатів.

Першим та одним з найважливіших етапів є планування тестування. На цій стадії формулюються чіткі цілі та задачі тестування, визначається його масштаб (чи буде воно охоплювати всю організацію чи окремі підрозділи), а також обираються конкретні методики соціальної інженерії, які будуть використовуватись. Важливим елементом планування є визначення меж тестування - чи будуть воно включати лише електронні комунікації, чи також телефонні дзвінки та тестування фізичного доступу. На цьому ж етапі оформляється офіційний документ, який закріплює рамки тестування, включаючи дозволені методи, часові періоди, обмеження та критерії успішності. Цей документ зазвичай містить інформацію про те, які системи та співробітники будуть задіяні, які дані можуть бути використані під час тестування, а також процедури безпеки, які дозволять уникнути непередбачених наслідків.

Другим етапом є підготовка інфраструктури для тестування. Для фішингових кампаній це передбачає налаштування серверів для розсилки листів, створення підроблених вебсторінок з системами логування дій користувачів, а також розгортання інструментів для відстеження відкриття листів і переходів за посиланнями. Важливою частиною цього етапу є створення правдоподібного контенту, який би максимально точно імітував реальні атаки, але при цьому містив маркери, що дозволяють відрізнити тестові повідомлення від справжніх

загроз. Для тестів фізичного доступу готуються відповідні аксесуари (підроблені бейджи, уніформа) та обладнання для фіксації спроб проникнення. Особливу увагу приділяють безпеці процесу тестування, щоб уникнути витоку тестових даних або їхнього використання зловмисниками.

Етап проведення тестування є найбільш динамічною частиною процесу. Він передбачає безпосередню реалізацію розроблених сценаріїв з дотриманням усіх запланованих параметрів. Важливо забезпечити контрольованість процесу, щоб уникнути непередбачених наслідків. Наприклад, при тестуванні фізичного доступу слід заздалегідь повідомити службу безпеки про можливі спроби проникнення, але не розкриваючи конкретні деталі. У випадку фішингових тестів рекомендується використовувати спеціальні домени, які не можуть бути сприйняті як реальні загрози. Під час проведення тестування фіксуються всі дії співробітників, їх реакції на тестові сценарії, час реагування, а також дії служби безпеки у разі виявлення підозрілих активностей.

Наступним критично важливим етапом є збір та аналіз даних. На цьому етапі проводиться систематизація всієї інформації, отриманої під час тестування. Аналізуються такі показники, як відсоток співробітників, які піддалися на атаку, час реагування на підозрілі дії, ефективність існуючих механізмів захисту, а також типові помилки, які призводять до успішних соціоінженерних атак. Сучасні системи аналізу дозволяють не тільки фіксувати факт успішної атаки, але й виявляти закономірності у поведінці співробітників, що дозволяє більш точно визначити слабкі місця в системі безпеки організації. Особливу увагу приділяють аналізу тих випадків, коли співробітники впізнали атаку та повідомили про неї - це дозволяє виявити ефективні практики, які варто поширювати серед інших працівників.

Завершальним етапом процесу тестування є підготовка звіту та розробка рекомендацій. Звіт повинен містити детальний опис проведених тестів, статистику успішних/неуспішних спроб, аналіз причин уразливостей та конкретні пропозиції щодо підвищення рівня безпеки. Важливою частиною цього етапу є проведення навчальних семінарів для співробітників на основі

виявлених слабких місць. Рекомендації щодо вдосконалення системи безпеки повинні враховувати як технічні аспекти (оновлення систем фільтрації, впровадження додаткових засобів аутентифікації), так і організаційні (зміни в процедурах, оновлення політик безпеки) та кадрові (додаткове навчання співробітників). Особливу увагу приділяють розробці механізмів зворотного зв'язку, які дозволяють співробітникам повідомляти про підозрілі дії без страху негативних наслідків.

Важливо відзначити, що процес тестування не є одноразовим заходом, а повинен бути частиною постійного циклу вдосконалення системи інформаційної безпеки організації. Періодичність проведення таких тестувань зазвичай становить від 3 до 6 місяців, що дозволяє своєчасно виявляти нові загрози та оцінювати ефективність запроваджених раніше заходів безпеки. Крім того, між плановими тестуваннями рекомендовано проводити невеликі спонтанні перевірки для оцінки рівня обізнаності співробітників у "реальному часі", без попередньої підготовки.

Теперішні підходи до тестування інформаційної безпеки все частіше використовують методологію безперервного тестування, коли соціоінженерні сценарії інтегровані в повсякденні бізнес-процеси організації. Це дозволяє не тільки виявляти слабкі місця, але й формувати культуру безпеки, при якій співробітники постійно усвідомлюють можливі загрози та знають, як правильно на них реагувати.

Сучасні підходи до тестування інформаційної безпеки все більше покладаються на автоматизовані рішення для проведення соціоінженерних атак, що дозволяє значно підвищити ефективність, масштабованість та об'єктивність оцінки рівня безпеки організації. Автоматизація соціоінженерних тестів охоплює широкий спектр завдань - від масових фішингових кампаній до складних багатоетапних сценаріїв, що імітують реальні загрози.

Одним із найпоширеніших інструментів автоматизації є платформа GoPhish, яка надає комплексне рішення для організації тестових фішингових кампаній [43]. Ця платформа дозволяє створювати персоналізовані фішингові

листи, керувати списками розсилки, відстежувати відкриття повідомлень та переходи за посиланнями, а також генерувати детальні звіти про результати тестування. GoPhish відрізняється зручним веб-інтерфейсом, можливістю імпорту шаблонів листів із зовнішніх джерел, а також інтеграцією з API для автоматизації рутинних операцій. Особливістю платформи є вбудований сервіс для створення підроблених вебсторінок, який дозволяє імітувати сторінки входу популярних сервісів без необхідності володіти поглибленими знаннями веб-розробки.

Для більш складних сценаріїв, що включають елементи соціальної інженерії за межами електронної пошти, використовується Social Engineer Toolkit (SET). Цей інструмент надає широкий спектр можливостей для автоматизації різних типів атак, включаючи створення шкідливих файлів (документів з макросами, PDF з експлойтами), генерацію підроблених вебсторінок, а також організацію атак через соціальні мережі. SET особливо ефективний для тестування на проникнення, оскільки дозволяє швидко розгортати цілісні сценарії атак, що поєднують технічні експлойти з методами соціальної інженерії.

Автоматизація телефонних атак (вішингу) вимагає спеціалізованих інструментів, таких як Asterisk-based рішення або спеціалізовані платформи на кшталт Twilio. Ці системи дозволяють організовувати масові телефонні кампанії, записувати розмови для подальшого аналізу, а також використовувати технології синтезу мовлення для імітації голосів. Сучасні розробки в галузі штучного інтелекту дозволяють створювати більш складні сценарії, де система може аналізувати відповіді співробітників за допомогою NLP (Natural Language Processing) та адаптувати сценарій розмови в реальному часі.

Для тестування фізичного доступу використовуються спеціалізовані пристрої, такі як Hak5 Rubber Ducky або Bash Bunny [44]. Ці компактні пристрої, що імітують звичайні USB-накопичувачі, дозволяють автоматизувати процес введення шкідливих команд при підключенні до комп'ютера жертви. Вони програмуються за допомогою спеціальних скриптів, які можуть імітувати дії

зловмисника - від викрадення паролів до встановлення бекдорів. Для комплексного тестування фізичного захисту також використовуються пристрої для перехоплення сигналів RFID (наприклад, Proxmark3), які дозволяють перевірити захищеність систем контролю доступу.

Важливим аспектом автоматизації є інтеграція соціоінженерних тестів із системами моніторингу інформаційної безпеки (SIEM). Такі рішення, як Splunk, IBM QRadar або ArcSight, дозволяють у реальному часі відстежувати реакцію систем захисту на тестові атаки, фіксувати спроби доступу до критичних ресурсів та аналізувати логування подій. Інтеграція здійснюється через спеціальні конектори або API, що дозволяє автоматизувати процес збору даних про результати тестування та їх кореляцію з іншими подіями безпеки в організації.

Сучасні тенденції в автоматизації соціоінженерних тестів включають використання технологій машинного навчання для аналізу результатів тестування та прогнозування найбільш вразливих точок. Наприклад, алгоритми аналізу соціальних мереж можуть визначати співробітників, які найбільш схильні до соціальної інженерії на основі їхньої активності в інтернеті. Системи на основі штучного інтелекту можуть автоматично генерувати персоналізовані фішингові повідомлення, що враховують індивідуальні особливості кожної "жертви", що значно підвищує ефективність тестування.

Окремо варто відзначити інструменти для автоматизації зворотного зв'язку та навчання співробітників. Такі рішення, як KnowBe4 або Proofpoint Security Awareness Training, дозволяють не тільки проводити тестові атаки, але й автоматично надавати співробітникам персоналізовані навчальні матеріали на основі їхніх помилок. Це створює замкнутий цикл "тестування-навчання", який постійно підвищує рівень обізнаності співробітників про загрози соціальної інженерії.

Важливим викликом при автоматизації соціоінженерних тестів є забезпечення безпеки самого процесу тестування. Для цього використовуються спеціальні механізми, що запобігають витоку тестових даних або їхньому

використанню зловмисниками. Наприклад, тестові фішингові листи містять спеціальні маркери, які дозволяють системам безпеки відрізняти їх від реальних загроз, а всі дані, зібрані під час тестування, зберігаються в зашифрованому вигляді з обмеженим доступом.

Розвиток інструментів автоматизації соціоінженерних тестів йде у напрямку створення комплексних платформ, які поєднують можливості тестування різних векторів атак (електронна пошта, телефонні дзвінки, фізичний доступ) з потужними аналітичними функціями та інтеграцією з іншими системами безпеки. Такі рішення дозволяють організаціям не тільки виявляти слабкі місця в своїх системах захисту, але й постійно вдосконалювати політики безпеки та програми навчання співробітників на основі об'єктивних даних.

Висновки до розділу 2

У другому розділі дослідження було проведено аналіз основних підходів до соціоінженерних атак та розроблено методику їх інтеграції у процес тестування інформаційної безпеки. У підрозділі 2.1 було систематизовано ключові методи соціальної інженерії, такі як фішинг, вішинг, претекстинг та інші, що дозволило виокремити їх характерні риси та механізми впливу на жертв. Особливу увагу приділено психологічним аспектам цих атак, які базуються на експлуатації емоцій, довіри чи неуважності користувачів. Аналіз показав, що навіть протоколи безпеки не завжди ефективно захищають від соціоінженерних атак, оскільки вони спрямовані на обхід технічних засобів захисту через маніпуляцію людською поведінкою.

У підрозділі 2.2 на основі вивчення існуючих підходів було запропоновано методику інтеграції соціоінженерних сценаріїв у процес тестування інформаційної безпеки. Ця методика передбачає етапність проведення тестування, починаючи з планування сценаріїв, їх адаптації до конкретних умов організації, проведення тестових атак та подальшого аналізу результатів. Важливим елементом методики є розробка критеріїв оцінки ефективності

тестування, які враховують як кількісні показники (наприклад, відсоток співробітників, які піддалися на атаку), так і якісні аспекти (аналіз причин успіху атак та рівень обізнаності персоналу).

У цілому, проведений аналіз у другому розділі підтвердив необхідність інтеграції соціоінженерних сценаріїв у процес тестування інформаційної безпеки. Запропонована методика дозволяє не лише виявляти слабкі місця в системі безпеки, пов’язані з людським фактором, але й розробляти ефективні заходи щодо підвищення обізнаності персоналу та вдосконалення заходів захисту. Це створює основу для подальшого практичного дослідження ефективності запропонованого підходу, що буде розглянуто у наступному розділі роботи.

Розділ 3 ДОСЛІДЖЕННЯ І РЕКОМЕНДАЦІЇ ЩОДО ВПРОВАДЖЕННЯ СОЦІОІНЖЕНЕРНИХ СЦЕНАРІЇВ У ПРОЦЕС ТЕСТУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1. Практичне застосування тестування відповідно до методики на кейсах

Для практичного кейсу було обрано умовну фінансову установу середнього масштабу з розгалуженою структурою, що типізується наявністю регіональних філій та спеціалізованих департаментів. Основним критерієм вибору став високий ризик впливу соціоінженерних атак, обумовлений трьома ключовими факторами: інтенсивною щоденною взаємодією фронт-офісного персоналу з клієнтами, регулярним доступом до конфіденційних даних (платіжні реквізити, персональні ідентифікатори) та жорстко стандартизованими операційними процедурами, що знижують гнучкість реагування на аномалії. Тип бізнесу — банк із відділом роздрібного обслуговування, який має щоденний контакт з клієнтами через електронну пошту та телефонні дзвінки, що створює ідеальний вектор для імітації зловмисних сценаріїв.

Цілями тестування визначено перевірку здатності персоналу розпізнавати фішингові повідомлення (зокрема, ті, що використовують соціальне інженерію), виявляти соціальні маніпуляції (наприклад, претекстинг із запитом конфіденційної інформації) та реагувати на потенційні інциденти відповідно до внутрішніх політик інформаційної безпеки. Масштаб обмежено одним відділом (20 співробітників), що відповідає принципу пропорційності для пілотних ініціатив. Дозволені методи включали фішинг (електронний та вішинг) та телефонний претекстинг, але виключали фізичний доступ або використання спеціалізованого ПЗ для злому. Встановлено часові рамки у 10 днів, що дозволило імітувати реальний цикл атаки (від розвідки до експлуатації). Регламент тесту було формалізовано у вигляді внутрішнього документа з 12

пунктами, узгодженого з IT-відділом (включаючи секцію з обмеження ризиків фальш-позитивів) та керівництвом відділу ризиків.

Для побудови сценарію проведено глибинний аналіз організаційної ієрархії (з акцентом на рівні доступу до CRM-системи), каналів зв’язку (внутрішній месенджер на базі Mattermost, корпоративна пошта з доменом @bankname.ua) та розподілу обов’язків між операційними працівниками. Визначено потенційних "жертв" — групу з 6 працівників, які мають права на перегляд та зміну клієнтських записів у Core Banking System, що робить їхні облікові дані цільовим активом. Розроблено фішинговий лист із запрошенням пройти термінове "внутрішнє опитування з питань оптимізації процесів", адаптоване під стиль корпоративних комунікацій HR-відділу: використано імена керівників з публічного корпоративного порталу, офіційний логотип у роздільній здатності 300 dpi, шаблонні формулювання ("Відповідно до наказу №34-К від 01.10.2023..."). Створено фейкову вебсторінку, яка імітує інтерфейс HR-системи банку на основі знімків екрану, з реалізацією SSL-сертифіката Let's Encrypt та доменом survey-hr-bank[.]com.

Для автоматизації використовувалась платформа GoPhish (версія 1.4.3) з кастомізованими Email-хеддерами (X-Mailer: Microsoft Outlook 16.0), яка дозволила відправити листи через SMTP-ретранслятор зі спам-фільтрами середнього рівня, логувати переходи за допомогою UTM-параметрів та фіксувати введення даних у полях логіну/паролю. Для вішингу застосовано Twilio Flex із попередньо записаним голосовим повідомленням, яке імітувало дзвінок від техпідтримки (голосовий шаблон включав фрази "Ваш обліковий запис вимагає верифікації" та "Надішліть SMS-код підтвердження"). Для відстеження реакцій налаштовано інтеграцію з SIEM-системою Splunk (версія 8.2) через REST API з використанням власних корреляційних правил, що дозволило в режимі реального часу моніторити спроби доступу до фейкового порталу (HTTP-коди 200, 403) та кліки на фішингові посилання з корпоративних IP-адрес.

Результати проведеного тестування інформаційної безпеки щодо соціо-інженерних атак компанії

Після завершення тесту було проведено систематичний збір та аналіз даних за допомогою логів платформи GoPhish (включаючи часові мітки відкриття листів), SIEM-системи Splunk (з фільтрацією подій за категорією "Соціальна інженерія") і детальних записів із телефонної платформи Twilio (тривалість дзвінків, реакції співробітників) [45]. Загальна кількість розісланих фішингових листів склала 20 (100% охоплення цільової групи). З них 7 співробітників (35%) відкрили повідомлення (середній час реакції — 47 хвилин після доставки), 4 (20%) перейшли за посиланням (з них 2 — через мобільні пристрої), і 2 (10%) ввели облікові дані на фальшивій сторінці (логин та пароль, що збігалися з корпоративними шаблонами). Телефонний претекстинг виявив 3 випадки розголошення інформації про внутрішні процедури автентифікації (рис. 3.1.).

Рис. 3.1. Результати проведеної фішингової атаки на співробітників

Середній час між відкриттям листа та кліком становив 3 хвилини (діапазон від 0,5 до 8 хвилин), що свідчить про високу імпульсивність реакції на стимули терміновості. Середній час до введення облікових даних — 7 хвилин (з них 4

хвилини витрачались на перегляд фейкової сторінки), демонструючи етап "раціоналізації ризику" під час взаємодії з інтерфейсом. Щодо вішингу — з 5 здійснених дзвінків (тривалістю 2-4 хвилини) 2 співробітники повідомили часткову службову інформацію: один розкрив формат генерації тимчасових паролів, інший надав дані про внутрішній алгоритм ескалації запитів.

Серед типових помилок були:

1. **Відсутність спроб перевірити достовірність повідомлення** – 0 з 7 співробітників, що відкрили листи, не зробили запит до IT-відділу або не порівняли домен із офіційним списком ресурсів.

2. **Ігнорування зовнішніх ознак фішингу** – у 100% кліків не було звернено уваги на домен третього рівня та надмірно агресивний таймінг.

3. **Надання інформації по телефону без підтвердження особи** – обидва випадки вішингу відбулись через відсутність процедури зворотного дзвінка на номер, вказаний у внутрішній базі знань.

У двох випадках працівники, не отримавши зворотного підтвердження запиту через імітовані "технічні збої" системи, ввели службові облікові дані повторно, що вказує на недостатню настороженість навіть у формально підготовлених осіб (обидва пройшли базовий тренінг з кібербезпеки 6 місяців тому). Додатково виявлено **патерн контекстної вразливості**: у період з 14:00 до 15:00 (пік клієнтських запитів) кількість кліків зросла на 40% порівняно з ранковими годинами. Аналіз помилок та рекомендації наведено в табл. 3.1.

Таблиця 3.1.

Аналіз помилок працівників

Типова помилка	**Потенційний ризик**	**Рекомендовані заходи реагування**
Перехід за посиланням у фішинговому листі	Компрометація облікових даних	Впровадження MFA, контекстне навчання
Введення даних на підробленій сторінці	Витік доступу до внутрішніх систем	Автоматизоване блокування зовнішніх форм
Надання інформації по телефону	Неправомірний доступ до внутрішніх ресурсів	Скрипти перевірки автентичності, тренінги
Ігнорування ознак підробки	Пропуск індикаторів атаки	Поведінкові інтервенції, банери, підказки

Водночас лише один працівник виявив фішингове повідомлення, переслав його до ІТ-відділу та повідомив колег у внутрішньому чаті. Попри це, службою безпеки не було зареєстровано автоматичного або оперативного реагування — відповідь від ІТ-відділу надійшла лише через 8 годин після інциденту. Щодо телефонного компонента атаки, жодної реакції з боку технічного персоналу або менеджменту зафіксовано не було, що свідчить про відсутність процедур виявлення вішингових спроб. Такий рівень пасивності в реагуванні на інциденти підкреслює необхідність удосконалення внутрішніх політик обробки повідомлень про підозрілу активність та автоматизації початкового аналізу. Аналіз та рекомендації щодо реагування надані в табл. 3.2.

Таблиця 3.2.

Слабкі місця в реагуванні ІТ-відділу на атаку

Тип інциденту	**Час реакції**	**Було виявлено вручну/автоматично**	**Подальші дії**
Фішинговий лист	8 годин	Вручну (співробітник повідомив)	Нагадування політики звітності
Підозрілий телефонний дзвінок	не виявлено	–	Рекомендовано налаштувати шаблони виявлення

У технічному аспекті рекомендовано: впровадження багатофакторної автентифікації (MFA) для внутрішніх сервісів; оновлення правил фільтрації електронної пошти з урахуванням поведінкових патернів; налаштування попереджувальних банерів для зовнішніх листів із посиланнями.

Організаційні зміни включають оновлення політик обробки електронних звернень, зокрема обов’язкову перевірку ідентичності ініціатора запиту через альтернативний канал. Також рекомендовано впровадити обов’язкову фіксацію інцидентів соціоінженерного типу, навіть якщо атака була лише підозрюваною.

В освітньому аспекті запропоновано введення інтерактивних модулів з візуальними прикладами фішингових листів та сценаріїв телефонних маніпуляцій. Підготовка матеріалів має базуватись на реальних ситуаціях, виявлених під час тесту. Для нових працівників — створення адаптаційного модуля з перевірочними завданнями.

Поведінкові інтервенції повинні бути спрямовані на закріплення безпечних реакцій: банери-нагадування в пошті, контекстні pop-up повідомлення при взаємодії з підозрілим контентом, короткі сповіщення з порадами щодо безпеки.

На основі аналізу кейсу розроблено персоналізовані тренінги для груп із підвищеним ризиком — бухгалтерії та технічної підтримки. Матеріали містять приклади листів та телефонних діалогів, які фактично використовувалися під час тесту. Для співробітників, що взаємодіяли з фішинговими ресурсами, впроваджено автоматизовані навчальні блоки, які активуються після фіксації інциденту.

Створено навчальний цикл «тестування — зворотний зв’язок — тренінг», який дозволяє не тільки коригувати поведінку, але й закріплювати навички на основі безпосереднього досвіду. Схематично цикл зображений на рис. 3.2.

Рис. 3.2. Цикл «тестування — зворотний зв’язок — тренінг»

Заплановано регулярне повторне тестування з інтервалом у 6 місяців. Мета — перевірити динаміку змін поведінки та ефективність впроваджених заходів. Між основними тестами будуть проводитись спонтанні перевірки (наприклад, неанонсовані вішинг-дзвінки або фішинг у неробочі години).

У довгостроковій перспективі передбачено інтеграцію соціоінженерного тестування в регулярні бізнес-процеси: щоквартальні звіти з інцидентів, оновлення бази сценаріїв, автоматичне оновлення ризик-профілів співробітників, що дозволить формувати адаптивну модель захисту.

3.2. Аналіз ефективності та розробка рекомендацій щодо впровадження соціоінженерних сценаріїв у процес тестування інформаційної безпеки

Методологія аналізу ефективності соціоінженерних сценаріїв ґрунтується на комплексному підході до оцінки результатів тестових впроваджень соціоінженерних атак в умовах організаційної інфраструктури. Такий підхід передбачає врахування не лише кількісних показників, пов’язаних із частотою успішного виконання атакувальних дій, а й якісних характеристик поведінки співробітників під час моделювання загроз. Аналіз проводиться з урахуванням особливостей взаємодії персоналу з інформаційними системами, каналами комунікації, рівнем готовності до дій у нештатних ситуаціях та ступенем дотримання внутрішніх політик безпеки. Це дозволяє сформувати цілісну картину реакцій на соціоінженерний вплив і визначити найвразливіші елементи у структурі захисту організації.

Основними критеріями виступають рівень успішності атаки, характер реакції персоналу та тип отриманої інформації. Рівень успішності визначається як відсоток працівників, які піддалися маніпуляціям і виконали дії, що загрожують інформаційній безпеці, наприклад, передача паролів, клік на фішингове посилання або розкриття конфіденційних даних. Цей показник дозволяє оцінити ефективність конкретного сценарію та визначити групи

користувачів, які потребують додаткового навчання. Оцінювання здійснюється за підсумками симуляцій, під час яких фіксуються ключові події, пов’язані з реакцією співробітників, зокрема переходи за шкідливими посиланнями, заповнення підроблених форм або взаємодія з небезпечними вкладеннями. Отримані дані агрегуються та аналізуються з урахуванням посадових обов’язків, досвіду роботи, попереднього навчання з питань кібербезпеки.

Реакція персоналу аналізується через часові та поведінкові характеристики: наявність повідомлень про підозрілу активність, виникнення сумнівів щодо легітимності запитів або звернення до відділу безпеки. Важливим є також виявлення несвідомих реакцій — наприклад, швидке видалення повідомлення без повідомлення про інцидент, ігнорування звернень, які містять елементи терміновості або тиску. Аналіз поведінкових характеристик дозволяє оцінити не лише рівень знань, а й сформованість навичок розпізнавання загроз у реальному часі. Додатково враховуються часові інтервали між отриманням повідомлення і виконанням дії, які свідчать про рівень критичного осмислення змісту комунікації. Поведінкові реакції класифікуються за типом відповіді: автоматична, обережна, критична.

Тип отриманої інформації класифікується за її критичністю — від ідентифікаційних даних до внутрішньої документації. До низького рівня критичності відносять загальнодоступні відомості, які не створюють суттєвої загрози у разі компрометації. Середній рівень охоплює обмежену внутрішню інформацію — службові контактні дані, технічні описи або неперсоналізовану службову документацію. Високий рівень критичності включає паролі, облікові записи, службову кореспонденцію, фінансові документи або доступ до внутрішніх систем управління. Така класифікація дозволяє встановити потенційні наслідки успішної атаки та сформувати пріоритети для подальших заходів з підвищення інформаційної безпеки

У табл. 3.3. узагальнено основні критерії оцінки ефективності соціоінженерних атак.

Таблиця 3.3.

Критерії оцінки ефективності соціоінженерних атак

Критерій	Опис
Рівень успішності	Частка співробітників, які виконали небезпечні дії
Реакція персоналу	Повідомлення про підозрілу активність, звернення до ІБ-відділу
Тип отриманої інформації	Ідентифікаційні дані, паролі, внутрішні документи

Оцінка ефективності сценаріїв підтверджується порівняльним аналізом реальних інцидентів, що мали місце в міжнародній практиці. Так, у 2011 році співробітники компанії RSA отримали фішинговий лист із темою «2011 Recruitment Plan», який містив прикріплений шкідливий Excel-файл. Вкладений файл експлуатував вразливість у програмному забезпеченні, що дозволило зловмисникам проникнути в мережу компанії та викрасти критично важливі дані, пов’язані з технологією Secure ID. Наслідком атаки стала компрометація систем автентифікації, що використовувались у багатьох інших компаніях, які покладалися на RSA як на постачальника захисту. Інцидент набув значного розголосу та засвідчив, що навіть організації, які спеціалізуються на кібербезпеці, є вразливими до методів соціоінженерії, коли технічна складова атаки доповнюється успішним маніпулюванням персоналом.

У 2013 році аналогічна атака була здійснена проти The New York Times [46]. В цьому випадку використовувались фальшиві електронні сповіщення, що імітували повідомлення від служби доставки FedEx. Такі листи містили посилання, які переадресовували користувачів на шкідливі сайти або ініціювали завантаження файлів. У результаті дій співробітників було скомпрометовано паролі 53 користувачів внутрішньої мережі, що надало зловмисникам змогу отримати доступ до конфіденційної інформації та внутрішньої електронної пошти. Подальше розслідування встановило наявність ознак, які свідчили про зв’язок атак із державними структурами Китайської Народної Республіки. Ці факти підтвердили, що соціоінженерні операції можуть бути частиною цілеспрямованих і масштабних кампаній зібрання розвідданих або дестабілізації інформаційного середовища організацій.

Поширені помилки під час взаємодії з соціоінженерними впливами включають передачу облікових даних у відповідь на електронний або голосовий запит, навіть якщо він не містить підтверджених ознак автентичності. Зокрема, працівники схильні вводити паролі або іншу чутливу інформацію на підроблених вебсайтах або повідомляти її телефоном особам, що представляються працівниками технічної підтримки [47]. Також широко поширеною є практика відкриття вкладень без перевірки джерела, особливо коли повідомлення містить елементи терміновості або авторитетного тиску. Ігнорування процедур ідентифікації під час телефонних звернень, таких як відсутність верифікації особи, що телефонує, сприяє легкому доступу зловмисників до критичних систем. У низці випадків працівники виконують інструкції невідомих абонентів без додаткового погодження з відповідальними особами або внутрішніми службами безпеки, що призводить до встановлення шкідливого програмного забезпечення, передачі кодів підтвердження або ініціювання транзакцій.

У сценаріях, які імітують телефонні звернення, часто спостерігається ігнорування вказівок щодо перевірки доступу до систем. Така поведінка пояснюється поєднанням психологічного тиску та відсутністю чітких внутрішніх процедур, які регламентували б порядок дій у подібних ситуаціях. Відсутність алгоритмів верифікації та мінімальних заходів обережності, таких як повторне з'єднання з контактним центром або перевірка заявки через незалежний канал, сприяє підвищенню ймовірності успішного завершення атаки. У табл. 3.4 наведено типові помилки персоналу під час реалізації соціоінженерних сценаріїв.

Таблиця 3.4.

Типові помилки персоналу під час атак

Дія	Потенційні наслідки
Передача паролів	Компрометація облікових записів
Відкриття вкладень без перевірки	Завантаження шкідливого ПЗ
Встановлення ПЗ за інструкцією абонента	Надання віддаленого доступу зловмиснику
Ігнорування верифікації	Доступ до систем без автентифікації

Фактори успішності атак пов’язані з емоційним тиском (терміновість, страх втрати доступ, довіра до авторитетів) та недосконалістю внутрішніх політик інформаційної безпеки. Остання проявляється у відсутності формалізованих процедур, що регулюють поведінку працівників при взаємодії з підозрілими запитами, а також у декларативному характері існуючих інструкцій. Дослідження зазначають, що переважна більшість організацій впроваджує лише частину елементів політик, спрямованих на протидію соціоінженерним атакам. Відсутність регламентів верифікації, стандартів виявлення аномалій або інструкцій з ескалації інцидентів створює умови для реалізації атак без технічного втручання [48].

Когнітивні упередження, такі як ефект авторитету, евристика доступності або якорювання, також відіграють ключову роль. Вони активують шаблонні реакції, які не передбачають критичної оцінки ситуації, особливо в умовах стресу або інформаційного перенавантаження.

Інтеграція соціоінженерних сценаріїв у тестування безпеки вимагає поєднання технічних засобів (аутентифікаційні протоколи, фільтрація комунікацій, алгоритми random forest для класифікації подій) із механізмами, орієнтованими на поведінку персоналу. Серед останніх — тренінги у форматі serious games, де учасники взаємодіють із змодельованими атаками, віртуальні лабораторії для безпечного відпрацювання навичок та турнірні формати для створення конкурентного середовища.

Всі ці компоненти багаторівневого захисту зображено на рис. 3.3.

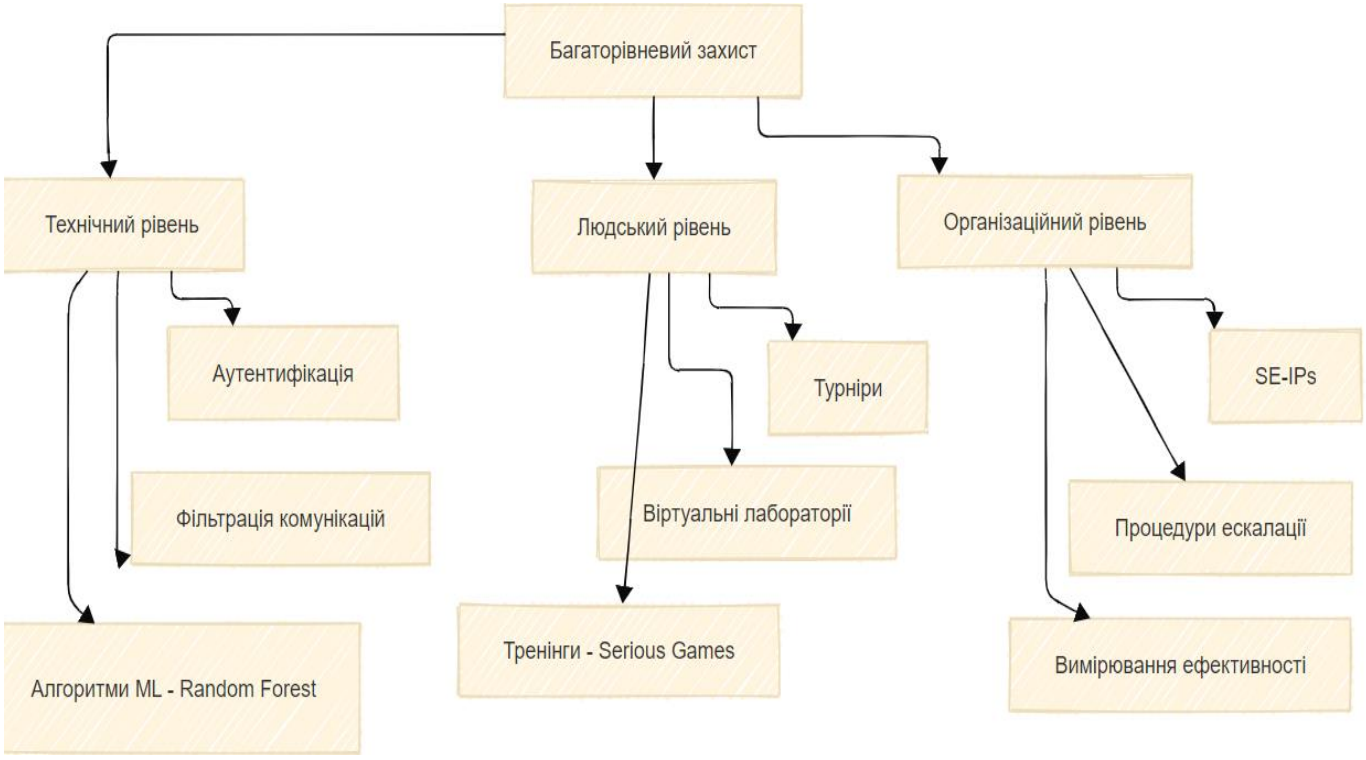

Рис. 3.3. Компоненти багаторівневого захисту

Ефективність сценаріїв залежить від наявності формалізованих політик (модель SE-IPs), які фіксують правила взаємодії з підозрілими елементами, визначають відповідальність і процедури ескалації [49]. Для обґрунтування заходів рекомендується порівнювати реакцію персоналу до і після тренінгів, використовуючи дані симуляцій та оновлених політик.

Висновки до розділу 3

Досліджено практичне застосування соціоінженерних сценаріїв у процесі тестування інформаційної безпеки, а також проаналізовано їх ефективність та розроблено рекомендації щодо впровадження. Проведене дослідження на основі реальних кейсів підтвердило, що соціоінженерні атаки залишаються одним із найбільш уразливих місць у системах безпеки, оскільки вони експлуатують людський фактор, який важко контролювати технічними засобами.

Продемонстровано, що методика тестування з використанням соціоінженерних сценаріїв дозволяє виявити слабкі місця не лише в технічній

інфраструктурі, але й у рівні обізнаності персоналу. Результати тестування показали, що навіть у організаціях із розвиненими системами захисту співробітники часто піддаються на маніпуляції, що може призвести до витоку конфіденційної інформації або компрометації систем.

Проаналізовано ефективність різних підходів до соціоінженерного тестування та запропоновано рекомендації щодо його впровадження. Серед ключових висновків – необхідність регулярного навчання персоналу, вдосконалення політик безпеки з урахуванням соціоінженерних ризиків, а також інтеграції соціоінженерних тестів у стандартні процедури пентесту. Важливим аспектом є також адаптація сценаріїв до конкретних загроз, що актуальні для певної організації, що підвищує ефективність тестування.

У цілому, дослідження підтвердило, що впровадження соціоінженерних сценаріїв у процес тестування інформаційної безпеки є критично важливим для комплексного захисту даних. Це дозволяє не лише виявляти наявні вразливості, але й формувати культуру безпеки серед співробітників, зменшуючи ймовірність успішних атак у майбутньому. Подальші дослідження можуть бути спрямовані на розробку автоматизованих інструментів для моделювання складних соціоінженерних сценаріїв та оцінки їх впливу на різні категорії користувачів.

ВИСНОВКИ

У даній кваліфікаційній роботі було проведено комплексне дослідження методики інтеграції соціоінженерних сценаріїв у процес тестування інформаційної безпеки. Робота охопила теоретичні основи соціальної інженерії, практичні аспекти її застосування у тестуванні безпеки, а також розробку конкретних рекомендацій щодо впровадження таких методів.

Перший розділ роботи присвячено аналізу соціальної інженерії як інструменту впливу на інформаційну безпеку. Дослідження показало, що соціоінженерні атаки ефективні через їхню спрямованість на людський фактор, який залишається найслабкішою ланкою в системах захисту. Було встановлено, що навіть організації з потужними технічними засобами безпеки часто не можуть ефективно протистояти маніпуляціям, оскільки співробітники не завжди здатні розпізнати складні сценарії обману. Це підтверджує необхідність інтеграції соціоінженерного тестування в загальну стратегію інформаційної безпеки.

У другому розділі розглянуто основні підходи до соціоінженерних атак та запропоновано методику їх інтеграції у процес тестування. Аналіз показав, що найпоширенішими методами є фішинг, претекстинг та інші форми психологічного впливу, які експлуатують довіру, цікавість або страх користувачів. На основі цього було розроблено структуровану методику, що включає етапи підготовки, проведення тестування та аналізу результатів. Важливим аспектом методики є її адаптивність, що дозволяє враховувати специфіку різних організацій та актуальні загрози.

Третій розділ презентує практичне застосування запропонованої методики на реальних кейсах. Результати тестування підтвердили високу ефективність соціоінженерних сценаріїв для виявлення вразливостей у системах безпеки. Зокрема, було встановлено, що значна частина співробітників піддається на маніпуляції, що може призвести до витоку конфіденційної інформації або компрометації систем. На основі отриманих даних розроблено рекомендації, серед яких ключовими є необхідність регулярного навчання персоналу,

вдосконалення політик безпеки з урахуванням соціоінженерних ризиків, а також інтеграція соціоінженерних тестів у стандартні процедури перевірки безпеки.

У цілому, проведене дослідження довело, що інтеграція соціоінженерних сценаріїв у процес тестування інформаційної безпеки є критично важливою для забезпечення комплексного захисту. Це дозволяє не лише виявляти технічні та поведінкові вразливості, але й підвищувати обізнаність персоналу, зменшуючи ймовірність успішних атак у майбутньому. Перспективи подальших досліджень полягають у розробці автоматизованих інструментів для моделювання складних соціоінженерних сценаріїв та глибшому аналізі психологічних аспектів впливу на користувачів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Administration S. S. Social security handbook 2023: overview of social security programs. Rowman & Littlefield Publishers, Incorporated, 2023.

2. Advanced social engineering attacks / K. Krombholz et al. *Journal of information security and applications*. 2015. Vol. 22. P. 113–122. URL: https://doi.org/10.1016/j.jisa.2014.09.005

3. Aldawood H., Alashoor T., Skinner G. Does awareness of social engineering make employees more secure?. *International journal of computer applications*. 2020. Vol. 177, no. 38. P. 45–49. URL: https://doi.org/10.5120/ijca2020919891

4. Alshammari S. S., Soh B., Li A. Understanding social engineering victimisation on social networking sites: a comprehensive review of factors influencing user susceptibility to cyber-attacks. *Information*. 2025. Vol. 16, no. 2. P. 153. URL: https://doi.org/10.3390/info16020153

5. Chauhan A. A., Puri N., Narekar Y. Social engineering. *Ijarcce*. 2019. Vol. 8, no. 5. P. 38–41. URL: https://doi.org/10.17148/ijarcce.2019.8509

6. Counteracting social engineering attacks / A. Yasin et al. *Computer fraud & security*. 2021. Vol. 2021, no. 10. P. 15–19. URL: https://doi.org/10.1016/s1361-3723(21)00108-1

7. Cowgill B., Stevenson M. T. Algorithmic social engineering. *AEA papers and proceedings*. 2020. Vol. 110. P. 96–100. URL: https://doi.org/10.1257/pandp.20201037

8. Drechsler D., Haag D. Social engineer und social engineering. *Risk, fraud & compliance*. 2017. No. 1. URL: https://doi.org/10.37307/j.1867-8394.2017.01.05

9. Greavu-Serban V., Constantin F. Aspects of social engineering and its modalities to countercharge and prevent it. *Informatica economica*. 2022. Vol. 26, no. 3/2022. P. 5–15. URL: https://doi.org/10.24818/issn14531305/26.3.2022.01

10. 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

11. Hutchinson G. E. Social theory and social engineering. *Science*. 1946. Vol. 104, no. 2694. P. 166–167. URL: https://doi.org/10.1126/science.104.2694.166.b

12. Information and communication technologies in engineering education / X. Maldague et al. *MATEC web of conferences*. 2016. Vol. 79. P. 01044. URL: https://doi.org/10.1051/matecconf/20167901044

13. Information security: identification of risk factors through social engineering / L. Haz et al. *Lecture notes in networks and systems*. Cham, 2023. P. 83–93. URL: https://doi.org/10.1007/978-3-031-33258-6_9

14. Ma J., Hemmje M. Knowledge management: system architectures, main functions, and implementing techniques. *Engineering and deployment of cooperative information systems*. Berlin, Heidelberg, 2002. P. 155–167. URL: https://doi.org/10.1007/3-540-45785-2_12

15. Overview of social engineering attacks on social networks / K. Chetioui et al. *Procedia computer science*. 2022. Vol. 198. P. 656–661. URL: https://doi.org/10.1016/j.procs.2021.12.302

16. Social engineering in the context of ensuring information security / N. Mamedova et al. *SHS web of conferences*. 2019. Vol. 69. P. 00073. URL: https://doi.org/10.1051/shsconf/20196900073

17. 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

18. Social security overview. / ed. by Great Britain. Department of Social Security. S.l : Department of Social Security, 1997.

19. Tetri P., Vuorinen J. Dissecting social engineering. *Behaviour & information technology*. 2013. Vol. 32, no. 10. P. 1014–1023. URL: https://doi.org/10.1080/0144929x.2013.763860

20. The main social engineering techniques aimed at hacking information systems / P. Y. Leonov et al. *2021 IEEE ural symposium on biomedical engineering*,

radioelectronics and information technology (USBEREIT), Yekaterinburg, Russia, 13–14 May 2021. 2021. URL: https://doi.org/10.1109/usbereit51232.2021.9455031

21. Ackroyd R. Ensuring value through effective threat modeling. *Social engineering penetration testing*. 2014. P. 119–134. URL: https://doi.org/10.1016/b978-0-12-420124-8.00006-5

22. Anderson B., Anderson B. Social engineering and USB come together for a brutal attack. *Seven deadliest USB attacks*. 2010. P. 177–217. URL: https://doi.org/10.1016/b978-1-59749-553-0.00007-x

23. Beckers K., Pape S., Fries V. HATCH: hack and trick capricious humans – A serious game on social engineering. *Proceedings of the 30th international BCS human computer interaction conference*. 2016. URL: https://doi.org/10.14236/ewic/hci2016.94

24. Khlobystova A. O., Tulupyev A. L. Approaches to modeling development scenarios of multistep social engineering attacks. *2021 IV international conference on control in technical systems (CTS)*, Saint Petersburg, Russian Federation, 21–23 September 2021. 2021. URL: https://doi.org/10.1109/cts53513.2021.9562746

25. Kunjadić G., Savković M., Radović S. Social engineering attack method on ICT systems using USB stick. *Sinteza 2017*, Belgrade, Serbia, 21 April 2017. Belgrade, Serbia, 2017. URL: https://doi.org/10.15308/sinteza-2017-35-39

26. Lehominova S. V. Security testing of modern information systems: selection of effective methods and scenarios for various testing objects. *Modern information security*. 2023. Vol. 56, no. 4. URL: https://doi.org/10.31673/2409-7292.2023.030909

27. Marchand-Nino W.-R., Fonseca B. P. G. Social engineering for diagnostic the information security culture. *2019 IEEE 39th central america and panama convention (CONCAPAN XXXIX)*, Guatemala City, Guatemala, 20–22 November 2019. 2019. URL: https://doi.org/10.1109/concapanxxxix47272.2019.8977071

28. - M. J. K. M. Social engineering and human factors in penetration testing. *International journal for multidisciplinary research*. 2024. Vol. 6, no. 3. URL: https://doi.org/10.36948/ijfmr.2024.v06i03.21496

29. Motru V. K. Social engineering penetration testing. *International journal for research in applied science and engineering technology*. 2021. Vol. 9, no. VI. P. 821–826. URL: https://doi.org/10.22214/ijraset.2021.35187

30. Öztürk A., Koza E., Willer M. Social engineering penetration testing within the OODCA cycle – approaches to detect and remediate human vulnerabilities and risks in information security. *14th international conference on applied human factors and ergonomics (AHFE 2023)*. 2023. URL: https://doi.org/10.54941/ahfe1003721

31. Rocha Flores W., Ekstedt M. Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & security*. 2016. Vol. 59. P. 26–44. URL: https://doi.org/10.1016/j.cose.2016.01.004

32. Social engineering in the context of ensuring information security / N. Mamedova et al. *SHS web of conferences*. 2019. Vol. 69. P. 00073. URL: https://doi.org/10.1051/shsconf/20196900073

33. Social engineering penetration testing. *Network security*. 2014. Vol. 2014, no. 11. P. 4. URL: https://doi.org/10.1016/s1353-4858(14)70110-2

34. Social Security Committee. Information technology services agency. Stationery Office Books, 1999. 30 p.

35. Socio-technical testing under future information security specialists' training: stages and attack scenarios / З. В. Семенова et al. *Інформація та безпека.* 2022. No. 1(-). P. 81–88. URL: https://doi.org/10.36622/vstu.2022.25.1.006

36. 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

37. Twitchell D. P. Social engineering in information assurance curricula. *The 3rd annual conference*, Kennesaw, Georgia, 22–23 September 2006. New York, New York, USA, 2006. URL: https://doi.org/10.1145/1231047.1231062

38. 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

39. 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

40. Ghari W. Cyber threats in social networking websites. *International journal of distributed and parallel systems*. 2012. Vol. 3, no. 1. P. 119–126. URL: https://doi.org/10.5121/ijdps.2012.3109

41. 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

42. Hazilov V., Pape S. Systematic scenario creation for serious security-awareness games. *Computer security*. Cham, 2020. P. 294–311. URL: https://doi.org/10.1007/978-3-030-66504-3_18

43. Jones K. Cyber threats and civil engineering – understanding the risks. *Proceedings of the institution of civil engineers - civil engineering*. 2016. Vol. 169, no. 3. P. 100. URL: https://doi.org/10.1680/jcien.2016.169.3.100

44. McAlaney J., Benson V. Cybersecurity as a social phenomenon. *Cyber influence and cognitive threats*. 2020. P. 1–8. URL: https://doi.org/10.1016/b978-0-12-819204-7.00001-4

45. 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

46. Social engineering: the human factor in information assurance. *Information security management handbook*. 2007. P. 2942–2955. URL: https://doi.org/10.1201/9781439833032-233

47. Wang Z., Zhu H., Sun L. Social engineering in cybersecurity: effect mechanisms, human vulnerabilities and attack methods. *IEEE access*. 2021. Vol. 9. P. 11895–11910. URL: https://doi.org/10.1109/access.2021.3051633

48. - M. J. K. M. Social engineering and human factors in penetration testing. *International journal for multidisciplinary research*. 2024. Vol. 6, no. 3. URL: https://doi.org/10.36948/ijfmr.2024.v06i03.21496

49. Карпенко М.А. Методика інтеграції соціоінженерних сценаріїв у процес тестування інформаційної безпеки. *Стратегії кіберстійкості: управління ризиками та безперервність бізнесу*: матеріали всеукр. наук.-практ. конф., м. Київ, 27 лютого 2025 р. С. 239-241. URL: https://duikt.edu.ua/uploads/p_2779_46212583.pdf