

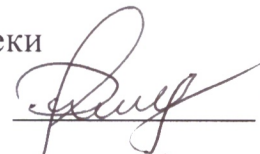
Міністерство освіти і науки України  
Державний університет «Житомирська політехніка»  
Факультет інформаційно-комп'ютерних технологій  
Кафедра комп'ютерної інженерії та кібербезпеки

**ПОЯСНЮВАЛЬНА ЗАПИСКА**  
до випускної кваліфікаційної роботи магістра  
на тему: «Методи та засоби захисту користувача  
інформаційних систем від атак соціальної інженерії»

Виконав: студент 2-го курсу групи КБм-22-1  
спеціальності 125 «Кібербезпека»

 Таргонський О.В.

Керівник: старший викладач кафедри комп'ютерної  
інженерії та кібербезпеки

 Трокоз Є.М.

Рецензент: доцент кафедри комп'ютерної інженерії та  
кібербезпеки, к.т.н., доцент

 Россінський Ю.М.

Житомир – 2023

Державний університет «Житомирська політехніка»  
Факультет інформаційно-комп'ютерних технологій  
Кафедра комп'ютерної інженерії та кібербезпеки  
Спеціальність 125 «Кібербезпека»  
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної  
інженерії

та кібербезпеки

 Сфіменко А. А.  
13 жовтня 2023 р.

## ЗАВДАННЯ

на випускню кваліфікаційну роботу магістра

Студент: Таргонський Олег Вікторович

Тема роботи: **«Методи та засоби захисту користувача інформаційних систем від атак соціальної інженерії»**

затверджена Наказом університету від 13 жовтня 2023 р. № 572/с

Термін здачі студентом закінченої роботи 11 грудня 2023 р.

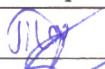
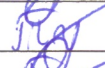
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

1. **Предмет дослідження** – методи та засоби захисту користувача інформаційних систем від атак соціальної інженерії.
2. **Об'єкт дослідження** – процес захисту користувача від атак соціальної інженерії.

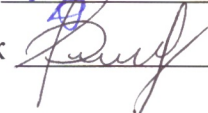
Обладнання та програмне забезпечення:

1. HTML, CSS
2. Редактор коду Notepad ++

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються:

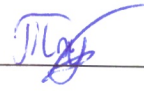
| Розділ | Консультант | Підпис, дата   |                                                                                              |
|--------|-------------|----------------|----------------------------------------------------------------------------------------------|
|        |             | Завдання видав | Завдання прийняв                                                                             |
| 1      | Шелуха О.О. | 16.10.23       | 16.10.23  |
| 2      | Шелуха О.О. | 06.11.23       | 06.11.23  |
| 3      | Шелуха О.О. | 03.12.23       | 03.12.23  |

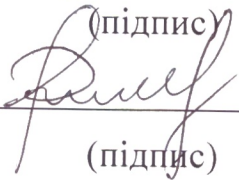
Студент  Таргонський О.В.

Керівник  Трокоз Є.М.

### Календарний план

| № з/п | Назва етапів випускної кваліфікаційної роботи                                                                       | Термін виконання етапів роботи     | Примітка                                                                                          |
|-------|---------------------------------------------------------------------------------------------------------------------|------------------------------------|---------------------------------------------------------------------------------------------------|
| 1     | Постановка задачі. Пошук, огляд та аналіз систем захисту від соціальної інженерії. Опрацювання літературних джерел. | 14 жовтня 2023 – 5 листопада 2023  | Виконано<br>   |
| 2     | Розробка структури системи захисту від фішингових атак                                                              | 16 жовтня 2023 – 20 жовтня 2023    | Виконано<br>   |
| 3     | Написання 1-2 розділу                                                                                               | 23 жовтня 2023 – 10 листопада 2023 | Виконано<br> |
| 4     | Розробка та тестування системи захисту протидії фішинговим атакам                                                   | 27 листопада 2023 – 1 грудня 2023  | Виконано<br> |
| 5     | Написання 3 розділу                                                                                                 | 16 листопада 2023 – 3 грудня 2023  | Виконано<br> |
| 6     | Захист                                                                                                              | 27 грудня 2023                     |              |

Студент  Таргонський О.В.

Керівник  Трокоз Є.М.  
(підпис)

## РЕФЕРАТ

Випускна кваліфікаційна робота магістра складається з проєкту захисту користувачів від атак соціальної інженерії та пояснювальної записки. Пояснювальна записка до випускної роботи містить 69 сторінок, 14 ілюстрацій та 3 таблиці.

Метою роботи є аналіз існуючих методів захисту від атак соціальної інженерії та розробка методу захисту проти атак соціальної інженерії.

У роботі визначено основні завдання для розробки методу захисту користувачів від атак соціальної інженерії, проаналізовано інформацію, яка буде використана для проєктування методу. Представлено опис методів та засобів, які використовують зловмисники для атак соціальної інженерії. Також наводяться приклад фішингової атаки на користувача.

**КЛЮЧОВІ СЛОВА:** СОЦІАЛЬНА ІНЖЕНЕРІЯ, ФІШИНГ, АТАКА НА КОРИСТУВАЧА, МЕТОДИ ЗАХИСТУ, КУЛЬТУРА БЕЗПЕКИ.

## ABSTRACT

The master's thesis consists of a project to protect users from social engineering attacks and an explanatory note. The explanatory note to the final thesis contains 69 pages, 14 illustrations and 3 tables.

The purpose of the work is to analyze existing methods of protection against social engineering attacks and develop a method of protection against social engineering attacks.

The paper identifies the main tasks for developing a method of protecting users from social engineering attacks, analyzes the information that will be used to design the method. A description of the methods and tools used by attackers for social engineering attacks is presented. An example of a phishing attack on a user is also given.

**KEYWORDS:** SOCIAL ENGINEERING, PHISHING, USER ATTACK, PROTECTION METHODS, SECURITY CULTURE.

## ЗМІСТ

|                                                                                                                                    |    |
|------------------------------------------------------------------------------------------------------------------------------------|----|
| ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....                                                                                                     | 8  |
| ВСТУП.....                                                                                                                         | 9  |
| РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ВИВЧЕННЯ АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ .....                                                              | 11 |
| 1.1 Визначення та сутність соціальної інженерії.....                                                                               | 11 |
| 1.2 Основні різновиди атак соціальної інженерії: фішинг, підманювання, техніки обману та маніпуляції .....                         | 15 |
| 1.3 Психологічні фактори, що впливають на успішність атак соціальної інженерії та способи маніпуляції психологією користувачів.... | 17 |
| Висновок до розділу 1 .....                                                                                                        | 22 |
| РОЗДІЛ 2. МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ КОРИСТУВАЧА ІНФОРМАЦІЙНИХ СИСТЕМ ВІД АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ .....                            | 23 |
| 2.1 Нормативно – правова база з протидії методам соціальної інженерії. 23                                                          |    |
| 2.2 Огляд методів ідентифікації та автентифікації користувачів .....                                                               | 27 |
| 2.3. Аналіз використання біометричних технологій у сфері інформаційних систем .....                                                | 32 |
| 2.4. Вплив соціальної інженерії на психологію користувачів та їх поведінку .....                                                   | 39 |
| Висновок до розділу 2 .....                                                                                                        | 41 |
| РОЗДІЛ 3. ПРАКТИЧНЕ ЗАСТОСУВАННЯ МЕТОДІВ ЗАХИСТУ ВІД АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ .....                                               | 43 |
| 3.1 Аналіз інцидентів соціальної інженерії .....                                                                                   | 43 |
| 3.2 Огляд сучасних інструментів та технологій соціальної інженерії .....                                                           | 47 |
| 3.3 Розробка та реалізація стратегій захисту в інформаційних системах                                                              | 51 |
| 3.4 Тестування та оцінка ефективності захисних заходів .....                                                                       | 60 |
| Висновок до розділу 3 .....                                                                                                        | 63 |
| ВИСНОВКИ .....                                                                                                                     | 64 |
| ДОДАТКИ .....                                                                                                                      | 69 |

## ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ООН – Організація Об'єднаних Націй

2FA – Двофакторна аутентифікація

PIN – A personal identification number

ЦРУ – Центральне розвідувальне управління

ISO – International Organization for Standardization

ІБ – Інформаційна безпека

СКУД – Системи контролю доступу

## ВСТУП

У сучасному світі інформаційні системи є невід'ємною частиною людської діяльності. Вони використовуються в бізнесі, освіті, медицині, уряді та інших сферах. Завдяки інформаційним системам ми можемо отримувати доступ до інформації, комунікувати з іншими людьми, виконувати завдання.

Однак інформаційні системи також є вразливими до атак. Одним з найнебезпечніших типів атак є атаки соціальної інженерії. Соціальна інженерія – це вид атаки, в якому зловмисник використовує саме людські вразливості, такі як довіра, співчуття або жадібність, щоб отримати доступ до інформації або системи.

Атаки соціальної інженерії є особливо ефективними, оскільки вони не вимагають технічних знань або навичок. Зловмисник може використовувати прості прийоми, такі як телефонний дзвінок, електронний лист або соціальні мережі, щоб обманути жертву.

Атаки соціальної інженерії можуть призвести до серйозних наслідків, таких як:

- викрадення даних;
- знищення даних;
- втручання в роботу системи;
- шантаж.

Для захисту від атак соціальної інженерії необхідно впроваджувати комплексні заходи, які включають інформаційне, організаційне та технологічне забезпечення захисту.

**Актуальність теми.** В сучасних умовах розвитку інформаційно-комунікаційних технологій все більшого поширення набувають кібератаки з використанням методів соціальної інженерії. На відміну від технічних атак, соціальна інженерія експлуатує "людський фактор" і покладається на маніпулювання користувачами для отримання конфіденційної інформації. Це робить користувачів найбільш вразливою ланкою в системі кібербезпеки. Тому

розробка ефективних методів та засобів захисту від атак соціальної інженерії є вкрай актуальною задачею.

**Мета дослідження** – проаналізувати існуючі методи та засоби захисту користувача від атак соціальної інженерії та запропонувати удосконалення для підвищення рівня захищеності інформаційно-комунікаційних систем.

**Об’єкт дослідження** – процес захисту користувача від атак соціальної інженерії.

**Предмет дослідження** – методи та засоби захисту користувача інформаційних систем від атак соціальної інженерії.

**Методи дослідження** – аналіз науково-технічної літератури, порівняльний аналіз існуючих методів захисту, моделювання захищеності в інформаційних системах.

**Наукова новизна роботи** полягає в удосконаленні існуючих та розробці нових методів і засобів захисту користувача від атак соціальної інженерії на основі комплексного підходу.

**Практичне значення отриманих результатів** – можливість впровадження запропонованих методів і засобів захисту для підвищення рівня інформаційної безпеки організацій та комерційних структур.

# РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ВИВЧЕННЯ АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

## 1.1. Визначення та сутність соціальної інженерії

У контексті кібербезпеки соціальна інженерія є одним з найнебезпечніших типів атак. Це пов'язано з тим, що вона не вимагає технічних знань або навичок. Зловмисник може використовувати прості прийоми, такі як телефонний дзвінок, електронний лист або соціальні мережі, щоб обманути жертву.

Атаки соціальної інженерії можуть мати серйозні наслідки. Вони можуть призвести до крадіжки конфіденційної інформації, витоку даних, втручання в роботу системи або навіть до шантажу.

Термін "соціальна інженерія" був введений в 1980-х роках Дональдом Кларком, професором комп'ютерних наук в Університеті штату Каліфорнія, Берклі. Кларк використовував цей термін для позначення техніки, яку зловмисники використовували для обману користувачів комп'ютерів з метою отримання доступу до їхніх систем [3].

У той час соціальна інженерія була відносно новою технікою, і вона не була широко відома. Однак з розвитком інформаційних технологій соціальна інженерія стала все більш поширеною.

Наприклад, у Стародавній Греції софісти використовували соціальну інженерію для переконання людей у своїй правоті. Вони використовували такі техніки, як риторика, логіка та психологія, щоб переконати своїх слухачів у своїх аргументах.

У Середньовіччі шахраї використовували соціальну інженерію для обману людей. Вони використовували такі техніки, як обман, маніпуляції та виманювання, щоб отримати гроші або майно від своїх жертв.

У Новий час соціальна інженерія використовувалася для політичних цілей. Наприклад, під час Французької революції публічні оратори використовували соціальну інженерію, щоб підняти дух людей і спонукати їх до революції.

У ХХ столітті соціальна інженерія стала все більш поширеною. Вона використовувалася для таких цілей, як реклама, маркетинг і пропаганда.

З розвитком інформаційних технологій соціальна інженерія стала все більш небезпечною. Зловмисники стали використовувати соціальну інженерію для проведення кіберзагроз, таких як фішинг, вішинг і інженерія соціальних мереж.

Розвиток соціальної інженерії від часів звичайних маніпуляцій до сучасних кіберзагроз можна розділити на кілька етапів:

- Етап маніпуляцій (до ХХ століття). На цьому етапі соціальна інженерія використовувалася для обману і маніпуляції людьми в особистому спілкуванні.
- Етап масової пропаганди (ХХ століття). На цьому етапі соціальна інженерія використовувалася для впливу на масову свідомість за допомогою засобів масової інформації.
- Етап кіберзагроз (ХХІ століття). На цьому етапі соціальна інженерія використовується для проведення кіберзагроз, таких як фішинг, вішинг і інженерія соціальних мереж.

Таблиця 1.1

Основні відмінності між соціальною інженерією в ці три періоди

| Період            | Відмінності                                                            |
|-------------------|------------------------------------------------------------------------|
| Маніпуляції       | Соціальна інженерія використовувалася в особистому спілкуванні.        |
| Масова пропаганда | Соціальна інженерія використовувалася для впливу на масову свідомість. |
| Кіберзагрози      | Соціальна інженерія використовується для проведення кіберзагроз.       |

#### 1.1.1. Методи та техніки, якими користуються зловмисники

Сучасна соціальна інженерія є серйозною загрозою кібербезпеці. Зловмисники використовують її для різних атак, таких як фішинг (електронні листи з посиланням на підроблені веб-сайти), вішинг (дзвінки, де зловмисник

виглядає як представник компанії), інженерія соціальних мереж, соціальна інженерія на основі штучного інтелекту та на основі мобільних пристроїв. Атаки можуть призводити до втрати конфіденційних даних або злому облікових записів. Підібрані методи включають в себе підроблення веб-сайтів, дзвінки від імітованих працівників, використання соціальних мереж та застосування штучного інтелекту. Захист від таких атак важливий для збереження конфіденційності інформації [3].

Атаки соціальної інженерії, що становлять серйозну загрозу для безпеки інформації, використовують різноманітні методи та техніки для досягнення своєї мети. Ці атаки можуть приймати форму маніпуляційної соціальної інтеракції, підманювання, фішингу чи інших видів обману [1].

Соціальні інженери використовують довіру, бажання допомогти, цікавість або страх втратити цінне для досягнення своєї мети. Розуміння цих методів є ключовим для розробки ефективних стратегій захисту від атак і збереження конфіденційності інформації.

Методи включають:

- Фальсифікація: створення підроблених документів, веб-сайтів або інших матеріалів для обману жертви та отримання конфіденційної інформації.
- Імітація: представлення зловмисником іншою особою або організацією для обману жертви та отримання доступу до інформації.
- Залякування: використання погроз або насильства для отримання конфіденційної інформації чи доступу до системи.
- Вигода: пропозиція чого-небудь цінного жертві в обмін на конфіденційну інформацію чи доступ до системи.

1.1.2. Психологічні та соціальні механізми, які використовують зловмисники

Зловмисники використовують психологічні та соціальні механізми для досягнення своїх цілей. Ефект авторитетності дозволяє їм виглядати як особи з високим ступенем довіри, намагаючись здобути довіру потенційних жертв. Застосовуючи стадне мислення, зловмисники намагаються переконати, що

багато інших людей вже прийняли ті чи інші рішення, спонукуючи жертву слідувати за ними. Ілюзія контролю створює враження, що жертва має вплив на ситуацію, викликаючи невірне сприйняття реального стану речей. Ці психологічні прийоми дозволяють зловмисникам маніпулювати поведінкою та рішеннями інших.

Механізми:

1. Довіра: жертва довіряє зловмиснику, що може призвести до обману чи розголошення конфіденційної інформації.

2. Співчуття: жертва відчуває співчуття до зловмисника, що може бути використано для отримання допомоги чи інформації.

3. Жадібність: жертва має бажання отримати щось, що пропонує зловмисник, і виконати його вимоги.

#### 1.1.3. Цілі та мотиви зловмисників соціальної інженерії

За атаками соціальної інженерії можуть стояти різні цілі і мотивації зловмисників. Вони можуть бути спрямовані на отримання фінансової вигоди, отримання конфіденційної інформації, шкодування або навіть політичні мотиви. Нижче розглянемо деякі з можливих мотивацій зловмисників:

Фінансова вигода. Багато атак соціальної інженерії мають на меті здобуття фінансової вигоди. Зловмисники можуть використовувати фішингові атаки для отримання конфіденційних банківських даних, номерів кредитних карток або доступу до електронних гаманців [18].

Крадіжка ідентичності. Деякі зловмисники використовують соціальну інженерію, щоб викрасти ідентичність своїх жертв. Вони можуть намагатися отримати доступ до особистих даних, таких як імена, дати народження, номери соціального страхування тощо, щоб здійснити шахрайські дії в ім'я жертви.

Шантаж і завдання шкоди. Деякі атаки соціальної інженерії можуть мати на меті завдати шкоди особі або організації. Зловмисники можуть використовувати отриману інформацію для шантажу, розповсюдження підроблених даних або навіть здійснення фізичної шкоди.

Політична мотивація. В окремих випадках атаки соціальної інженерії можуть бути пов'язані з політичною мотивацією. Зловмисники можуть намагатися отримати доступ до конфіденційних політичних даних або використовувати маніпуляцію, щоб вплинути на погляди або рішення осіб, важливих для політичних процесів.

Ці мотивації не є вичерпним списком, і зловмисники можуть мати інші цілі або мотивації. Важливо розуміти, що атаки соціальної інженерії можуть стати загрозою для будь-якої особи або організації, незалежно від їх статусу чи потреб.

Соціальна інженерія є серйозною загрозою інформаційній безпеці. Зловмисники використовують соціальну інженерію для проведення різноманітних атак, які можуть призвести до крадіжки конфіденційної інформації, витоку даних, втручання в роботу системи або навіть до шантажу.

## 1.2 Основні різновиди атак соціальної інженерії: фішинг, підманювання, техніки обману та маніпуляції

Соціальна інженерія в сучасному інформаційному світі стала невід'ємною частиною стратегій кіберзлочинців. Далі розглянемо основні різновиди атак соціальної інженерії, які включають в себе фішинг, підманювання, техніки обману та маніпуляції [3].

Фішинг – це вид соціальної інженерії, при якому зловмисники відправляють електронне повідомлення від імені надійного джерела, просячи надати конфіденційну інформацію, наприклад, логіни і паролі.

Метою фішингових атак є отримання конфіденційних даних – логінів, паролів, номерів карток або особистої інформації.

Приклади фішингових атак:

- електронний лист від банку про блокування рахунку;
- SMS про проблеми з доставкою, що вимагає введення даних картки;
- повідомлення про злам облікового запису з проханням змінити пароль;

Як захиститися:

- не вводити дані на підозрілих сайтах;
- перевіряти посилання в повідомленнях;
- уникати відповідей на сумнівні прохання;
- використовувати складні паролі та двофакторну аутентифікацію[18].

Підманювання – це метод соціальної інженерії, при якому зловмисники використовують привабливі пропозиції або стимули, щоб заманити жертву в пастку. Наприклад, зловмисники можуть запропонувати жертві безкоштовну продукцію або послугу, якщо вона надасть свою особисту інформацію.

Приклади:

- створення сайту з обіцянкою безкоштовного продукту в обмін на особисті дані;
- розміщення оголошень у соцмережах про безкоштовні товари чи послуги для збору персональної інформації;

Як захиститися:

- скептично ставитися до надто привабливих пропозицій;
- ретельно перевіряти інформацію перед наданням даних;
- не переходити за підозрілими посиланнями;
- перевіряти підозрілі пропозиції з офіційними представниками.

Техніки обману – це методи соціальної інженерії, де зловмисники використовують неправдиву інформацію або маніпуляції, щоб ошукати жертву. Наприклад, створення фейкового сайту компанії для збору особистих даних.

Приклади атак:

- створення фейкового сайту банку для збору логінів і паролів;
- дзвінок від імені співробітника компанії про блокування рахунку з вимогою даних для розблокування.

Як захиститися:

- перевіряти інформацію перед наданням персональних даних;
- не переходити за підозрілими посиланнями;
- звертатися до офіційних представників компанії у разі сумнівів.

Техніки маніпуляції – це методи соціальної інженерії, де зловмисники використовують психологічні прийоми, щоб вплинути на поведінку жертви. Наприклад, грають на емоціях страху чи сорому.

Приклади атак:

- дзвінок від імені поліції про використання даних для шахрайства та вимога надати інформацію;
- пропозиція безкоштовної послуги на сайті в обмін на реєстрацію з наданням персональних даних.

Як захиститися:

- не піддаватись емоціям при отриманні інформації від невідомих осіб;
- ретельно перевіряти інформацію перед прийняттям рішень;
- не дозволяти маніпулювати своїми емоціями.

1.3 Психологічні фактори, що впливають на успішність атак соціальної інженерії та способи маніпуляції психологією користувачів

Сучасна реальність, наповнена взаємодіями та соціальними контактами, відкриває можливості для соціальних інженерів, які використовують психологічні особливості людей для досягнення своєї мети. Розглянемо ключові психологічні аспекти, що піддаються маніпуляціям:

1. Довірливість: Люди за своєю природою довірливі, особливо до тих, кого вони знають або хто має авторитет. Соціальні інженери використовують цю довірливість для обману.

2. Прагнення допомагати: Люди тяжіють допомагати іншим, що може бути використано соціальними інженерами для отримання вигоди, шкідливої для жертви.

3. Цікавість: Люди цікавляться і хочуть знати більше про світ навколо. Соціальні інженери привертають увагу жертви, отримуючи конфіденційну інформацію.

4. Страх втратити щось цінне: Люди бояться втратити гроші, майно або репутацію. Соціальні інженери використовують цей страх для залякування жертви і досягнення своїх цілей [1].

1.3.1 Вразливість людського мислення: Як евристики та соціальна інженерія впливають на рішення та безпеку

У світі, де інформація швидко поширюється, короткі шляхи мислення, відомі як евристики, можуть спрощувати рішення, але також ставити під загрозу вразливість до маніпуляцій соціальних інженерів. Розглянемо деякі ключові психологічні аспекти:

1. Ефект авторитетності:
  - Тенденція довіряти авторитетним особам без належного аналізу.
  - Приклад: Використання імені відомої особи для підтримки аргументу.
2. Стадне мислення:
  - Тенденція впливу групи на індивідуальне прийняття рішень.
  - Приклад: Використання рейтингів чи відгуків для впливу на дії.
3. Ілюзія контролю:
  - Віру в більший контроль над ситуацією, ніж є насправді.
  - Приклад: Створення враження власної безпеки через псевдо-контрольовану ситуацію.

Комбінація ефекту авторитетності, стадного мислення та ілюзії контролю може створювати враження, що легше використовувати для соціальної маніпуляції. Розуміння цих психологічних механізмів може сприяти розвитку критичного мислення та обачливості у власних рішеннях, особливо в соціальних ситуаціях.

1.3.2. Як соціальні інженери маніпулюють нашою психологією

Соціальна інженерія, як вид кіберзлочинності, ґрунтується на вмілому маніпулюванні людською психологією. Цей метод включає застосування різних технік, таких як залякування, лестощі, створення почуття невпевненості та гра на емоціях жертви. Зловмисники все частіше використовують ці стратегії, щоб викликати у потенційних жертв почуття страху та вразливості, з метою досягти

своїх цілей. Розуміння цих технік є ключовим для підвищення обізнаності та забезпечення власної кібербезпеки в епоху, коли соціальна інженерія стає все поширенішим методом атак в кіберпросторі. Розглянемо кожен з методів маніпуляції.

1. Залякування:

- Техніка, що викликає у жертв почуття загрози чи небезпеки.
- Застосовується для змушення до певних дій або розкриття конфіденційної інформації.

2. Лестощі:

- Використання компліментів і позитивного підходу для отримання вигоди.

- Створює позитивне враження та отримує довіру для досягнення мети.

3. Створення почуття невпевненості:

- Включає в себе створення ситуацій, де жертва відчуває власну невпевненість чи неспроможність.
- Використовує психологічний тиск для збільшення вразливості до маніпуляцій.

4. Гра на емоціях жертви:

- Використання емоцій для ефективної маніпуляції.
- Сприйняття через емоції, такі як страх, сором чи вина, може призвести до контролю жертви.

Розуміння цих технік маніпуляції є важливим для захисту від соціальних атак і збереження психологічної стійкості. Навчання розпізнаванню цих прийомів та обачлива реакція на них є ключем до особистої безпеки в світі, де реальна та віртуальна реальність часто переплітаються [2].

1.3.3. Прийоми соціальних хакерів: як вони працюють

Насамперед, слід відзначити, що соціальна інженерія є одним із найпоширеніших методів атак на інформаційну безпеку. Соціальні хакери використовують різні психологічні методи та маніпуляції, щоб отримати доступ до конфіденційних даних або систем.

Один з таких прийомів – принцип взаємності, який базується на природній потребі людей у співробітництві та допомозі. Спочатку соціальний хакер може розкривати особисті проблеми, створюючи враження довіри та співчуття, а потім використовувати це для отримання конфіденційної інформації.

Інша тактика – "нога-в-дверях", коли хакер починає із мінімальних запитань, на які більшість легко згодиться, створюючи враження згоди. Після цього йому може бути легше домогтися більш значущих даних.

Соціальні хакери також можуть створювати хибне враження для отримання доступу до конфіденційної інформації. Вони можуть виглядати як представники компаній, друзі або колеги, щоб підірвати обороноздатність та впевнити людину в своїх намірах.

Для захисту від підступів соціальних хакерів, важливо розрізняти легітимні запитання від підозрілих осіб, уникаючи розкриття конфіденційної інформації неперевіреною особам, чи через неконтрольовані канали зв'язку. Оновлення програмного забезпечення та використання складних, унікальних паролів також допомагають у підвищенні рівня безпеки.

Найважливішими компонентами боротьби з соціальною інженерією є свідомість та розуміння ризиків. Регулярне навчання та тренування з питань безпеки співробітників допомагає уникнути співпраці з соціальними хакерами та зберегти конфіденційні дані в безпеці.

1.3.4. Використання когнітивних упереджень у процесі прийняття рішень: ефект прив'язки, стереотипізація та раціоналізація

Прийняття рішень є неодмінною складовою нашого повсякденного життя. Проте, наші рішення нерідко не є повністю об'єктивними і залежать від ряду когнітивних упереджень, які впливають на наше мислення і сприйняття інформації. Розглянемо три основні когнітивні упередження: ефект прив'язки, стереотипізація та раціоналізація, і їх вплив на процес прийняття рішень.

1. Ефект прив'язки: Ефект прив'язки пояснює, чому ми переоцінюємо значення речей або ідей, з якими вже маємо прив'язку. Це може впливати на

прийняття рішень, роблячи нас надто ризикованими або обмежуючи наше бачення альтернатив.

2. Стереотипізація: Стереотипи можуть значно впливати на прийняття рішень, змушуючи нас переоцінювати чи недооцінювати людей чи ситуації на підставі загальнопоширених уявлень.

3. Раціоналізація: Раціоналізація включає у себе пошук обґрунтувань для наших рішень, навіть якщо вони не є логічними. Це може призвести до втрати об'єктивності та надійності прийняття рішень.

Розуміння когнітивних упереджень, таких як ефект прив'язки, стереотипізація та раціоналізація, допоможе бути більш свідомими та критичними в процесі прийняття рішень. Шляхом визнання цих упереджень, можемо запобігти як небажаним наслідкам, так і покращенню нашого прийняття рішень. Навчання розпізнаванню цих упереджень і розвиток навичок критичного мислення може значно полегшити процес прийняття рішень і покращити життя загалом [2].

1.3.5. Реальні випадки успішної соціальної інженерії. Найвідоміші атаки в період 2020-2023 років

Хоч соціальна інженерія існує вже давно, саме в останні роки вона набула широкого поширення як ефективний інструмент кіберзлочинців. Розглянемо декілька резонансних прикладів.

Атака на Twitter в 2020 році. Зловмисники змогли отримати доступ до акаунтів відомих осіб, включаючи Барака Обаму, Ілона Маска, Білла Гейтса. Вони використали метод "соціального хакінгу" – переконування співробітників Twitter надати паролі.

Фішинг від імені співробітників СБУ 2021 року. Шахраї розсилали листи від імені СБУ зі шкідливими посиланнями, які викрадали дані користувачів. Багато хто повірив у справжність листів через авторитет.

Фішингова атака на Ubiquiti в 2021 році. Хакери розіслали співробітникам компанії підроблені листи від служби техпідтримки зі шкідливими посиланнями, завдяки чому отримали доступ до корпоративної мережі і вкрали дані.

Атака на LinkedIn 2022 року. Зловмисники реєстрували фейкові акаунти під виглядом рекрутерів та виманювали у користувачів особисті дані. Грали на бажанні людей працевлаштуватися.

Фішинг у Viber 2023 року. Шахраї розсилали повідомлення про блокування акаунту через скарги інших користувачів. Жертвам пропонувалося перейти за посиланням, щоб вирішити проблему.

Ці приклади вказують на те, що соціальна інженерія стає все більш вдосконаленою, використовуючи психологічні прийоми для ефективних кібератак. Практичні приклади показують, наскільки важливо бути обережним та навчати персонал розпізнавати можливі загрози в онлайн та офлайн середовищі.

#### Висновок до розділу 1

У першому розділі детально розглянуто теоретичні аспекти вивчення атак соціальної інженерії. Зокрема, наведено визначення та сутність соціальної інженерії, проаналізовано її історичний аспект та еволюцію від простих маніпуляцій до сучасних кіберзагроз. Детально описано методи та техніки, що використовують зловмисники під час атак соціальної інженерії, такі як фішинг, вішинг, персоніфікація тощо. Також розглянуто психологічні та соціальні механізми, які дозволяють маніпулювати користувачами. Проаналізовано можливі цілі та мотивації зловмисників при проведенні атак соціальної інженерії. Серед них фінансова вигода, крадіжка даних, шкода репутації, шпигунство тощо. Окремо розглянуто психологічні фактори, що впливають на успішність атак, зокрема евристики, стереотипи, емоції людини. Описано основні техніки маніпулювання та прийоми соціальних хакерів.

Загалом, розділ дозволяє глибоко зрозуміти сутність та механізми атак соціальної інженерії. На основі цих знань можна розробити ефективні заходи протидії та захисту користувачів від подібних загроз. Висновки стануть фундаментом для подальшого дослідження у наступних розділах.

## РОЗДІЛ 2. МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ КОРИСТУВАЧА ІНФОРМАЦІЙНИХ СИСТЕМ ВІД АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

### 2.1 Нормативно – правова база з протидії методам соціальної інженерії

#### 2.1.1 Нормативно-правова база у сфері кібербезпеки

Нормативно-правова база відіграє важливу роль у протидії атакам. Закони, які протидіють кіберзлочинності, допомагають захистити користувачів і організації від кібератак.

Нормативно-правова база у сфері кібербезпеки виконує низку важливих та ключових функцій, спрямованих на забезпечення ефективного контролю та протидії сучасним кіберзагрозам.

Визначення відповідальності за кіберзлочинність. Закони, які визначають відповідальність за кіберзлочинність, допомагають притягувати кіберзлочинців до відповідальності.

Забезпечення співробітництва між правоохоронними органами. Закони, які забезпечують співробітництво між правоохоронними органами, допомагають ефективніше розслідувати кібератаки.

Захист прав і свобод користувачів. Закони, які захищають права і свободи користувачів, допомагають запобігти порушенням кібербезпеки.

У світі існує велика кількість нормативно-правових актів, розроблених з метою протидії кіберзлочинності, що створює чіткий правовий план для боротьби з цією небезпекою. Серед найважливіших та ключових нормативних документів, які надають законодавчу основу в цьому контексті, можна виділити:

- Конвенція про кіберзлочинність прийнята Радою Європи в 2001 році. Ця конвенція встановлює кримінальну відповідальність за ряд кіберзлочинів, таких як комп'ютерний шахрайство, порушення конфіденційності комп'ютерних даних та розповсюдження шкідливого програмного забезпечення.

- Конвенція про боротьбу з незаконними актами, пов'язаними з використанням комп'ютерних мереж, прийнята ООН в 2001 році. Ця конвенція

встановлює кримінальну відповідальність за ряд кіберзлочинів, таких як злом комп'ютерних систем, шахрайство з використанням комп'ютерних систем та незаконне використання комп'ютерних мереж.

- Закон України "Про кібербезпеку" прийнятий у 2019 році. Цей закон визначає правові та організаційні засади забезпечення кібербезпеки в Україні. Він встановлює вимоги до забезпечення кібербезпеки об'єктів критичної інфраструктури, державних інформаційних ресурсів та персональних даних.

Нормативно-правова база відіграє важливу роль у протидії атакам. Закони, які протидіють кіберзлочинності, створюють умови для того, щоб правоохоронні органи могли ефективно розслідувати кібератаки та притягувати кіберзлочинців до відповідальності. Це, в свою чергу, демотивує кіберзлочинців і знижує рівень кібератак.

#### 2.1.2 Роль правових норм у попередженні соціально-інженерних загроз

Соціально-інженерні загрози, ґрунтуючись на використанні людської психології для отримання доступу до інформації чи систем, є поширеним видом кіберзлочинності. Правові норми відіграють ключову роль у попередженні цих загроз, створюючи правила та механізми для захисту конфіденційності та доступу до інформації в цифровому середовищі.

Щоб підвищити обізнаність громадян про соціально-інженерні загрози, закони, які протидіють кіберзлочинності, можуть визначати правила щодо використання та розголошення персональних даних. Крім того, створення правових засад для притягнення кіберзлочинців до відповідальності за соціально-інженерні атаки важливо для запобігання цього типу кіберзлочинності.

Закон України "Про кібербезпеку" визначає кримінальну відповідальність за кіберзлочини, такі як "незаконне використання інформації, яка містить персональні дані", "розголошення державної таємниці" та "незаконне використання засобів телекомунікації". Це створює правові основи для притягнення кіберзлочинців до відповідальності за соціально-інженерні атаки.

Закони, що регулюють кіберзлочинність, сприяють підвищенню обізнаності громадян щодо соціально-інженерних загроз. Наприклад, Закон України "Про кібербезпеку" містить розділ, присвячений правовим основам захисту персональних даних, визначаючи несанкціоноване використання персональних даних як кіберзлочин, за який передбачена кримінальна відповідальність.

Правові норми також утворюють основи для притягнення кіберзлочинців до відповідальності за соціально-інженерні атаки. Наприклад, Закон України "Про кібербезпеку" передбачає кримінальну відповідальність за "незаконне використання інформації, яка містить персональні дані", "розголошення державної таємниці" та "незаконне використання засобів телекомунікації". Ці злочини можуть бути використані для здійснення соціально-інженерних атак.

Таким чином, правові норми відіграють важливу роль у попередженні соціально-інженерних загроз. Вони допомагають підвищити обізнаність громадян про ці загрози та створюють правові основи для притягнення кіберзлочинців до відповідальності.

Додаткові заходи, які можуть допомогти в попередженні соціально-інженерних загроз:

- Освіта та навчання. Громадяни повинні бути обізнані про різні види соціально-інженерних атак та про те, як їх розпізнавати та протистояти.
- Технічні заходи. Організації повинні впроваджувати відповідні технічні заходи безпеки для захисту своїх систем та даних від соціально-інженерних атак.
- Соціальні заходи. Організації повинні створювати культуру безпеки, яка заохочує співробітників повідомляти про підозрілі події.

Комплексний підхід, який включає в себе правові, освітні, технічні та соціальні заходи, може допомогти в ефективному попередженні соціально-інженерних загроз.

#### 2.1.2 Пропозиції щодо вдосконалення нормативно-правової бази

Нинішня нормативно-правова база у сфері кібербезпеки в Україні є достатньою для вирішення основних завдань у цій галузі. Однак є ряд напрямків, у яких вона може бути вдосконалена.

Одним із напрямків є запровадження більш жорстких санкцій за кіберзлочини. Нинішня практика передбачає, що за більшість кіберзлочинів передбачено лише адміністративну відповідальність. У деяких випадках передбачена кримінальна відповідальність, однак вона є досить м'якою. Наприклад, за порушення конфіденційності персональних даних передбачено штраф у розмірі від 5100 до 10200 гривень. Цей штраф є досить низьким, і тому не є достатньою мірою покарання за такі серйозні злочини.

Ще одним напрямком є розширення сфери застосування нормативно-правової бази на нові види кіберзагроз. З огляду на постійний розвиток світу і зростання кількості кіберзагроз, важливо постійно актуалізувати законодавство. Наприклад, Закон України "Про кібербезпеку" не враховує кібервійну, кібертероризм та кібершпигунство, тому важливо внести відповідні поправки для підвищення рівня кібербезпеки в Україні.

У сфері кібербезпеки спостерігаються актуальні тенденції. Зростання складності кіберзагроз є однією з них, оскільки кіберзлочинці систематично розробляють більш складні та ефективні методи атак. Це вимагає від організацій і громадян підвищувати рівень готовності до кібератак.

Іншою важливою тенденцією є зростання ролі штучного інтелекту в кібербезпеці. Штучний інтелект може використовуватися для виявлення та запобігання кіберзагрозам, але його використання кіберзлочинцями також може призвести до розробки більш ефективних атак.

Розвиток міжнародного співробітництва – ще одна тенденція, що заслуговує на увагу. Країни співпрацюють у боротьбі з кіберзлочинністю, що сприяє ефективній протидії кіберзагрозам.

Нормативно-правова база в цій області відіграє ключову роль у протидії кіберзагрозам і вдосконалення її сприятиме підвищенню рівня кібербезпеки.

Актуальні тенденції вимагають від організацій і громадян підвищувати готовність до кібератак [17].

## 2.2 Огляд методів ідентифікації та автентифікації користувачів

2.2.1 Поняття ідентифікації та автентифікації: різниця та важливість кожного етапу.

Ідентифікація та автентифікація є важливими для забезпечення безпеки систем та даних. Це два різних процеси, які часто плутають, але мають ключову відмінність.

Ідентифікація визначає, хто є користувачем, застосовуючи різні методи, такі як: ім'я користувача, пароль, біометрія або IP-адреса. Це перший крок у забезпеченні безпеки, дозволяючи системі визначити суб'єкта.

Автентифікація, у свою чергу, підтверджує, що ідентифікований користувач дійсно є тим, за кого він себе видає. Це може включати запит на додаткову інформацію, таку як відповідь на секретне запитання або введення коду з мобільного телефону. Цей етап робить складнішим для неавторизованих осіб отримати доступ.

Однак ідентифікація сама по собі недостатня для повноцінного захисту, оскільки може бути використана незаконно. Тільки в поєднанні з автентифікацією вона стає ефективним заходом у протидії несанкціонованому доступу, використанню та модифікації систем та даних.

Ідентифікація та автентифікація використовуються в широкому спектрі систем, включаючи:

- системи комп'ютерної безпеки;
- системи електронної комерції;
- системи управління доступом;
- системи банківських послуг.

Існує безліч методів ідентифікації та автентифікації і вибір конкретного залежить від потреб системи. Найпоширеніші серед них:

1. Ім'я користувача та пароль: найбільш поширений метод, але не завжди надійний.

2. Біометричні дані: відбитки пальців, обличчя або райдужна оболонка ока є більш надійними для ідентифікації.

3. Двофакторна аутентифікація (2FA): включає додатковий етап, такий як код з мобільного телефону, для забезпечення більш високого рівня безпеки.

Важливо використовувати комбінації цих методів для підвищення безпеки систем та ресурсів.

### 2.2.2 Популярні методи паролльної ідентифікації та їх обмеження

Парольна ідентифікація є найпоширенішим методом автентифікації, який використовується в інтернеті та інших системах. Він простий у використанні та запровадженні, але має ряд обмежень.

Стандартний пароль – це простий текст, який користувач створює самостійно. Він є найпоширенішим методом паролльної ідентифікації, оскільки простий у використанні та запам'ятовуванні. Однак стандартні паролі часто легко піддаються злому, оскільки вони часто містять особисту інформацію, таку як імена, дати народження або номери телефонів.

The screenshot shows the Netis Quick Setup interface. At the top, there is a 'netis' logo, a 'Select Language' dropdown menu, and an 'Advanced' button with a gear icon. The main section is titled 'Quick Setup' and contains two sub-sections: 'Internet Connection Type' and 'Wireless Setup'.

**Internet Connection Type**

Options: ☐ DHCP, ☒ Static IP, ☐ PPPoE, ☐ Other

Fields:

- WAN IP Address: 172.16.65.103
- Subnet Mask: 255.255.255.0
- Default Gateway: 172.16.65.1
- Primary DNS: 10.0.0.1
- Secondary DNS: 0.0.0.0 (Optional)

**Wireless Setup**

Fields:

- SSID: netis
- Security: ☐ Disable, ☒ Enable
- Password: password (Please enter 8-63 characters.)

A red rectangle highlights the Password field and its label.

At the bottom, there is a 'Save' button.

Рисунок 2.1 – Приклад стандартного паролю

Парольна фраза – це коротша версія стійкого пароля. Він складається з кількох слів, які пов'язані між собою. Парольні фрази складніше піддаються злому, ніж стандартні паролі, оскільки вони містять більше символів і їх складно передбачити.



Рисунок 2.2 – Приклад парольної фрази

Стійкий пароль – це довгий, складний пароль, який не містить особистої інформації. Він складніше піддається злому, ніж стандартні паролі, парольні фрази або одноразові паролі.

The screenshot shows a web interface for checking password strength. At the top, it says "Перевірте надійність пароля: чи безпечний ваш пароль?" (Check password reliability: is your password safe?). Below this is a text input field containing "c)5F3z%ln2mY5AS". A green bar below the input indicates "Надійний Пароль" (Reliable Password). To the left of the bar, it says "Символів: 15". To the right, there are four green checkmarks with labels: "Великі літери" (Uppercase letters), "Маленькі літери" (Lowercase letters), "Спеціальні символи" (Special symbols), and "Цифри" (Numbers). Below the bar, there are two boxes: a red one on the left saying "Занадто короткий" (Too short) and a green one on the right saying "Включає символи всіх типів" (Includes symbols of all types). Below these is a text box stating: "Ваш пароль надійний. Хакерам було б дуже важко його зламати. Вам не потрібно вносити жодних змін, але обов'язково регулярно змінюйте свій пароль і зберігайте його в надійному місці, щоб уникнути злому." (Your password is reliable. It would be very difficult for hackers to break it. You do not need to make any changes, but you must regularly change your password and store it in a safe place to avoid a breach). Below this is a clock icon and the text "Час на злам паролю Століття" (Time to crack password: Centuries). At the bottom, it says "Рекомендовані паролі — виберіть надійну альтернативу вашому паролю нижче:" (Recommended passwords — choose a reliable alternative to your password below:). There are three buttons with example passwords: "JvR%5bZlcTxgs(tlqT", "jKNF^RAHEXs<leQ2F", and "W@>5?/\_1pf-w&)8;E".

Рисунок 2.3 – Приклад стійкого паролю

Одноразовий пароль – це пароль, який генерується для кожного входу. Одноразовий пароль часто генеруються за допомогою мобільного додатку або апаратного пристрою. Вони складніше піддаються злому, ніж стандартні паролі, оскільки вони змінюються щоразу, коли користувач входить у систему.

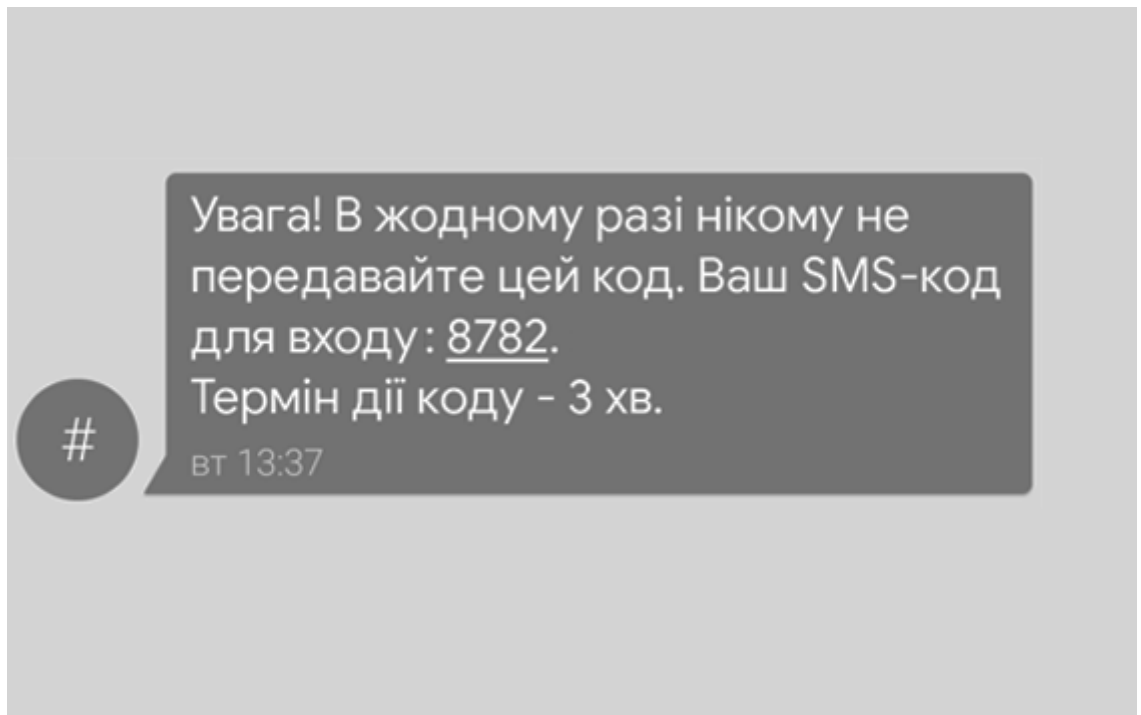


Рисунок 2.4 – Приклад одноразового паролю

Парольна ідентифікація має обмеження, включаючи слабку безпеку, незручність та недоступність для користувачів. Для покращення безпеки можна використовувати такі методи:

1. Використання стійких паролів: Застосування паролів із не менше, ніж 12 символів, що включають комбінації великих і малих букв, цифр та символів.
2. Використання менеджерів паролів: Використання програм, які допомагають генерувати та зберігати складні паролі.
3. Використання двофакторної автентифікації (2FA): Додавання додаткового рівня безпеки за допомогою одноразових кодів, надісланих на телефон або генерованих апаратним пристроєм.

Використання комбінації цих методів може допомогти покращити безпеку парольної ідентифікації та захистити користувачів від атак.

#### 2.2.3 Двофакторна автентифікація: переваги та сценарії використання

Двофакторна автентифікація (2FA) – метод, який вимагає введення додаткового фактора, окрім ім'я користувача та пароля, для входу в систему. Цей

фактор може бути одноразовим кодом, надісланим на телефон користувача, або біометричними даними, такими як відбиток пальця чи обличчя.

Переваги двофакторної аутентифікації (2FA) охоплюють різні аспекти, роблячи її ефективним та надійним засобом захисту:

1. **Покращена безпека:** 2FA додає додатковий шар захисту, ускладнюючи доступ для злоумисників, які знають ім'я користувача та пароль.

2. **Зручність:** 2FA може бути зручнішою для користувачів, оскільки не вимагає запам'ятовування складних паролів.

3. **Заощадження часу:** 2FA допомагає економити час користувачів, уникнувши скидання паролів у випадку їхнього забуття.

Двофакторна аутентифікація використовується у різних сценаріях, таких як вхід у систему, онлайн-шопінг та віддалений доступ. Вона застосовується для захисту облікових записів електронної пошти, банківських рахунків та інших важливих облікових записів, а також для захисту онлайн-покупок та віддаленого доступу до систем.

Різноманітність двофакторної аутентифікації (2FA) охоплює різні типи, які використовують різні методи та засоби впізнавання. Виділяють такі:

1. **Одноразові паролі:** генеруються за допомогою мобільного додатка або апаратного пристрою.

2. **Біометричне розпізнавання:** використовує фізичні характеристики, такі як відбиток пальця або обличчя.

3. **СМС-підтвердження:** використовує текстові повідомлення для надсилання одноразового коду.

Вибір конкретного типу залежить від потреб користувача чи організації. Одноразові паролі прості у використанні, біометричне розпізнавання — надійніше, але може бути менш зручним. СМС-підтвердження менш надійне, але може бути єдиним доступним варіантом.

Рекомендації для максимального захисту при використанні 2FA:

1. Використовуйте стійкі паролі для облікових записів.

2. Увімкніть 2FA для всіх важливих облікових записів.

3. Регулярно оновлюйте пристрої 2FA для уникнення вразливостей.

2FA — важливий інструмент безпеки, який захищає облікові записи від несанкціонованого доступу. Використання його для всіх важливих облікових записів забезпечить ефективний захист [1].

### 2.3. Аналіз використання біометричних технологій у сфері інформаційних систем

#### 2.3.1 Огляд основних біометричних технологій: від сканування відбитків пальців до розпізнавання обличчя

Існує багато різних біометричних технологій, кожна з яких має свої переваги та недоліки. Деякі з найпоширеніших біометричних технологій включають:

Сканування відбитків пальців — це найпоширеніша біометрична технологія. Відбитки пальців унікальні для кожної людини і не змінюються протягом життя. Сканер відбитків пальців використовує світло або інфрачервоне світло для створення цифрового зображення відбитка пальця.

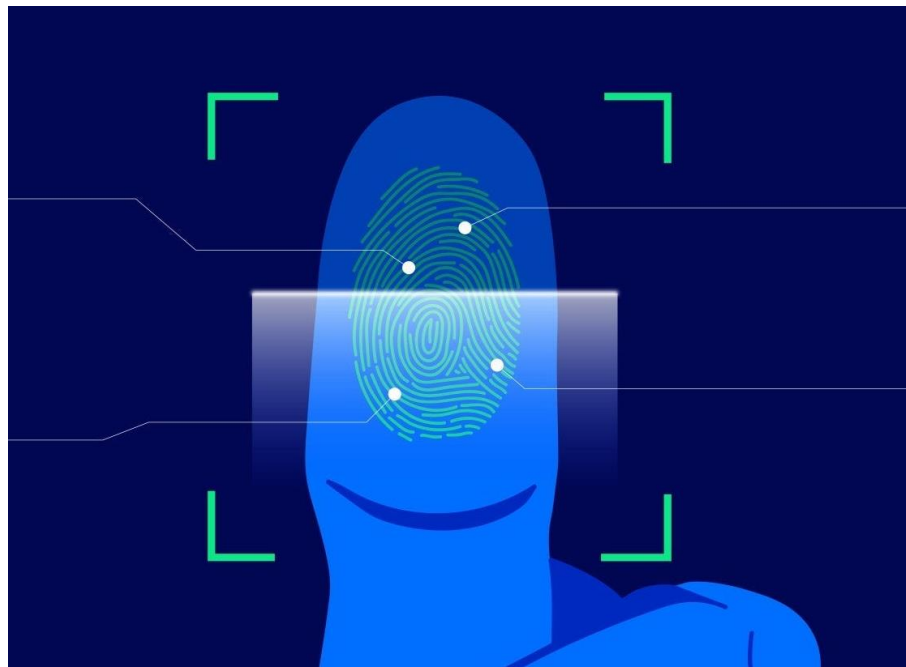


Рисунок 2.5 – Сканування відбитків пальців

Розпізнавання обличчя – це друга за популярністю біометрична технологія. Особа людини унікальна і не змінюється протягом життя. Розпізнавання обличчя використовує камери для створення цифрового зображення обличчя.



Рисунок 2.6 – Розпізнавання обличчя

Сканування райдужної оболонки ока – це біометрична технологія, яка використовує унікальний шаблон райдужної оболонки ока людини для її ідентифікації. Сканування райдужної оболонки ока є одним із найбезпечніших біометричних методів, оскільки райдужна оболонка ока неможливо підробити.



Рисунок 2.7 – Сканування райдужної оболонки ока

Сканування сітківки ока – це біометрична технологія, яка використовує унікальний шаблон сітківки ока людини для її ідентифікації. Сканування сітківки

ока є ще одним із найбезпечніших біометричних методів, оскільки сітківку ока неможливо підробити.



Рисунок 2.8 – Сканування сітківки ока

Розпізнавання голосу – це біометрична технологія, яка використовує унікальний звуковий підпис людини для її ідентифікації. Розпізнавання голосу є зручним способом ідентифікації, оскільки не вимагає фізичного контакту з користувачем.

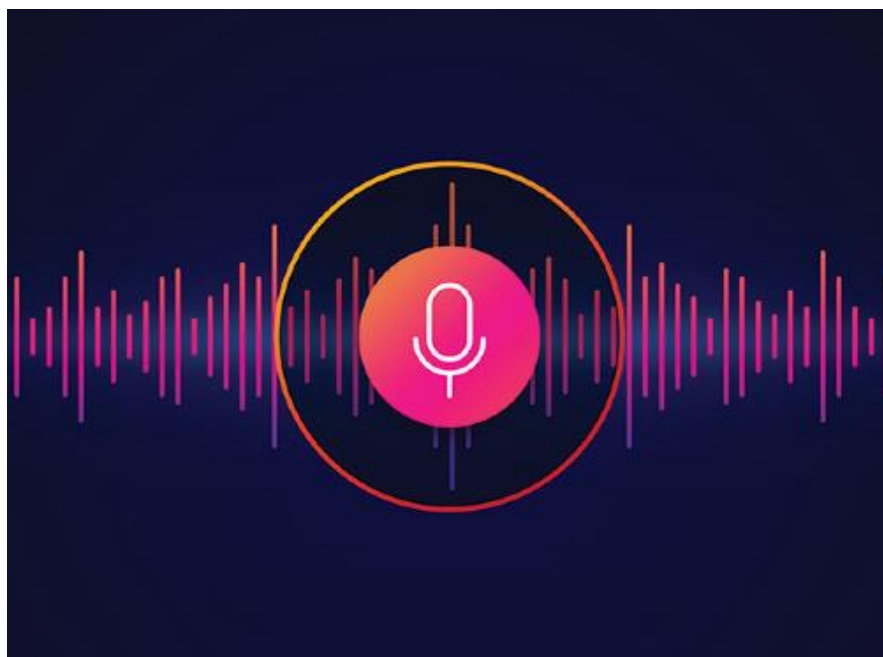


Рисунок 2.9 – Розпізнавання голосу

Сканування вен руки – це біометрична технологія, яка використовує унікальний шаблон вен руки людини для її ідентифікації. Сканування вен руки є відносно новим методом, але він швидко набуває популярності, оскільки є безпечним і зручним.



Рисунок 2.10 – Сканування вен руки

Біометричні технології мають ряд переваг порівняно з традиційними методами ідентифікації, такими як паролі та PIN-коди. Біометричні технології: більш безпечні, зручні та швидкі.

Біометричні дані важко підробити, що робить біометричні технології більш безпечними, ніж традиційні методи ідентифікації. Біометричні технології не вимагають запам'ятовування паролів або PIN-кодів, що робить їх більш зручними для використання. Біометричні технології можуть бути використані для швидкої ідентифікації користувачів.

Біометричні технології стають все більш популярними, оскільки вони пропонують ряд переваг порівняно з традиційними методами ідентифікації. Однак важливо розуміти переваги та недоліки біометричних технологій, перш ніж впроваджувати їх у конкретних застосуваннях.

2.3.2 Переваги та обмеження біометричних технологій в порівнянні з іншими методами ідентифікації

Біометричні технології виходять за рамки традиційних методів ідентифікації, таких як паролі та PIN-коди, маючи кілька вагомих переваг:

1. Більша безпека: Біометричні дані важко підробити, що робить ці технології безпечнішими порівняно з традиційними методами.

2. Зручність: Біометричні технології не потребують запам'ятовування паролів або PIN-кодів, що робить їх більш зручними для використання.

3. Швидкість: Біометричні технології можуть швидко ідентифікувати користувачів, спрощуючи процес доступу.

Важливо розуміти як переваги, так і недоліки біометричних технологій перед їх впровадженням у конкретних застосуваннях.

Таблиця 2.1

Порівняння переваг біометричних технологій та традиційних методів ідентифікації

| Тип технології<br>Переваги | Біометричні технології | Традиційні методи ідентифікації |
|----------------------------|------------------------|---------------------------------|
| Безпека                    | Більш безпечні         | Менш безпечні                   |
| Зручність                  | Більш зручні           | Менш зручні                     |
| Швидкість                  | Швидші                 | Повільніші                      |

Однак біометричні технології також мають деякі недоліки, такі як: вартість, неприйнятність та вразливість.

Біометричні технології можуть бути дорогими для впровадження та підтримки. Деякі люди можуть не приймати біометричні технології з міркувань конфіденційності або комфорту. Біометричні технології можуть бути недостатньо надійними для деяких застосувань, таких як доступ до критичних систем.

Порівняння обмежень біометричних технологій та традиційних методів  
ідентифікації

| Тип технології                        | Біометричні технології            | Традиційні методи ідентифікації   |
|---------------------------------------|-----------------------------------|-----------------------------------|
| <b>Переваги</b>                       |                                   |                                   |
| <b>Вартість</b>                       | Можуть бути дорогими              | Немає                             |
| <b>Неприйнятність для суспільства</b> | Деякі люди можуть не приймати     | Немає                             |
| <b>Недоліки</b>                       | Можуть бути недостатньо надійними | Можуть бути недостатньо надійними |

Біометричні технології мають переваги порівняно з традиційними методами ідентифікації, такими як паролі та PIN-коди. Вони використовуються у безпеці, системах доступу, фінансових операціях та медичній ідентифікації. Проте важливо усвідомлювати їх обмеження перед впровадженням.

Біометричні технології застосовуються в різних сферах, включаючи банківську сферу, медицину та авіацію. Вони гарантують безпеку, контроль доступу та захист фінансових операцій. Також вони використовуються для ідентифікації пацієнтів у лікарнях.

Розвиток біометричних технологій продовжується, і передбачається, що їх використання зросте. Перспективи розвитку включають використання нових характеристик та інтеграцію з іншими технологіями, такими як штучний інтелект та машинне навчання, для підвищення безпеки та зручності.

### 2.3.3 Виклики та питання конфіденційності при використанні біометричних даних

Біометричні технології із використанням біометричних даних, набувають популярності завдяки перевагам порівняно з традиційними методами ідентифікації, такими як паролі та PIN-коди. Проте їхнє використання також викликає виклики та питання конфіденційності.

Зловживання біометричними даними може призвести до крадіжки особистої інформації або несанкціонованого доступу до систем. Також важливо враховувати можливість порушення конфіденційності, оскільки біометричні дані можуть використовуватися для створення профілів людей.

Використання біометричних технологій стикається з низкою викликів, серед яких нерівність доступу є важливою проблемою. Деякі люди, зокрема ті, хто має обмежені можливості, можуть зіткнутися з труднощами у використанні біометричних технологій.

Основним ризиком використання біометричних даних є їхнє зловживання. Хакерські атаки або крадіжка обладнання можуть призвести до незаконного отримання біометричних даних, що дозволяє зловмисникам отримати особисту інформацію та навіть несанкціонований доступ до систем.

Ризик порушення конфіденційності також є важливим аспектом. Біометричні дані унікальні для кожної особи і можуть використовуватися для створення детальних профілів, що може призвести до різноманітних неприємностей, включаючи дискримінацію та шантаж.

Нарешті, біометричні технології можуть бути недоступними для тих, хто має обмежені можливості, таких як люди з порушеннями зору або слуху, які можуть зазнавати труднощі з використанням систем, що вимагають зору або слуху.

Для вирішення викликів і питань конфіденційності, пов'язаних з біометричними даними, існують рекомендації:

1. **Захист біометричних даних:** Важливо застосовувати сильні методи шифрування та аутентифікації для ефективного захисту біометричних даних.

2. **Прозорість:** Організації повинні забезпечувати прозорість у використанні, зборі та зберіганні біометричних даних, надаючи чітку інформацію про ці процеси.

3. **Контроль користувачів:** Користувачі повинні мати активний контроль над своїми біометричними даними, зокрема можливість видалення або зміни цих даних за власним бажанням.

Біометричні технології, незважаючи на свої переваги, вимагають обачливого підходу до конфіденційності. Організації повинні дотримуватися рекомендацій, щоб забезпечити безпеку біометричних даних та зберігати прозорість у своїй діяльності.

#### 2.4. Вплив соціальної інженерії на психологію користувачів та їх поведінку

Соціальні інженери використовують підробку, обман і шантаж для змушення жертв до виконання їхніх вимог. Їхні методи впливають на психологію користувачів, спричиняючи емоції, такі як довіра, страх і емоційність.

1. Довіра: зловмисники можуть представлятися як представники надійних організацій, таких як банки або урядові установи, використовуючи цей підхід для отримання конфіденційної інформації.

2. Страх: Заяви про кримінальні злочини або загрози оприлюднення даних можуть використовуватися соціальними інженерами для змушення жертв до виконання їхніх вимог.

3. Інші емоції: Соціальні інженери можуть використовувати жадібність або гордість, наприклад, пропонуючи вигідні угоди або високо оцінюючи жертву, щоб отримати від неї бажаний результат.

Вплив соціальної інженерії може бути серйозним, оскільки зловмисники можуть отримати конфіденційну інформацію, завдати шкоди системам або впровадити шкідливе програмне забезпечення.

##### 2.4.1 Роль психології користувачів у схильності до соціальної інженерії

Однією з ключових причин, чому соціальна інженерія може бути успішною, є людська природа і її вразливість до маніпуляцій та впливу. Зловмисники використовують знання про психологічні особливості користувачів для створення ситуацій, в яких люди можуть бути схильні розкрити конфіденційну інформацію або виконати небезпечні дії.

Одним з методів соціальної інженерії є фішинг – відправка електронних листів або повідомлень, які виглядають як легітимні, з метою отримати від

користувача конфіденційну інформацію, таку як паролі або номери кредитних карток. Знання про психологію користувачів допомагає зловмисникам створювати переконливі історії та сценарії, які змушують людей реагувати і діяти необдуманно [18].

Більшість людей мають природний інстинкт довіри та бажання допомогти іншим. Це може бути використано зловмисниками, які можуть видаватися за довірену особу або авторитетну організацію, щоб отримати доступ до конфіденційних даних. Знання про психологію користувачів допомагає зловмисникам створювати ситуації, в яких люди відчуються зобов'язаними виконати прохання або надати інформацію. Однак, важливо пам'ятати, що психологія користувачів також може бути використана для запобігання соціальній інженерії. Налагодження свідомості та освіта щодо методів атаки можуть допомогти користувачам розпізнавати підозрілі ситуації та уникати небезпеки.

Отже, роль психології користувачів у схильності до соціальної інженерії не може бути недооцінена. Розуміння психологічних механізмів, які використовуються зловмисниками, може допомогти забезпечити більшу свідомість та захист користувачів від цього виду атак.

#### 2.4.2 Способи навчання та підвищення обізнаності користувачів для захисту від соціально-інженерних атак

Навчання та підвищення обізнаності користувачів визнані як один із найефективніших та ключових способів захисту від соціально-інженерних атак. Завдяки правильній освіті, користувачі отримують інструменти та знання, які дозволяють їм бути більш освідомленими та обізнаними щодо потенційних загроз. Коли користувачі мають достатні знання про різні методи соціально-інженерних атак, вони стають більш схильними розпізнавати підступні сценарії та вчасно реагувати на потенційні небезпеки. Важливо, щоб навчання було комплексним та охоплювало різні аспекти соціально-інженерних атак, включаючи фішинг, обман, імперсонація та інші тактики, які можуть використовуватися

зловмисниками. Існує безліч способів навчання та підвищення обізнаності користувачів про соціально-інженерні атаки.

Онлайн-курси та тренінги. Онлайн-курси та тренінги є хорошим способом навчити користувачів про різні методи соціально-інженерних атак. Ці курси та тренінги часто включають практичні вправи, які допомагають користувачам розвинути навички розпізнавання та протидії соціально-інженерним атакам.

1. Посібники та інформаційні матеріали: Посібники та інформаційні матеріали можуть бути корисним способом навчити користувачів про соціально-інженерні атаки. Ці матеріали часто включають інформацію про те, як розпізнавати та протистояти різним методам соціально-інженерних атак.

2. Відео та презентації: Відео та презентації можуть бути ефективним способом навчання користувачів про соціально-інженерні атаки. Ці матеріали часто включають інтерактивні елементи, які допомагають користувачам краще зрозуміти різні методи соціально-інженерних атак.

3. Програми навчання та підвищення обізнаності на робочому місці: Багато організацій пропонують програми навчання та підвищення обізнаності на робочому місці, які охоплюють питання захисту від соціально-інженерних атак. Ці програми часто включають практичні вправи та навчання, які допомагають користувачам розвинути навички розпізнавання та протидії соціально-інженерним атакам.

## Висновок до розділу 2

У другому розділі наголошено на ролі нормативно-правової бази у сфері кібербезпеки, яка виконує низку важливих та ключових функцій, спрямованих на забезпечення ефективного контролю та протидії сучасним кіберзагрозам. Закцентовано увагу на необхідності її удосконалення.

Детально проаналізовано методи ідентифікації та аутентифікації користувачів в інформаційних системах для захисту від атак соціальної інженерії.

Зокрема, розглянуто поняття ідентифікації та автентифікації, їх відмінності та важливість на кожному етапі. Описано популярні методи парольної ідентифікації та обмеження. Детально проаналізовано переваги, сценарії застосування та рекомендації щодо використання двофакторної аутентифікації.

Також досліджено можливості застосування біометричних технологій для ідентифікації користувачів. Наведено огляд основних біометричних методів та порівняльний аналіз їх переваг і недоліків. Розглянуто виклики та питання конфіденційності при роботі з біометричними даними.

Окремий підрозділ присвячено впливу соціальної інженерії на психологію користувачів, проаналізовано методи маніпулювання та шляхи підвищення обізнаності для протидії атакам.

## РОЗДІЛ 3. ПРАКТИЧНЕ ЗАСТОСУВАННЯ МЕТОДІВ ЗАХИСТУ ВІД АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

### 3.1 Аналіз інцидентів соціальної інженерії

Найбільш небезпечним елементом у системах комп'ютерної безпеки виявляється не апаратне чи програмне забезпечення, а користувачі. Про це добре обізнані найвидатніші хакери та експерти з кібербезпеки. Соціальна інженерія представляє собою процес маніпулювання людьми чи конкретною особою з метою отримання доступу до конфіденційної інформації або розголошення цієї інформації. Цей метод ґрунтується на використанні людських слабкостей і вважається надзвичайно руйнівним.

Соціальна інженерія розвивається як окрема галузь прикладної психології і є предметом навчання для шпигунів і таємних агентів. Всі техніки соціальної інженерії базуються на особливостях прийняття рішень людьми, які відомі як когнітивні спотворення. Ці хитрощі використовуються в різних комбінаціях для створення оптимальної стратегії обману в кожному конкретному випадку.

Навіть не дивлячись на те, що поняття соціальної інженерії недавно з'явилося, люди використовували її техніки у різних формах здавна. В давній Греції та Римі цінувалися особи, які вміли різними способами переконати співрозмовника в його "неправоті". Вони, виступаючи від імені верхів, проводили дипломатичні переговори, часто вдаючись до брехні та вигадкування аргументів для вирішення проблем, які не могли б бути вирішені інакше, крім застосування сили. У світі розвідки соціальна інженерія завжди була ключовою зброєю. Агенти ЦРУ, видаючи себе за інших, здатні були отримувати доступ до цілком таємних державних таємниць.

Обман людей по телефону для отримання інформації або виклику до певних дій вважалося справжнім мистецтвом. Фахівці в цій галузі можуть, навіть за допомогою загальних запитань або інтонації голосу, визначити комплекси та

страхи людини, використовуючи їх на свою користь.

Багато інформаційних технологів приділяють увагу неправильному уявленню, що їх дані можна достатньо захистити, використовуючи лише стандартні технічні заходи безпеки: системи виявлення вторгнень, міжмережні екрани, засоби аутентифікації тощо. Важливо розуміти, що безпека – це не лише технічна проблема, але й проблема, пов'язана з людьми та управлінням [10].

Окрім технічних методів захисту інформації, важлива також робота з персоналом, навчання співробітників застосуванню політики безпеки та методів протидії соціальним інженерам. Лише в цьому випадку система забезпечення інформаційної безпеки матиме повноцінне значення.

На рисунку 3.1 показані основні області застосування соціальної інженерії.

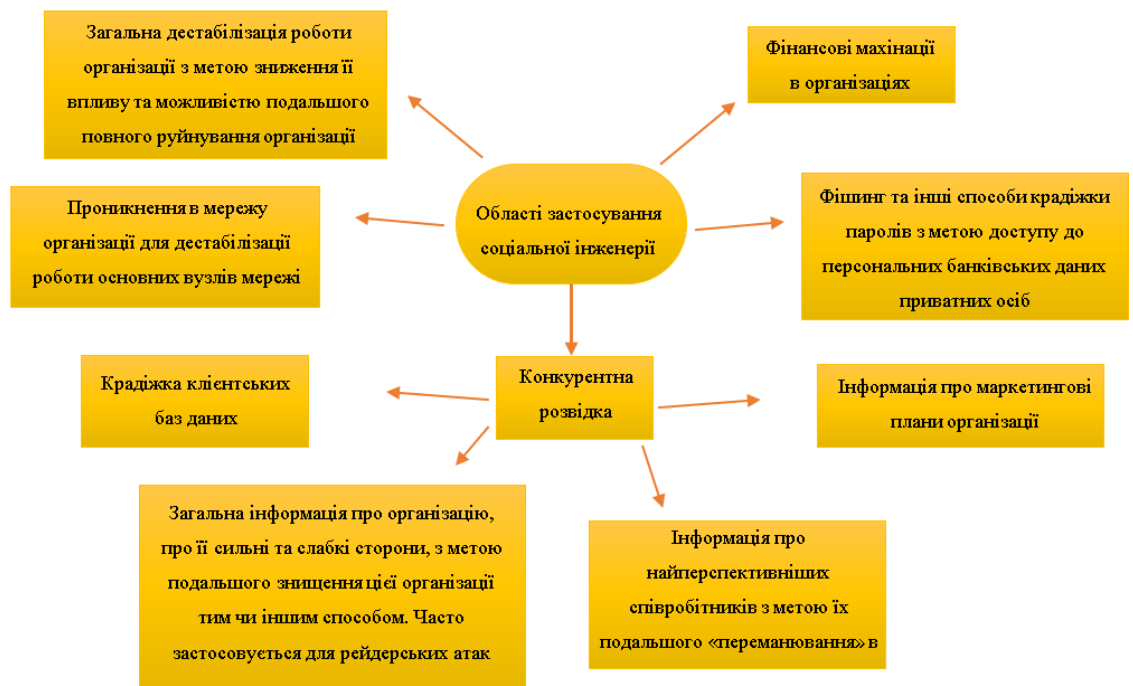


Рисунок 3.1 – Області застосування соціальної інженерії

Соціальна інженерія використовується з метою досягнення наступних цілей:

1. Збір інформації про потенційну жертву:
  - Спрямовано на отримання детальної інформації про потенційну жертву.
2. Отримання конфіденційної інформації:
  - Шляхом спілкування з жертвою соціальний інженер завойовує довіру

та отримує конфіденційну інформацію.

3. Отримання інформації для несанкціонованого доступу:

- Направлено на збір інформації, необхідної для отримання несанкціонованого доступу до систем чи даних.

4. Вимушення об'єкта вчинити необхідні дії:

- Ціль – змусити об'єкт (жертву) вчинити дії, які можуть становити потенційну небезпеку для інформаційної безпеки.

Переважає більшість соціальних інженерів використовує схожі шаблони дій, що дозволяє виявити основні етапи їх атак. Спочатку визначається мета атаки на конкретний об'єкт, тобто жертву. Потім здійснюється збір інформації про об'єкт для визначення найефективніших точок впливу. Після цього настає етап атракції, коли створюються умови для впливу на об'єкт. Важливим є етап примусу, коли здійснюється вимушення об'єкта вчинити необхідні дії, часто використовуючи раніше зібрану інформацію та здобуту довіру.

У світі інформаційних технологій соціальна інженерія успішно використовується кіберзлочинцями, такими як хакери, фішери, спамери і т.д. Вони активно атакують "людський фактор" через інтернет-технології, такі як блоги, соціальні мережі та електронна пошта, не вступаючи у фізичний контакт із своєю жертвою. Зазвичай, метою їхніх атак є викрадення інформації у її носія.

Основні методи цих атак включають:

1. Претекстинг. Вивчена дія за наперед визначеним сценарієм або "претекстом", часто використовується через телефон. Вимагає попередніх досліджень та персоналізації для забезпечення довіри цілі, наприклад, дзвінок від імені адміністратора, який просить повідомити пароль.

2. Фішинг. Досягається через масові розсилки електронних листів від імені популярних брендів або сервісів. Лист містить посилання на фальшиву веб-сторінку для введення конфіденційної інформації.

3. Вішинг (голосовий фішинг). Використовує попередньо записані голосові повідомлення для відтворення офіційних дзвінків від банківських або інших IVR систем.

4. Фармінг. Перенаправлення жертви на хибну інтернет-адресу, часто за допомогою навігаційних змін у файлі "hosts" або системі доменних імен.

5. HDoS (Людська відмова в обслуговуванні). Створення видимості виконання операції для відволікання уваги, прикриваючи інші дії.

6. "Людський фактор" та електронна пошта. Використання електронної пошти для імітації повідомлень від знайомих та фальсифікації адрес відправників.

7. Збір інформації із відкритих джерел. Використання соціальних мереж та інших відкритих джерел для збору інформації про потенційну жертву.

8. Багатоетапні атаки соціальної інженерії. Включають ретельно планований ряд кроків, комбінуючи маніпуляції та технологічні знання, для досягнення мети через просту пряму атаку або складні методи, використовуючи залякування, переконання або використання довірчих відносин [1].

Використовуючи соціальну інженерію, можна не лише витягти інформацію від жертви, але й безпосередньо встановити на її комп'ютер спеціальні програмні засоби, такі як закладки, які автоматично виконують необхідні завдання. Для впровадження таких засобів використовуються наступні методи:

1. Троянський кінь: Цей метод використовує цікавість або жадібність цільової особи. Троянські програми розповсюджуються через відкриті ресурси, носії інформації або служби обміну повідомленнями. Користувач, відкривши прикріплений файл, несвідомо запускає шкідливе програмне забезпечення.

2. Дорожнє яблуко: Цей вид атаки є модифікацією троянського коня та використовує фізичні носії. Зловмисник залишає "інфіковані" носії інформації в публічних місцях, приваблюючи увагу співробітників. Наприклад, диск із корпоративним логотипом може містити шкідливі дані.

3. Телефонний злом: Зловмисник, виглядаючи як технічна підтримка, телефонує в компанію, викликаючи ситуацію аудиту. Використовуючи соціальні інженерні методи, він отримує доступ до систем, вводячи команди під час вирішення хмарних "проблем".

### 3.2 Огляд сучасних інструментів та технологій соціальної інженерії

XXI століття відзначається процвітанням кіберзлочинів. Якщо на початку століття успіх зловмисників часто залежав від наявності серйозних вразливостей у програмному забезпеченні та недоліків у протоколах безпеки, то в кінці другої декади сцена кіберзлочинності вражає своєю еволюцією. Це стало можливим завдяки створенню міжнародних співтовариств професіоналів в галузі інформаційної безпеки (тут і далі – ІБ), визначенню галузевих стандартів (наприклад, сімейства ISO 27001) та впровадженню сертифікаційних процедур. Одночасно із розвитком технічних засобів протидії загрозам спостерігається зменшення відносної частки "технічних" атак.

Зараз відзначається стабільне зростання абсолютної кількості проблем в області ІБ. Це відбувається внаслідок того, що зловмисники змінили свій фокус, звертаючи увагу з технічних аспектів на людину, яка є найбільш слабкою ланкою в сучасних ІТ-системах. На відміну від роботів та алгоритмів, живий оператор ІТ-системи стає об'єктом атак, використовуючи соціальну інженерію – сукупність психологічних та соціологічних прийомів, методів та технологій, які дозволяють зловмисникам досягати своїх цілей.

Зловмисницькі цілі можна узагальнити та впорядкувати за ступенем небезпеки для жертви та оточуючих. Більш детальну класифікацію (відповідно до статей Кримінального кодексу) можна отримати від юристів, що спеціалізуються на кримінальному праві.

1. Розіграш, жарт чи хуліганство.
2. Дискредитація (мета публічного приниження жертви).
3. Крадіжка грошей чи інших матеріальних цінностей.
4. Крадіжка особистих даних жертви.
5. Крадіжка іншої інформації, включаючи конфіденційну (наприклад, ноу-хау компанії, корпоративні облікові записи, державні таємниці тощо).

Зазвичай у двох останніх випадках крадіжка даних є лише початковим етапом повного вектора атаки, мета якої може включати завдання шкоди конкретній людині, включаючи вчинення протиправних дій від її імені, або отримання несанкціонованого доступу до корпоративних комп'ютерних мереж та програмного забезпечення.

Часто зловмисники використовують людські слабкості або негативні риси характеру, такі як жадібність, бажання отримати щось безкоштовно ("на халяву"), страх (за себе або своїх близьких), неуважність та надмірну довірливість. Ключовим завданням соціального інженера є атака на підсвідомість, тимчасове переведення жертви в стан, де вона не може раціонально мислити, розкриваючи широкі можливості для атаки. Згідно з Microsoft Digital Defense Report за 2022 рік, для сучасного зловмисника в середньому потрібно приблизно 80 хвилин, щоб отримати доступ до облікових записів жертви соціальної інженерії, використовуючи підроблений сайт для крадіжки паролів, та близько 100 хвилин, щоб почати просування по корпоративній мережі з отриманими обліковими даними.

Отже, якщо зустріч з методами соціальної інженерії – це лише питання часу, важливо дотримуватися певних правил для визначення підозрілих повідомлень:

1. Використовувати офіційні канали зв'язку
  - а. Пам'ятати про офіційні канали зв'язку всередині та поза організацією.
  - б. Критично ставитися до будь-якого повідомлення, отриманого через не офіційний канал.
2. Перевірка автентичності
  - а. Якщо є сумніви у вірогідності отриманого повідомлення, зв'язатися з відправником через інший довірений канал для перевірки.
3. Червоні прапорці підозри
  - а. Повідомлення, що спрямовані на емоційне впливання (зокрема, загрози).
  - б. Попередження від поштового клієнта або месенджера про ненадійність відправника.

- с. Орфографічні та граматичні помилки.
- d. Неправильний домен електронної пошти.
- е. Незвичайний формат підпису.

#### 4. Запит на конфіденційну інформацію

а. Бути обережним, якщо повідомлення запитує конфіденційні дані чи гроші.

б. У разі загроз негативними наслідками за відмову потрібно бути особливо обачними.

#### 5. Посилання та вкладення:

а. Перед відкриттям посилань, навести курсор мишки, щоб побачити справжню адресу.

б. Використовувати антивірусне програмне забезпечення для перевірки вкладень.

с. Уникати автоматичного переходу за посиланнями у QR-кодах.

#### 6. Повідомлення про підозру:

а. У випадку сумнівів повідомляти про підозрілі комунікації в ІБ в організації або провайдеру електронної пошти/месенджера.

Велика кількість експертів в галузі інформаційної безпеки стверджують, що не існує єдиного методу, який гарантовано запобігав би соціальній інженерії на 100%. Тому ключовим є комплексний та багатоканальний підхід, спрямований на потенційних жертв за допомогою різних способів. Треба також усвідомити, що атакуюча сторона завжди шукає нові техніки атаки, непомітні раніше, тому жертва може зіткнутися з новими загрозами, які раніше їй не були відомі.

Практично всі методи протидії соціальній інженерії, які розглядаються далі, застосовуються ефективно як у сфері захисту особистих даних та домашніх комп'ютерів, так і в сфері захисту корпоративних і державних мереж та систем зберігання даних. З метою класифікації розглянуто симетричні методи, пов'язані з аналізом підозрілих повідомлень, та асиметричні, які дозволяють знизити ризик успішної атаки, не впливаючи безпосередньо на джерела проблем.

Розглянемо спочатку асиметричні методи, які є найбільш ефективними економічно та забезпечують максимальне зниження ризику успішної атаки за мінімальні витрати на їх впровадження:

- Використання двофакторної автентифікації:
  - Для ключових облікових записів, таких як соціальні мережі та особиста та корпоративна електронна пошта.
  - Рекомендується уникати використання SMS-кодів та переходити на апаратні брелки чи генератори одноразових кодів, наприклад, Yubikey.
- Використання спеціалізованого програмного забезпечення для зберігання паролів:
  - Дозволяє мати унікальні паролі для кожного веб-ресурсу та уникнути повторного використання паролів.
  - Менеджери паролів спрощують заміну паролів у випадку успішної атаки.

Більшість прямих методів протидії базуються на підвищенні уваги потенційних жертв та їх постійному тренуванні на реальних прикладах, а також на технічних заходах захисту. Доброю аналогією прямих методів є заходи, вживані медичними працівниками для запобігання великим епідеміям та пандеміям:

- Ознайомлення користувачів із загрозами соціальної інженерії та протидії атакам:
  - Застосовується як для користувачів, які вже зіштовхнулись з атаками соціальної інженерії, так і для тих, хто ще не був атакований методом соціальної інженерії.
- Випуск інформаційних стендів із інформацією про загрози соціальної інженерії:
  - Нагадує про загрози та заходи для запобігання, подібно до практики банків.
- Тестування стійкості працівників підприємств до соціальної інженерії:

- Включає в себе метрики, такі як відсоток відкритих листів, відсоток провалених тестів та відсоток повідомлень про атаку.
- Використання технічних засобів захисту:
  - Системи захисту електронної пошти, антивірусне програмне забезпечення, брандмауери нового покоління та інші.
  - Використання «чорних списків» та репутаційних оцінок ресурсів для блокування небезпечних адрес.

Ці заходи допомагають зменшити ризик соціальної інженерії, забезпечуючи багатоканальний та системний підхід до захисту.

### 3.3 Розробка та реалізація стратегій захисту в інформаційних системах

Для розробки ефективної методики навчання персоналу важливо розглядати вразливість людей до атак і вивчати методи маніпуляцій, що використовуються соціальними інженерами. Роберт Чалдіні визначив ключові риси маніпуляцій, які успішно використовуються:

1. Авторитетність:
  - люди бажають служити особі з авторитетом.
2. Уміння розташувати до себе:
  - люди відповідають на запити осіб зі схожими інтересами або проблемами.
3. Взаємність:
  - Отримання відповіді на подарунок чи послугу є ефективним способом впливу.
4. Відповідальність:
  - люди тенденційно дотримуються обіцянок.
5. Соціальна приналежність до авторизованих користувачів:
  - довіра людей особам, які належать до їхньої соціальної групи.

Ці методи маніпуляції є основою для успішних соціально-інженерних атак, і наведені приклади ілюструють їх використання в реальних ситуаціях.

У сучасних умовах практично будь-яка діяльність співробітників пов'язана з обробкою інформації. Тому політика безпеки організації повинна охоплювати всю компанію, незалежно від посади співробітників.

Організація повинна не лише встановлювати чіткі правила політики безпеки, але й стимулювати співробітників, активно ознайомлюватися та дотримуватися цих правил. Більше того, важливо переконатися, що всі працівники організації розуміють мотивацію застосування конкретних положень у правилах, щоб вони не намагалися обійти ці правила задля особистої вигоди.

Правила безпеки мають бути реалістичними, уникати надмірно складних вимог, які ймовірно будуть ігноровані працівниками. Також, програма навчання з безпеки повинна переконати співробітників, що виконання робочих завдань швидко не повинно ігнорувати систему безпеки, оскільки це може стати шкідливим для самої організації та її працівників.

Навіть після вивчення всіх документів і участі в навчальних програмах, багато працівників, ймовірно, не змінять свою щоденну поведінку. Для досягнення цього мети важливо забезпечити належне підкріплення, яке може бути подано у двох формах: негативному та позитивному.

Негативне підкріплення передбачає покарання за порушення заходів безпеки (наприклад, якщо під час перевірки виявлено, що працівник прикріпив лист з паролем до монітора, йому слід отримати догану).

Інший спосіб забезпечити увагу до питань безпеки – включити їх у щорічний звіт про роботу кожного працівника, викликаючи розуміння їх важливості та відповідальності за безпеку. Використання негативного підкріплення може служити запобіганням серйозним порушенням.

Організація може вважати, що досягнуті цілі, якщо всі працівники будуть усвідомлювати, що захист інформації – це невід'ємна частина їхніх обов'язків. Співробітники повинні повністю розуміти, що соціальні інженери проводять реальні атаки, а втрата оброблюваної інформації загрожує не лише організації, але і кожному співробітникові особисто, його роботі та добробуту [1].

В основі навчального тренінгу має бути структура, яку відвідували б всі співробітники. Новоприйняті працівники повинні проходити тренінг, як частину свого вступу і ознайомлення з новою роботою. Рекомендується взагалі не допускати співробітників до роботи з комп'ютером, доки вони не пройдуть тренінг із засвоєння основ інформаційної безпеки.

Перше заняття має бути приурочене до екстрених ситуацій і систем оповіщення. Знайомство з короткими важливими повідомленнями сприятиме кращому розумінню матеріалу співробітниками.

Особливий акцент у першому занятті слід робити на гармонії, яка встановлюється в організації після впровадження цієї програми. Більш важливою за навчання є мотивація, яка повинна стимулювати співробітників брати персональну відповідальність за безпеку.

Системні інструменти охоплюють програми, спрямовані на визначення користувачів, управління доступом, шифрування інформації, очищення робочої інформації, тестування ефективності системи захисту і багато іншого.

Комбіновані апаратно-програмні рішення виконують завдання, які включають як апаратні, так і програмні компоненти, поєднуючи їхні характеристики.

Організаційні засоби включають організаційно-технічні та організаційно-правові заходи. Переваги організаційних засобів включають рішення різноманітних проблем, простоту в реалізації та швидку реакцію на небажані дії в мережі.

Технічні засоби захисту включають в себе, наприклад, міжмережні екрани, системи шифрування, проксі-сервери, системи контролю доступу (СКУД) та системи охорони та сигналізації. Прикладом комплексного антивірусу є Panda Internet Security, який використовує Firewall, хмарні технології та проактивний захист. Цей продукт має інструменти для захисту від шкідливих і фішингових веб-сайтів, а також для забезпечення безпеки персональних даних та онлайн резервного копіювання.

Основні характеристики Panda Internet Security включають:

- Антивірус для захисту від всіх типів вірусів, черв'яків і троянів.
- Технологію TruPrevent для блокування невідомих вірусів та аналізу їхньої поведінки.
- Антишпигун / Анти-adware для захисту від шпигунів і рекламного ПЗ.
- Захист від онлайн-шахрайства (антифішинг) для безпеки роботи з онлайн-банками і магазинами.
- Firewall для захисту від проникнення хакерів.
- Блокування підозрілих веб-сторінок для запобігання доступу до веб-сторінок із небезпечними скриптами.
- Виявлення загроз в Wi-Fi мережах для забезпечення безпеки бездротових з'єднань.
- Захист особистих даних і контроль приватності для безпеки персональних даних та захисту від онлайн-крадіжок.
- Антиспам для блокування небажаної пошти.
- Віртуальну клавіатуру для безпечного введення паролів.
- Менеджер домашньої мережі для перевірки статусу безпеки домашніх комп'ютерів.
- Онлайн-резервування для доступу до даних з будь-якого місця з виділеним простором об'ємом 2 ГБ.
- Віддалений доступ до ПК для забезпечення доступу до домашнього або офісного комп'ютера.
- Шифрування файлів.
- Знищення файлів для остаточного видалення непотрібних файлів.



Рисунок 3.2 – Робота Panda Internet Security

Отже, Panda Internet Security виявляється оптимальним вибором для організації, оскільки цей продукт надійно захищає робочі станції від різних мережесих атак, таких як фішинг, спам, реклама та банери. З точки зору ціноутворення та функціональності, це є найбільш оптимальним варіантом. Встановлення даного продукту на кожному робочому місці може істотно зменшити кількість інтернет-атак.

Для створення методики протидії загрозам, пов'язаним з використанням соціальної інженерії, необхідно виконати три дії. Важливо пам'ятати, що ефективність захисту визначається під час планування:

1. Розробити стратегії управління забезпеченням безпеки, визначивши завдання захисту від загроз соціальної інженерії та призначивши відповідальних співробітників.
2. Провести оцінку ризиків, аналізуючи кожен загрозу та визначаючи її потенційну небезпеку та можливі збитки для організації.
3. Ввести принципи захисту від атак соціальних інженерів в політику безпеки організації, розробивши процедури для дій співробітників у ситуаціях, які можуть бути об'єктом атак соціальних інженерів.

Стратегія управління забезпеченням безпеки створює загальне уявлення про загрози соціальної інженерії, якими може бути вражена організація. Основні співробітники, які відповідають за розробку політик і процедур для протидії цим загрозам, включають:

1. Куратор з безпеки. Відповідальний за те, щоб усі співробітники ставилися серйозно до забезпечення безпеки і мав необхідний авторитет для цього.

2. Адміністратор з безпеки. Відповідає за організацію розробки політик безпеки та їх оновлення відповідно до змін вимог.

3. Адміністратор по інформуванню. Керівний співробітник, який відповідає за розробку та проведення кампаній з інформування співробітників про загрози та методи їх відвертання.

Ці співробітники, виконуючи вказані ролі, формують керівний комітет із забезпечення безпеки, який визначає основні цілі стратегії управління забезпеченням безпеки. Визначення цілей є критичним для залучення інших співробітників до участі в проектах забезпечення безпеки та оцінки їх результатів. Першим завданням керівного комітету у сфері забезпечення безпеки є виявлення вразливостей в корпоративному середовищі, які можуть бути використані соціальними інженерами для атак. При розробці заходів забезпечення безпеки завжди необхідно оцінювати рівень ризику, що може виникнути при різних типах атак на організацію. З використанням інформації про ключові елементи стратегії управління забезпеченням безпеки, були визначені та групувані фактори ризику. Далі подано перелік категорій ризику: витік інформації (ВІ), збиток репутації організації (ЗРО), зниження працездатності організації (ЗПО), втрата ресурсів (ВР), фінансові втрати (ФВ).

При реєстрації інциденту важливо визначити, чи є він новою чи зміненою загрозою для організації. На основі отриманих висновків слід створити або оновити політики і процедури. Для управління інцидентами використовується протокол, в якому реєструється така інформація:

1. Жертва атаки;

2. Дата;
3. Напрямок атаки;
4. Опис атаки;
5. Результат атаки;
6. Наслідки атаки;
7. Подальші рекомендації.

Реєстрація інцидентів дозволяє виявляти шаблони атак і вдосконалювати захист від майбутніх нападів.

При повному аналізі організації виявлено такі фактори, що роблять її вразливою до атак:

1. Збільшена кількість співробітників створює можливість для соціального інженера провести атаку, представившись керівником або представником головного центру.

2. Відсутність документів, які регламентують політики та правила безпеки, а також відсутність повного навчання співробітників цим правилам, сприяє соціальному інженеру, оскільки співробітники не навчені, як вести себе в різних ситуаціях, що надає інженеру можливість маніпулювати ними без зусиль.

3. Документи, які не повинні бути загальнодоступними, але є комерційною таємницею, можуть бути переплутані, втрачені або вилучені відвідувачами.

4. Відсутність повідомлень від співробітників про інциденти, що стосуються оброблюваної інформації, дозволяє соціальному інженеру використовувати атаку знову і знову, надіючись на те, що інші співробітники не будуть проінформовані про події.

5. Використання особистих поштових скриньок на робочому місці створює уразливості в комп'ютерних мережах організацій, оскільки відсутні перевірки вхідних листів та недбалість працівників.

Для подальшого виявлення вразливостей необхідно визначити працівників, які є основними об'єктами атак соціальних інженерів. У першу чергу, до них відносяться:

- Секретар в приймальній, який, завойовуючи довіру, може дозволити соціальному інженеру отримати телефони інших співробітників.
- Співробітник, що працює з клієнтами, який, представляючи інтереси клієнта, може здобути інформацію про відповідну організацію.
- Телефонні довідники, які надають можливість знаходження необхідних номерів та отримання уявлення про структуру організації, включаючи точні назви відділів та посади.

Після виявлення вразливостей прийнято рішення щодо їх усунення. Серед заходів, які були впроваджені в організації, варто відзначити:

1. Розробка політик безпеки та процедур
  - a. Розроблено політику безпеки інформації, яка визначає секретну інформацію організації та способи її захисту, охоплюючи як паперові, так і електронні носії.
  - b. Визначена політика використання комп'ютерів, яка регулює доступ та використання комп'ютерних систем, забороняючи несанкціоноване підключення до внутрішніх систем через зовнішні джерела.
  - c. Визначена політика ідентифікації і аутентифікації, включаючи мінімальні вимоги до паролів та інші характеристики вибору пароля.
  - d. Розроблена політика управління доступом, яка встановлює вимоги до управління доступом до електронних файлів, гарантуючи авторизованим користувачам відповідний доступ.
2. Розробка переліків комерційної таємниці
  - a. Створено переліки інформації, що становить комерційну таємницю, забезпечуючи її адекватний захист.
3. Надання методичного матеріалу інструкцій та політик безпеки:
  - a. Усі співробітники були ознайомлені з політиками безпеки, пройшли інструктажі та курси з протидії соціальному інжинірингу.
4. Розсилка інформаційних матеріалів та нагадувань

а. Через електронну пошту, локальну мережу та особистий контакт співробітникам постійно розсилалися оновлені інформаційні матеріали та нагадування з питань безпеки.

5. Публікація найбільш надійного працівника місяця

а. Запроваджено заходи щодо визначення та нагородження співробітників, які виявилися найбільш відповідальними та вірними політикам безпеки.

6. Створення зберігачів екрану та екранних заставок

а. Розроблені екранні заставки, які регулярно надавали нагадування про можливі атаки соціальних інженерів.

7. Створення системних повідомлень в локальній мережі

а. Розроблена програма для локальної мережі, яка виводила спливаючі вікна з нагадуваннями для співробітників.

8. Створення єдиного поштового клієнт-сервера

а. Створено єдиний поштовий клієнт-сервер для контролю вхідної і вихідної пошти, зменшуючи ймовірність загрози, пов'язаної з електронною поштою.

9. Постійне обговорення питань безпеки

а. Забезпечено постійне обговорення питань безпеки на зборах та інших форумах для підтримання своєчасності та постійної уваги до цих питань.

У підсумку, організація виявила вразливості в своїй системі безпеки і успішно впровадила комплекс заходів для їх усунення та підвищення рівня безпеки. Серед цих заходів є розробка та впровадження політик безпеки і процедур, розробка переліків комерційної таємниці, інструктажі та навчання співробітників, а також постійна інформаційна робота, яка включала розсилку матеріалів, публікацію результатів та нагородження відповідальних працівників.

Також важливо відзначити використання технічних інструментів, таких як екранні заставки та системні повідомлення, які сприяли постійній увазі до питань безпеки. Створення єдиного поштового клієнт-сервера і контроль за вхідною та вихідною поштою також виявилися ефективними заходами для зменшення загрози, пов'язаної з електронною поштою.

Організація активно залучила співробітників до процесу змін у системі безпеки, створюючи культуру безпеки, що виявилось дієвим способом уникнення соціальної інженерії та інших загроз. Нагородження найбільш надійних працівників стало додатковим стимулом для всього колективу. Всі ці заходи допомогли підняти загальний рівень безпеки та стійкості організації до потенційних загроз.

### 3.4 Тестування та оцінка ефективності захисних заходів

Розглянемо техніку фішингу, яка імітує вікно веб-переглядача в браузері, щоб підробити законний домен.

Для фахівців із безпеки URL-адреса зазвичай є найбільш надійним аспектом домену. Так, існують такі атаки, як IDN Homograph і DNS Hijacking, які можуть знизити надійність URL-адрес, але не настільки, щоб зробити URL-адреси ненадійними.

Все це зрештою змушує задуматися, чи можна зробити пораду «Перевірте URL»? Розглянемо приклад атаки з підміною кнопки.

Досить часто, коли ми проходимо автентифікацію на веб-сайті через Google, Microsoft, Apple тощо, ми надаємо спливаюче вікно з проханням про автентифікацію. На зображенні нижче показано вікно, яке з'являється, коли хтось намагається увійти в Canva за допомогою свого облікового запису Google.

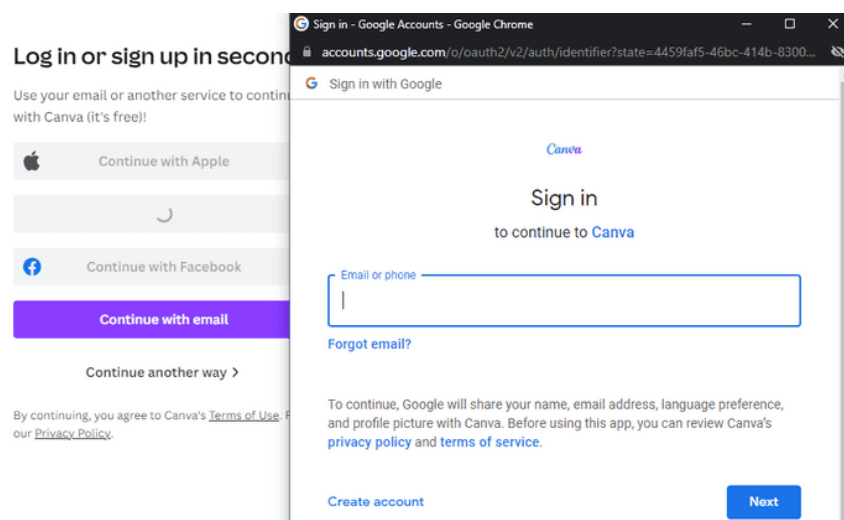


Рисунок 3.3 – Вхід в Canva за допомогою Google

Відтворимо дизайн вікна за допомогою HTML/CSS. Код вікна описано в додатку А.

Поєднаємо дизайн вікна з `iframe`, що вказує на шкідливий сервер, на якому розміщено фішингову сторінку, і його практично неможливо розрізнити. На зображенні нижче показано фальшиве вікно в порівнянні зі справжнім вікном. Дуже мало людей помітять невеликі відмінності між ними.

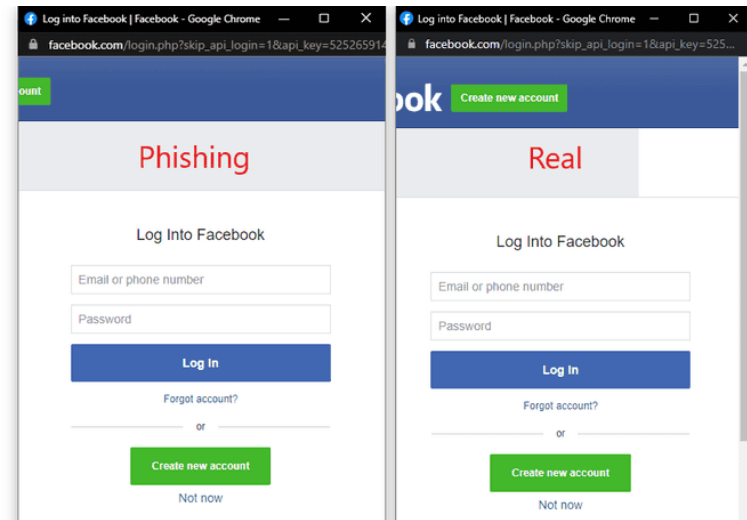


Рисунок 3.4 – Фальшиве вікно в порівнянні зі справжнім вікном

JavaScript можна легко використовувати, щоб вікно з'являлося під час натискання посилання чи кнопки, під час завантаження сторінки тощо. І, звичайно, можна зробити вікно привабливим за допомогою анімації, доступної в бібліотеках, таких як JQuery.

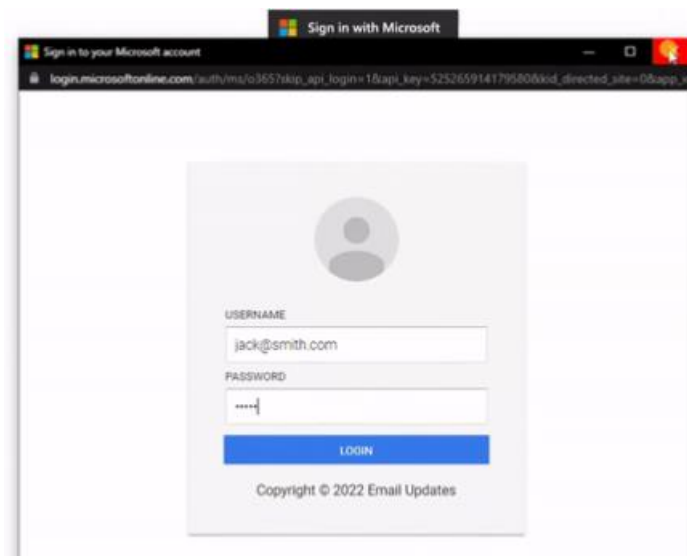


Рисунок 3.5 – Вигляд вікна після наведення та натискання фальш кнопки

Перевірка легітимності URL-адреси шляхом наведення курсора не є дуже ефективною, особливо якщо ввімкнено JavaScript. У загальному вигляді, HTML-код для посилань виглядає наступним чином:

```
<a href ="https://gmail.com"> Google</a>
```

Якщо додано подію onclick, яка повертає false, то при наведенні курсора на посилання веб-сайт продовжуватиме відображатися в атрибуті href , але коли натиснуто посилання, атрибут href ігноруватиметься. Можна використати ці знання, щоб зробити спливаюче вікно більш реалістичним.

```
<a href ="https://gmail.com" onclick="return launchWindow ();">
Google</a>
```

```
function launchWindow ( ){
// Запуск вікна підробленої автентифікації
return false; // Це гарантує, що атрибут href ігнорується
}
```

Отже, якщо стикаєтеся з фішинговими вікнами або атаками, рекомендується вжити наступних заходів

a. Не натискати на посилання та не відправляти конфіденційну інформацію. Уникати відкривання невідомих посилань чи вводу особистої інформації на сумнівних веб-сайтах.

b. Використовувати антивірусні програми та захисні розширення для браузера. Ці інструменти можуть блокувати або попереджати про потенційно шкідливі веб-сайти.

c. Оновлювати браузер та програми. Забезпечити, щоб браузер та всі встановлені програми вчасно оновлювались до останніх версій, оскільки це може допомогти усунути вразливості.

d. Навчитись розпізнавати фішингові атаки. Знаходити і навчати інших розпізнавати знаки фішингу, такі як посилання URL, невідомі відправники, тощо.

e. Повідомляти про атаку. Якщо зіштовхнулись з фішинговою атакою, повідомляти про це відповідні служби чи організації.

Насправді, взаємодіючи з подібними вікнами, просто потрібно бути обережними. Вони розраховані на людей, які поспішають. А так, як дана атака розрахована на на вхід в аккаунт, то ця дія загалом ніколи не викликає запитань. Що і є, по суті, проблематикою даної атаки, так як люди на автоматі вводять свої дані і вони залишаються в зловмисника. Однак від них є додатковий захист, це додаткова аутентифікація за допомогою простого e-mail або інших засобів.

### Висновок до розділу 3

У розділі розглянуто практичні аспекти застосування методів захисту від атак соціальної інженерії в інформаційних системах.

Зокрема, проаналізовано реальні інциденти соціальної інженерії, розглянуто сучасні інструменти та технології, які використовують зловмисники. Окрему увагу приділено розробці та реалізації конкретних стратегій захисту в організаціях, включаючи політики безпеки, навчання персоналу, моніторинг інцидентів тощо.

Важливим моментом є тестування та оцінка ефективності захисних заходів на конкретних прикладах атак, зокрема фішингу. Це дозволяє краще зрозуміти можливі слабкі місця та шляхи їх усунення.

Загалом, у розділі продемонстровано, що лише комплексне та системне застосування технічних і організаційних методів дає змогу забезпечити належний рівень захисту від загроз соціальної інженерії. При цьому "людський фактор" відіграє одну з ключових ролей.

## ВИСНОВКИ

Атаки соціальної інженерії залишаються одними з найбільш витончених та складних загроз, які супроводжують інформаційне суспільство сучасності. Цей вид кіберзагроз не лише еволюціонував, але й пройшов трансформацію від простих маніпуляцій до високотехнологічних кібератак, що створюють серйозні виклики для безпеки та конфіденційності інформації. Його вражаючий вплив захоплює увагу як вчених, так і практиків, викликаючи необхідність постійного вдосконалення захисних стратегій та поглибленого вивчення природи цієї складної кіберзагрози.

Однією з ключових концепцій, що вдалося висвітлити, є визначення та детальне розкриття основних рис атак соціальної інженерії, таких як фішинг, вішинг та персоніфікація. Аналіз історичного контексту не лише дозволяє визначити коріння цих атак, але й розкриває їхню постійну трансформацію та адаптацію до нових умов технологічного прогресу. Ця еволюція відбувається в контексті стрімкого розвитку сучасного інформаційного суспільства, що підкреслює потребу у постійному удосконаленні заходів забезпечення кібербезпеки та виявленні новітніх стратегій для взаємодії зі зростаючими загрозами соціальної інженерії.

Глибокий аналіз психологічних та соціальних аспектів атак, проведений у першому розділі роботи, викликає серйозні сумніви щодо стійкості багатьох користувачів перед маніпулятивними техніками соціальних хакерів. Робота виокремлює важливість урахування цих факторів при розробці стратегій захисту, які повинні бути адаптовані до психологічних особливостей та соціокультурного контексту користувачів. Об'єктивно визначаючи вплив соціальної інженерії на психологію користувачів, робота висвітлює необхідність систематичного підвищення рівня обізнаності та освіти серед них. Це вимагає не лише технічних заходів безпеки, але й розвитку ефективних програм навчання та інформаційних кампаній, спрямованих на формування у користувачів критичного мислення та вміння визнавати потенційні загрози в кіберпросторі.

У другому розділі наголошено на ролі нормативно-правової бази у сфері кібербезпеки, яка виконує низку важливих та ключових функцій, спрямованих на забезпечення ефективного контролю та протидії сучасним кіберзагрозам. Закцентовано увагу на необхідності її удосконалення.

Детально проаналізовано методи ідентифікації та аутентифікації користувачів, звернена увага на необхідність вдосконалення та розширення існуючих методик для захисту від атак соціальної інженерії. Висвітлено концепції ідентифікації та аутентифікації, наголошено на важливості двофакторної аутентифікації та використанні біометричних технологій.

Розділ, присвячений практичним аспектам застосування методів захисту від атак соціальної інженерії, розкриває реальні інциденти та аналізує використовувані зловмисниками інструменти та технології. Покладаючи основний акцент на розробку конкретних стратегій захисту в організаціях, включаючи політики безпеки, навчання персоналу та моніторинг інцидентів, робота висвітлює важливість тестування та оцінки ефективності захисних заходів.

Проаналізувавши виконану роботу можна зазначити, що дипломний проєкт глибоко досліджує та аналізує важливі аспекти захисту від атак соціальної інженерії, пропонуючи не лише конкретні рекомендації, але і системний погляд на їхні теоретичні та практичні виміри. Запропоновані стратегії захисту виокремлюються комплексним підходом, який охоплює як технічні, так і організаційні аспекти, і в центрі уваги стоїть роль "людського фактора".

Розглядаючи проблему безпеки в інформаційних системах як невід'ємну частину взаємодії технологій і людей, робота визначає важливість врахування психологічних та соціокультурних аспектів при розробці та впровадженні заходів забезпечення безпеки. Такий глибокий інтегрований підхід є ключем до успішного досягнення високого рівня захищеності інформаційних систем у сучасному кіберпросторі.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ : підручник / В. КОЗЮРА та ін. ; ред. В. Дудикевич. Чернігів : ТПК «Орхідея», 2020. 236 с.
2. Корченко О., Казмірчук С., Б.Б. Ахметов Б. ПРИКЛАДНІ СИСТЕМИ ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ : монографія. Київ : ЦП «Компринт», 2017. 435 с.
3. Савчук . Соціальна інженерія: як шахраї використовують людську психологію в інтернеті. Радіо Свобода. URL: <https://www.radiosvoboda.org/a/socialna-inzhenerija-shaxrajstvo/29460139.html> (дата звернення: 02.12.2023).
4. Cialdini R. B. Influence: The psychology of persuasion. New York, USA : Collins, 2007. 320 с.
5. Dark Reading | Security | Protect The Business. Dark Reading | Security | Protect The Business. URL: <https://www.darkreading.com/> (дата звернення: 02.12.2023).
6. Defending Against Ransomware in Industrial Control Systems | SANS Institute. Cyber Security Training | SANS Courses, Certifications & Research. URL: <https://www.sans.org/blog/defending-against-ransomware-industrial-control-systems/> (дата звернення: 02.12.2023).
7. Mitnick K. D., Simon W. L. The Art of Deception: Controlling the Human Element of Security. Wiley, 2003. 366 с.
8. The 15 Most Famous Social Engineering Attacks. phoenixNAP Blog. URL: <https://phoenixnap.com/blog/social-engineering-examples> (дата звернення: 02.12.2023).
9. The Social-Engineer Newsletter – Security Through Education. Security Through Education. URL: <https://www.social-engineer.org/newsletter/> (дата звернення: 02.12.2023).

10. Золотар О. ІНФОРМАЦІЙНА БЕЗПЕКА ЛЮДИНИ: ТЕОРІЯ І ПРАКТИКА : монографія. Київ : ТОВ «Вид. дім «АртЕк», 2018. 446 с.
11. Чубаєвський В. І. Корпоративна інформаційна безпека : монографія. Київ : Держ. торг.-екон. ун-т, 2022. 272 с.
12. Krutz R. L. The CISSP prep guide. Indianapolis, Ind : Wiley Pub., 2003. 944
13. Лісовська Ю. Кібербезпека: ризики та заходи : навч. посіб. Київ : Кондор, 2019. 272 с.
14. How cyber attacks work. NCSC. URL: <https://www.ncsc.gov.uk/information/how-cyber-attacks-work> (дата звернення: 02.12.2023).
15. Не вір нікому. Що таке соціальна інженерія та як не стати її жертвою | Київстар. Мобільний зв'язок від Київстар | Національний оператор мобільного зв'язку. URL: <https://kyivstar.ua/uk/cybersecurity/ne-vir-nikomu-shcho-take-socialna-inzheneriya-ta-yak-ne-statyi-yiyi-zhertvoyu> (дата звернення: 02.12.2023).
16. Плечовий серфінг – що це таке, способи захисту в громадських місцях. ESET. ESET. URL: <https://www.eset.com/ua/support/information/entsiklopediya-ugroz/plechevoy-serfing/> (дата звернення: 02.12.2023).
17. Програма-вимагач – що таке вірус-вимагач, як його видалити. ESET. ESET. URL: <https://www.eset.com/ua/support/information/entsiklopediya-ugroz/programma-vymogatel/> (дата звернення: 02.12.2023).
18. Соціальна інженерія – що це таке, атаки з використанням соціальної інженерії. ESET. ESET. URL: <https://www.eset.com/ua/support/information/entsiklopediya-ugroz/sotsialnaya-inzheneriya/> (дата звернення: 02.12.2023).
19. Троян – вірус, замаскований в програмному забезпеченні. ESET. ESET. URL: <https://www.eset.com/ua/support/information/entsiklopediya-ugroz/trojan/> (дата звернення: 02.12.2023).

20. Фішинг – що це таке і яка мета фішингу? Енциклопедія ESET. ESET. URL: <https://www.eset.com/ua/support/information/entsiklopediya-ugroz/fishing/> (дата звернення: 02.12.2023).

21. The Next-Gen Antivirus for Windows, Mac and Android – Panda Security. pandasecurity.com. URL: <https://www.pandasecurity.com/en/> (дата звернення: 02.12.2023).

# ДОДАТКИ

## ДОДАТОК А

```
<!DOCTYPE html>
<html>
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link rel="stylesheet" href="style.css">
  <script
src="https://ajax.googleapis.com/ajax/libs/jquery/3.5.1/jquery.min.js"></script
>
</head>
<body>
<div id="window">
<!-- Title bar start -->
<div id="title-bar-width">
  <div id="title-bar">
    <div style="margin-top:5px;">
      
      <span id="logo-description">XX-TITLE-XX</span>
    </div>
    <div>
      <span id="minimize">&#8212;</span>
      <span id="square">□</span>
      <span id="exit">X</span>
    </div>
  </div>
  <div id="url-bar">
    
    <span id="domain-name">XX-DOMAIN-NAME-XX</span>
    <span id="domain-path">XX-DOMAIN-PATH-XX</span>
  </div>
</div>
<!-- Content start -->
<iframe id="content" src="XX-PHISHING-LINK-XX" frameborder="0"></iframe>
</div>
</body>
<script src="script.js"></script>
</html>
```