МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

КВАЛІФІКАЦІЙНА РОБОТА

На тему « РОЗРОБКА МЕТОДІВ АТАКИ ТА ЗАХИСТУ ВІД МАНІПУЛЮВАННЯ ЛЮДЬМИ ДЛЯ ОТРИМАННЯ ДОСТУПУ ДО ІНФОРМАЦІЇ»

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека
освітньо-професійної програми Управління інформаційною безпекою

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

_____Олександр Фелісієнко
(підпис) Ім'я, ПРІЗВИЩЕ здобувача

Виконав: Здобувач вищої освіти гр.УБДМ 61
Олександр Фелісієнко

Керівник: к.в.н.,
доц. Якименко Юрій Михайлович

Рецензент:к.держ.упр.,доц. Мужанова Тетяна Михайлівна

Київ – 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра Управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти магістр

Спеціальність 125 Кібербезпека

Освітньо-професійна програма Управління інформаційною безпекою

"**ЗАТВЕРДЖУЮ**"
Завідувач кафедри УІКБ
_____ С.В.Легомінова

"___"_____2024 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту **Фелісієнку Олександру Олександровичу**

1. Тема кваліфікаційно їроботи: :"Розробка методів атаки та захисту від маніпулювання людьми для отримання доступу до інформації "

Керівник кваліфікаційної роботи Юрій Якименко, к.в.н.

затверджені наказом Державного університету інформаційно-комунікаційних технологій від"19"жовтня2023 р. №145

2. Строк подання кваліфікаційної роботи"18" грудня 2023 р

3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпекап, методи та засоби захисту від маніпулювання людьми для отримання доступу до інформації*

4.Перелік питань, які потрібно розробити:

4.1 Розглянути теоретико-методологічні засади дослідження маніпулювання людьми.

4.2 Проаналізувати методи атаки та захисту від маніпулювання людьми.

4.3 Провести дослідження і розробити рекомендації по захисту від маніпулювання людьми для отримання доступу до інформації.

4.4. Перелік ілюстративного матеріалу:*презентація*

5. **Дата видачі завдання «**2» жовтня 2023 р.

КАЛЕНДАРНИЙ ПЛАН
виконання кваліфікаційної роботи
студентом Фелісієнком Олександром Олександровичем
Дата видачі завдання: «26»вересня2023 р.

№ з/п	Етапи роботи	Термін виконанняетапів	Примітка
1.	Визначення об'єкту, предмету, мети та завдань дослідження.	26.09.2023	
2.	Збір та аналіз літератури.	3.10.2023	
3.	Розділ 1. Теоретико-методологічні засади дослідження маніпулювання людьми	17.10.2023	
4.	Розділ 2. Характеристика методів атаки та захистувід маніпулювання людьми	31.10.2023	
5.	Розділ 3. Розробка рекомендацій по захисту від маніпулювання людьми для отримання доступу до інформації	14.11.2023	
6.	Формулювання висновків за результатами проведеного дослідження	01.12.2023	
7.	Оформлення роботи	8.12.2023р.	
8.	Оформлення презентації	15.12.2023р.	
9.	Отримання рецензії на роботу .	23.12.2023	
10.	Захист в ДЕК	___01.2024 р.	

Студент О.О.Фелісієнко
(підпис)

Науковий керівник Ю.М. Якименко
(підпис)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДОЗАХИСТУ КВАЛІФІКАЦІЙНОЇРОБОТИ
На здобуття освітнього ступеня магістра

Направляється здобувач Фелісієнко О.О.до захисту кваліфікаційної роботи
(прізвищетаініціали)
За спеціальністю 125 Кібербезпека
(код,найменуванняспеціальності)
Освітньо-професійної програми Управління інформаційною безпекою
(назва)
на тему:“Розробка методів атаки та захисту від маніпулювання людьми для отримання доступу до інформації ”
Кваліфікаційна робота і рецензія додаються.

ДиректорННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім’я,ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач **Фелісієнко Олександр** у кваліфікаційній роботі дослідив методи атаки та захисту від маніпулювання людьми для отримання доступу до інформації , визначив основні проблеми та розробив пропозиції і рекомендації щодо запобіганням таким маніпуляціям. **Фелісієнко Олександр** показав розуміння проблеми дослідження та бачення основних теоретичних та практичних напрямів її вирішення, довів уміння самостійного застосування методів наукового дослідження, проявив себе як організований, відповідальний виконавець.

Це дозволяє оцінити виконану кваліфікаційну роботу здобувачу **Фелісієнко Олександра** на оцінку “_____”та присвоїти йому кваліфікацію “Магістр кібербезпеки за освітньо-професійною програмою “Управління інформаційною безпекою”.

Керівник кваліфікаційноїроботи_____ Ю.М. Якименко
(підпис) *(Ім’я,ПРІЗВИЩЕ)*

“___“_____2024 року

Висновок кафедри про кваліфікаційну роботу

Завідувачкафедри
Управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім’я,ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 80 стор., 12 рис., 1 табл., 62 джерел.

Метою роботи є дослідження розробка Методів атаки та захисту від маніпулювання людьми для отримання доступу до інформації. Об’єктом дослідження є процес маніпулювання людьми для отримання доступу до інформації.

Предмет дослідження - є методи атаки та захисту від маніпулювання людьми.

Короткий зміст роботи. Як результат у роботі проведено аналіз основних методів маніпулювання людьми основним з яких є соціальна інженерія. Такий вид кіберзлочинності, який що використовує різні психологічні,технічні способи для доступу до інформації. Описані правила доступу до інформації що зменшать можливість маніпулювання. Вони допомагають ідентифікувати та мінімізувати потенційні загрози, встановлюючи чіткі очікування та процедури для поводження з інформацією. Ці правила допомагають запобігти несанкціонованому доступу до інформації, що може бути використане для маніпулювання людьми.

Галузь застосування. Розроблені підходи можуть бути використані при плануванні та реалізації системи управління інформаційною безпекою підприємства та особистої інформаційної безпеки людини

КЛЮЧОВІ СЛОВА :СОЦІАЛЬНА ІНЖИНЕРІЯ,ІНФОРМАЦІЙНА БЕЗПЕКА,ЦИФРОВИЙ СЛІД,ІНФОРМАЦІЙНА ГІГІЄНА,МАНІПУЛЯЦІЯ.

ABSTRACT

The text part of the qualification work for obtaining an educational degree master's degree: 80 pages, 12 figures, 1 table, 62 sources.

The purpose of the work is to research and develop Methods of attack and protection against manipulation of people to gain access to information.

Object of research is the process of manipulating people to gain access to information.

Subject of research is methods of attack and protection against human manipulation.

Brief content ofresearch. As a result, the work analyzes the main methods of manipulating people, the main of which is social engineering. This type of cybercrime uses various psychological and technical methods to access information. The rules of access to information that will reduce the possibility of manipulation are described. They help identify and minimize potential threats by establishing clear expectations and procedures for handling information. These rules help prevent unauthorized access to information that can be used to manipulate people

Field ofresearch The developed approaches can be used in the planning and implementation of the information security management system of the enterprise and the personal information security of a person

KEY WORDS: SOCIAL ENGINEERING, INFORMATION SECURITY, DIGITAL FOOTPRINT, INFORMATION HYGIENE, MANIPULATION

ЗМІСТ

DDoS атака (розшифровується як distributeddenial-of-service) – це кібер-атака, під час якої зловмисник старається зробити певний мережний ресурс

недоступним для користувачів, при цьому трафік на мережевий ресурс жертви надходить з різних джерел.

SET (Social EngineeringToolkit) - один із ключових та потужних інструментів для проведення комп'ютерної атаки, який включає всі необхідні інструменти для здійснення атак.

Wifiphisher – це унікальний інструмент соціальної інженерії, який автоматизує фішинг-атаки на мережах Wi-Fi для отримання паролів WPA / WPA2 від цільової групи користувачів.

MSFPC – це зручний інструмент, який спрощує процес створення основних корисних навантажень.

ВСТУП

Про актуальність - У сучасному світі інформація є одним з найважливіших ресурсів. Вона використовується в усіх сферах життєдіяльності людини, від бізнесу до державного управління. Разом з тим, інформація є й одним з найуразливіших ресурсів. Вона може бути легко втрачена, викрадена або спотворена.

Одним із способів отримання доступу до інформації є маніпулювання людьми. Маніпулювання - це вплив на думки, почуття та поведінку людини з метою досягнення певних цілей. Дослідники активно обговорюють поняття маніпулювання та надають різні визначення, найбільш характерні з яких наведені в таблиці

Таблиця

Визначення поняття маніпулювання людьми рвзними авторами[1]

№ з/п	Автори	Визначення
1.	Бессонов Б.М.	Форма духовного впливу прихованого панування, здійснювана насильницьким шляхом.
2.	Волкогонов Д.А.	Панування над духовним станом, управління зміною внутрішнього світу.
3.	Гудін Р.	Приховане застосування влади (сили) всупереч передбачуваній волі іншого.
4.	Йокояма О.Т.	Оманливий непрямий вплив на користь маніпулятора.
5.	Прото Л.	Прихований вплив на здійснення вибору.
6.	Рікер У.	Така структуризація світу, яка дає можливість вигравати.
7.	Рудінов Дж.	Спонукання поведінки за допомогою обману або гри на передбачуваних слабкостях іншого.
8.	Сагатовський В.М.	Ставлення до іншого як до засобу, об'єкта, знаряддя.
9.	Шиллер Г.	Приховане примушення, програмування думок, намірів, відчуттів, взаємин, установок, поведінки.
10.	Шостром Е.	Управління й контроль, експлуатація іншого, використання в ролі об'єктів, речей.
11.	Робінсон П.	Майстерне управління або використання.

Маніпулювання людьми може здійснюватися різними способами, зокрема, за допомогою соціальної інженерії. Соціальна інженерія - це вид кіберзлочинності, який полягає в використанні психологічних прийомів для

обману або спокуси людей з метою отримання від них доступу до інформації або виконання небажаних дій. Актуальність дослідження методів атаки та захисту від маніпулювання людьми для отримання доступу до інформації обумовлена такими факторами:

- Зростаючим значенням інформації в сучасному світі;
- Поширенням кіберзлочинності, зокрема, соціальної інженерії;
- Необхідністю підвищувати рівень захисту інформації від несанкціонованого доступу.

Мета дослідження полягає в розробці методів атаки та захисту від маніпулювання людьми для отримання доступу до інформації.

Об'єктом дослідження є процес маніпулювання людьми для отримання доступу до інформації. *Предметом* дослідження є методи атаки та захисту від маніпулювання людьми.У рамках даної роботи було поставлено такі *завдання*:

- Проаналізувати теоретичні основи дослідження маніпулювання людьми;
- Охарактеризувати типи загроз для кібербезпеки та види атак, які можуть використовуватися для маніпулювання людьми;
- Розглянути методи захисту від маніпулювання людьми для отримання доступу до інформації;
- Розробити рекомендації щодо захисту від маніпулювання людьми для отримання доступу до інформації.

Для досягнення поставлених завдань були використані такі *методи* дослідження:

- Аналіз наукової літератури;
- Аналіз статистичних даних;
- Експериментальне дослідження

Наукова новизна одержаних результатів. У межах проведеного дослідження були розроблені нові методи атаки та захисту від маніпулювання людьми для отримання доступу до інформації.

Практичне значення одержаних результатів. Розроблені методи атаки та захисту можуть бути використані для підвищення ефективності кібератаків і захисту від них. Методи атаки можуть бути використані для отримання доступу до секретної інформації, дестабілізації роботи організацій або поширення дезінформації. Методи захисту можуть бути використані для підвищення обізнаності користувачів про кіберзагрози, а також для розробки нових технологій захисту від кібератак.

Апробація результатів кваліфікаційної роботи.

*Структу рароботи.Р*обота складається з вступу, трьох розділів, висновків та списку використаних джерел.

РОЗДІЛ 1

ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ МАНІПУЛЮВАННЯ ЛЮДЬМИ

1.1 Соціальна інженерія як основний метод маніпулювання

Соціальна інженерія - це спосіб несанкціонованого доступу до даних чи систем зберігання даних, використовуючи слабкості людського фактору. Цей метод може бути руйнівним, коли зловмисник отримує інформацію, використовуючи різні техніки, такі як збір даних про службовців, телефонні дзвінки або імітація представників організації. Незважаючи на те, що ідея соціальної інженерії з'явилася недавно, люди використовували її прийоми здавна. У Стародавній Греції та Римі впливові особистості вміло переконували і маніпулювали, використовуючи брехню та вигідні аргументи. Спецагенти КДБ і ЦРУ також вправно використовували соціальну інженерію для отримання таємниць [3].

На початку 70-х років, під час розквіту фрікінгу, телефонні користувачі розважалися, викликаючи операторів корпорації Bell з вуличних автоматів та перевіряючи їх компетентність. Поступово вони розуміли, що змінюючи фрази та надаючи неправдиву інформацію, можна отримати конфіденційні дані від технічного персоналу. Фрікери експериментували та до кінця 70-х років майстерно маніпулювали операторами, здобуваючи необхідну інформацію. Соціальна інженерія в цій області перетворилася на мистецтво, де вправні соцінжери використовували своє чуття для отримання потрібних відомостей та маніпулювання людьми. З приходом комп'ютерів фрікери перейшли до використання своїх навичок в комп'ютерних мережах, стаючи хакерами та використовуючи соціальну інженерію для отримання конфіденційних даних. Наприклад, аферист може зателефонувати до працівника компанії, вигадавши ситуацію технічного збою, та вимагати пароль, представляючись членом технічної служби. Цей хід часто працює,

особливо якщо зловмисник використовує приємний голос та акторські здібності. Інший спосіб - дослідження відходів організацій, викрадення портативних комп'ютерів або носіїв даних, що використовується, коли атакуючий визначив конкретну організацію як ціль. Також існують інші методи соціальної інженерії для отримання даних [10].

Проблема маніпулювання людьми в сучасному контексті, особливо з використанням інформаційних технологій, стала надзвичайно актуальною та важливою. У зв'язку з масовою цифровізацією даних та послуг важливість збереження конфіденційності невпинно зростає. Кількість персональних комп'ютерів та смартфонів постійно зростає, а попит на послуги з обробки інформації стає все більш актуальним. Великі обсяги даних, що збираються різними компаніями для поліпшення надання своїх послуг, надають зручність кінцевим споживачам, але також стають об'єктом інтересу для зловмисників, таких як конкуренти, злочинці та вороги держави.

Проблема викрадення, пошкодження чи несанкціонованого доступу до інформації стає все більш актуальною і може призвести не тільки до втрат коштів, але й до загрози життю людей в країнах, де ведеться війна. Підвищення загального рівня захисту інформації у різних структурах, незалежно від форми власності, має невпинно продовжуватись. Проте, при постійному технічному розвитку засобів захисту інформації, найбільш вразливим залишається сам користувач.

Ця проблема охоплює різні аспекти, такі як поширення фейк-новин та дезінформації, використання соціальних мереж для маніпулювання громадською думкою, а також мікротаргетування та персоналізація реклами для впливу на конкретних користувачів. Дослідження цих аспектів вимагає інтердисциплінарного підходу, що об'єднує інформаційні технології, соціальну психологію, право та етику. Подолання цих проблем вимагає спільних зусиль уряду, технологічних компаній та громадськості для забезпечення інформаційної безпеки та захисту прав та свобод громадян у цифровому світі.

Соціальна інженерія вивчає вплив різних факторів на структуру соціальних систем, а також включає в себе маніпулювання людьми для досягнення певних цілей і отримання інформації [4]. Залежно від мети завдань, які стоять перед соціальним інженером (наприклад, завдання може бути спрямоване на завдання шкоди або отримання конфіденційної інформації), цей напрямок може бути ресурсозалежним і обмежуватися в часовому аспекті. Соціальна інженерія, яка спрямована на користувачів, являє собою слабке місце в ланцюжку кібербезпеки, оскільки користувачі не можуть бути ефективно захищені від таких атак

інструментами, як брандмауери і антивірусні програми. Вони завжди вразливі і можуть видавати інформацію, яка використовується зловмисниками для атак, навіть у тих моментах, коли цього менше очікується.

Хоча технічні рішення в галузі кібербезпеки значно покращилися, соціальна інженерія використовує психологічні методи для отримання інформації і може бути ефективною, враховуючи еволюцію людської природи. Хакери усвідомлюють складність технічних захисних заходів, які захищають системи, і тому вони звертають увагу на кінцевих користувачів, які є вразливішими. Соціальна інженерія, спрямована на різні аспекти психології людини, використовується для отримання інформації та компрометації мереж і ресурсів.

Окремо потрібно окреслити тему залучення штучного інтелекту при проведенні атак з копіюванням голосу за технологією “Deep fake” що найближчим часом стане великою проблемою в руках вправних соціальних інженерів.

На прикладі (рис.1.1.) представлено схему різних методів атак, які можуть бути використані зловмисниками для збирання інформації.

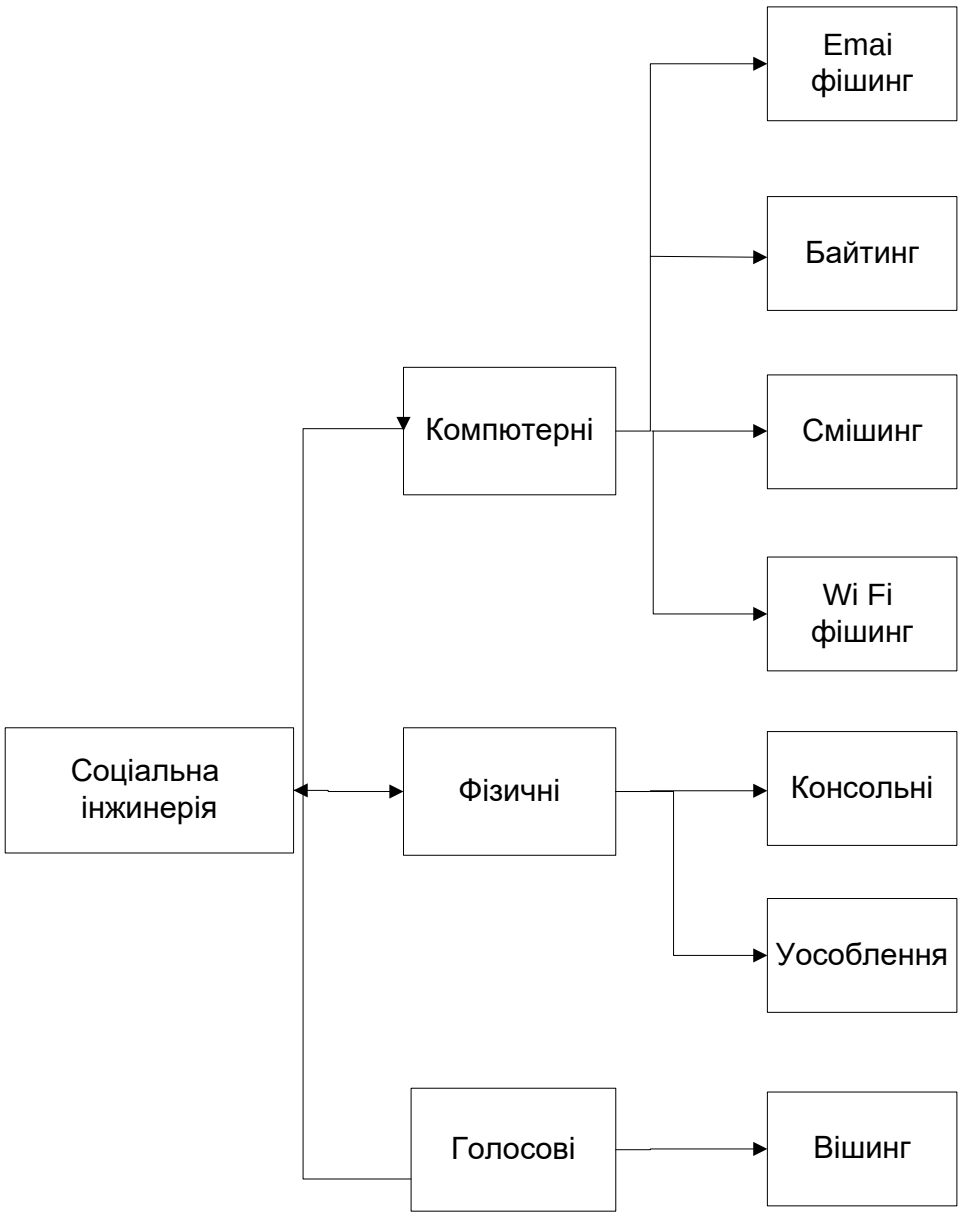

Рис. 1.1. Типи атак соціальної інженерії [12]

Соціальна інженерія розділяється на три головні категорії: комп'ютерні, голосові та фізичні атаки. Розглянемо кожну з них: комп'ютерні атаки, фізичні втручання та фішинг електронної пошти [12].

1. Комп'ютерні атаки

Фішинг: Цей метод використовує електронну пошту для збору інформації або для використання вразливостей програмного забезпечення у системі. Наживка: Ця стратегія використовує підступ, щоб переконати вас виконати дії, що дозволяють хакеру інфікувати ваш комп'ютер шкідливим програмним забезпеченням. USB-пристрої можуть бути використані як підступ, залишаючи їх у офісах або на парковках з етикетками "ЗП", "Фото корпоратив" і т. д. Люди, які їх знаходять, вставляють їх у комп'ютер, і вірус, прихований всередині, швидко поширюється на їх пристрій.

SMS ishing: Це форма фішингу через SMS. Аферисти відправляють жертві SMS-повідомлення з посиланням на фішинговий веб-сайт, мотивуючи їх ввести дані на цьому веб-сайті. Фішинг Wi-Fi: Тестери на проникнення можуть використовувати цей метод для збору імен користувачів та паролів, створивши альтернативну мережу Wi-Fi, схожу на мережу цільової компанії.

За данними CERT-UA, фішинг був найпомітнішою тактикою, яку зловмисники застосовували в першому півріччі 2023 р. (рис. 1.2). Це суттєва відмінність, адже в першому та другому півріччі 2022 року домінувало розповсюдження ШПЗ. Однак зараження шкідливим ПЗ і робота через Remote Access Trojan та C2, поряд із проникненнями через відомі експлуатовані вразливості чи скомпрометовані облікові записи, виділяються серед усього спектру як улюблені та досі дуже дієві стратегії.

Рис.1.2 Розподіл типів інциндентів ,зареєстрованого в перше півріччя 2023 року [19]

2. Голосові атаки

Голосова соціальна інженерія - це будь-яка атака, що використовує голосове повідомлення для обману користувача та спонукає його виконати певні дії на комп'ютері або призводить до розкриття конфіденційної інформації. ViShing - це один з методів соціальної інженерії, при якому зловмисники використовують телефонну комунікацію, граючи певні ролі (наприклад, співробітника банку або покупця), щоб виманити конфіденційну інформацію або надихнути власника картки на певні дії.

3. Фізичні атаки

Фізичні атаки передбачають присутність зловмисника на місці, який виконує соціальну інженерну атаку. Фізичні консольні атаки, зазвичай виконуються, коли зловмисники мають фізичний доступ до системи. "Листи від банків" представляють собою широко використовуваний метод соціальної інженерії. Він відрізняється від традиційного фішингу, оскільки зловмисники не чекають, коли користувачі самі потраплять на підроблений сайт. Замість цього вони самі підштовхують їх до цього, використовуючи фальшиві повідомлення від банків чи інших установ.

Також поширеною технікою є "емоційна буря", що є яскравим прикладом соціальної інженерії. Ці "WOW-повідомлення" використовують природню цікавість та емоційність користувачів, маючи вигляд коротких повідомлень від друзів в електронній пошті, соцмережах або месенджерах, які спонукають перейти за посиланням у тілі повідомлення. Посилання можуть вести як на фішингові сайти, так і на автоматичне завантаження шкідливого програмного забезпечення для крадіжки конфіденційної інформації.

Перетекстування - це використання заздалегідь підготовленого сценарію (претексту) для отримання від особи конкретних відомостей або проведення певних дій, часто з використанням телефону. Такий метод атаки часто базується на неправдивій інформації і вимагає попередніх досліджень, таких як персоналізація (наприклад, знання дати народження чи суми останнього рахунку) для вигляду довіри. До цього типу атак також відносять атаки через месенджери, такі як ICQ чи Skype.

Дорожнє яблуко - це метод атаки, який використовує троянського коня на

фізичних носіях даних. Зловмисник може залишити інфікований CD чи флеш-накопичувач в місцях, де їх легко знайти, таких як туалети, ліфти чи парковки. Носій виглядає як офіційний і може мати супровідний підпис, що викликає зацікавленість. Наприклад, диск із корпоративним логотипом та посиланням на сайт компанії може мати напис "Заробітна плата керівного складу". Співробітник, не пізнавши загрози, може використати диск на своєму комп'ютері або принести його в організацію як "добрий самаритянин".

В боротьбі з соціальною інженерією важливо дотримуватися кількох правил. По-перше, треба уважно ставитися до написання адрес сайтів та уникати переходу за посиланням з підозрілих електронних листів. При введенні логіна та паролю на сайтах слід звертати увагу на будь-які незвичайні зміни у вигляді сторінок. Дотримання цих правил може суттєво поліпшити рівень інформаційної безпеки та зменшити вразливість до методів соціальної інженерії.

Отже, соціальна інженерія є актуальною проблемою, яка впливає на свідомість людей. Недовіра користувачів є найслабшим ланкою в будь-якій системі, незалежно від рівня її захисту. Тому перед відкриттям будь-якого листа, отриманого по електронній адресі, важливо перевірити правильність адреси відправника та зміст повідомлення, а також приділяти увагу прикріпленим файлам.

1.2 Актуальність правил доступу до інформації

Поняття "інформація" є широко використовуваним і ключовим у різних галузях знань, хоча наукового визначення, яке було б загальноприйнятим, не існує. Це пояснюється багатогранністю інформації, яка існує в різних сферах, включаючи живу і неживу природу, кібернетичні системи та суспільство. Різноманітні форми інформації в матеріальному світі, різні способи її вивчення і використання різними галузями науки і практики також внесли свої особливості в визначення цього поняття.

У різні періоди часу переважали три основні підходи до визначення інформації: недетермінований, техноцентричний і антропоцентричний. 1. Недетермінований підхід:

· Не обмежує тлумачення інформації, вважаючи її фундаментальним поняттям з необмеженими рамками.

· Наприклад, Норд Вінер, засновник кібернетики, визначав інформацію як позначення змісту, отриманого зовнішнім світом в процесі пристосування і приведення його у відповідність до нашого мислення.

2. Техноцентричний підхід:

· Ототожнює інформацію з даними, що мають кількісний вимір, такі як обсяг, швидкість передачі тощо.

· Клод Шеннон визначав інформацію як "упорядковану субстанцію, яку можна описати математично".

3. Антропоцентричний підхід:

· Ототожнює інформацію з відомостями або фактами, які можуть бути засвоєні та перетворені в знання.

· Застосовується в юридичній науці і законодавстві, де інформацію вбачають у вигляді відомостей, які можна засвоїти та перетворити на знання.

У сучасному інформаційному суспільстві роль інформації стрімко зростає, визначаючи реалізацію прав суб'єктів на інформацію. Правові режими доступу до інформації, зокрема адміністративно-правові, використовуються для захисту інформації та регулювання доступу до неї. Однак обмеження доступу до певних видів інформації встановлені для забезпечення правового захисту конфіденційності.

Інформація дає людям можливість приймати поінформовані рішення, брати участь у демократичних процесах та стимулювати інновації. Однак, зростаюча доступність інформації також створила сприятливий ґрунт для маніпуляцій та експлуатації. Легкість, з якою можна поширювати інформацію та обмінюватися нею, зробила її потужним інструментом впливу на людей та формування громадської думки. Як наслідок, розуміння та усунення вразливостей, які виникають внаслідок маніпуляцій, набули першочергового значення.

Правила доступу до інформації відіграють вирішальну роль у захисті людей і суспільств від шкідливого впливу маніпуляцій. Ці правила

встановлюють межі, керівні принципи та протоколи, які регулюють збір, зберігання, поширення та використання інформації. Вони забезпечують повагу, конфіденційність і цілісність інформації, захищаючи приватне життя людей і запобігаючи несанкціонованому доступу або зловживанню нею. Ефективні правила доступу до інформації слугують кільком важливим цілям:

1. Захищають приватність і конфіденційність: Інформація про фізичних осіб часто є чутливою та особистою, і її несанкціоноване розголошення може мати серйозні наслідки. Правила доступу до інформації гарантують, що приватне життя людей поважається, а їхні персональні дані не розголошуються без їхньої згоди або в незаконних цілях.

2. Сприяти прозорості та підзвітності: Відкритий і прозорий доступ до інформації має важливе значення для забезпечення підзвітності установ та окремих осіб за їхні дії. Правила доступу до інформації сприяють прозорості, роблячи державні документи, державні кошти та інші форми інформації доступними для громадськості. Така прозорість дозволяє здійснювати контроль і нагляд, перешкоджаючи корупції та сприяючи належному врядуванню.

3. Розширення прав і можливостей громадян та громад: Доступ до інформації розширює можливості людей приймати поінформовані рішення щодо свого життя та життя своїх громад. Це дозволяє їм брати участь у демократичних процесах, долучатися до громадянської дискусії та вимагати підзвітності від своїх лідерів. Правила доступу до інформації гарантують, що люди мають знання та ресурси, необхідні для того, щоб робити поінформований вибір і робити значущий внесок у життя суспільства.

4. Сприяти інноваціям та економічному зростанню: Добре поінформоване суспільство є більш інноваційним та процвітаючим. Доступ до інформації дозволяє окремим особам і компаніям виявляти можливості, приймати обґрунтовані рішення та адаптуватися до мінливих обставин. Правила доступу до інформації сприяють розвитку економіки, заснованої на знаннях, сприяючи вільному поширенню ідей та інформації.

Цілі правил доступу до інформації

В умовах маніпуляцій правила доступу до інформації слугують важливою лінією захисту. Вони допомагають виявити та пом'якшити потенційні загрози,

встановлюючи чіткі очікування та протоколи поводження з інформацією. Забезпечуючи відповідальний доступ до інформації та її використання, ці правила можуть допомогти запобігти маніпуляціям, захистити права громадян та зберегти цілісність самої інформації. Ефективні правила доступу до інформації мають бути всеосяжними, адаптивними та примусовими. Вони повинні охоплювати всі форми інформації, включаючи цифрові, фізичні та усні дані. Вони також повинні адаптуватися до розвитку технологій та зміни суспільних норм. Крім того, для забезпечення дотримання правил і належного реагування на їх порушення необхідні потужні механізми правозастосування.

Отже, правила доступу до інформації - це не просто юридичні чи бюрократичні конструкції; вони є фундаментальними гарантіями для людей і суспільств у світі, що стає все більш інформаційно керованим. Захищаючи приватність, сприяючи прозорості, розширюючи можливості людей, сприяючи інноваціям і зменшуючи маніпуляції, ці правила відіграють
життєво важливу роль у забезпеченні того, щоб інформація використовувалася на благо всіх.

Висновки до першого розділу. У першому розділі роботи було розглянуто теоретичні основи маніпулювання людьми, зокрема, поняття маніпулювання, види маніпулятивних впливів, методи та техніки маніпулювання.Було встановлено, що маніпулювання - це вплив на думки, почуття та поведінку людини з метою досягнення певних цілей. Маніпулятивні впливи можуть бути різноманітними, але вони завжди мають на меті змінити думку або поведінку людини в бажаному для маніпулятора напрямку.

Основним методом маніпулювання людьми є соціальна інженерія. Соціальна інженерія - це вид кіберзлочинності, який полягає в використанні психологічних прийомів для обману або спокуси людей з метою отримання від них доступу до інформації або виконання небажаних дій. Правила доступу до інформації відіграють важливу роль у захисті людей і суспільства від маніпулювання. Вони допомагають ідентифікувати та мінімізувати потенційні загрози, встановлюючи чіткі очікування та процедури для поводження з інформацією. Забезпечуючи відповідальний доступ до інформації, правила

доступу до інформації можуть допомогти запобігти маніпуляції, захистити права людей і зберегти цілісність інформації. На основі проведеного дослідження можна зробити висновок, що правила доступу до інформації є важливим інструментом захисту від маніпулювання людьми. Ці правила допомагають запобігти несанкціонованому доступу до інформації, що може бути використане для маніпулювання людьми.

РОЗДІЛ 2
ХАРАКТЕРИСТИКА МЕТОДІВ АТАКИ ТА ЗАХИСТУ ВІД МАНІПУЛЮВАННЯ ЛЮДЬМИ

2.1 Типи загроз для кібербезпеки і види атак

У нашому сучасному суспільстві комп'ютери широко використовуються у всіх сферах. Захист важливої інформації стає необхідністю, особливо для великих компаній, які мають кібербезпекових фахівців. Однак у невеликих та середніх організаціях це питання залишається невирішеним. На жаль, немає універсальних рішень, але важливо звертати увагу на основні типи кіберзагроз. Наприклад, захист від атак на мережевий периметр отримує багато уваги, і багато пристроїв вже оснащені базовими засобами безпеки. Зробимо акцент на загрозах, які можуть бути менш очевидними або їх важливість зазвичай недооцінюється. П'ять основних типів кіберзагроз включають програми-вимагачі, цільові кібератаки, DDoS атаки, фішинг та внутрішні загрози, пов'язані з інсайдерами та людськими помилками. Згідно з останнім звітом «Verizon 2020 Data Breach Report: Money Still Makes the Cyber-Crime World Go Round», 86% кібератак мають фінансову мотивацію, зловмисники вимагають гроші від своїх жертв [22] .

Оператори зв’язку, фінансові установи, ритейл-мережі та промисловий сектор сьогодні найчастіше стають жертвами кібератак. Зростає інтерес зловмисників до малих і середніх підприємств через високу конкуренцію та обмежені можливості кіберзахисту. Важливим фактором є також розповсюдження віддаленої роботи, що розширює периметр мережі на особисті пристрої співробітників. Основні типи кіберзагроз включають програми-вимагачі, цільові атаки, DDoS, інсайдерські загрози та фішинг. Важливо вживати комплекс заходів, таких як системна профілактика, оцінка ризиків, міжмережеві екрани та резервні копії, для ефективного захисту.

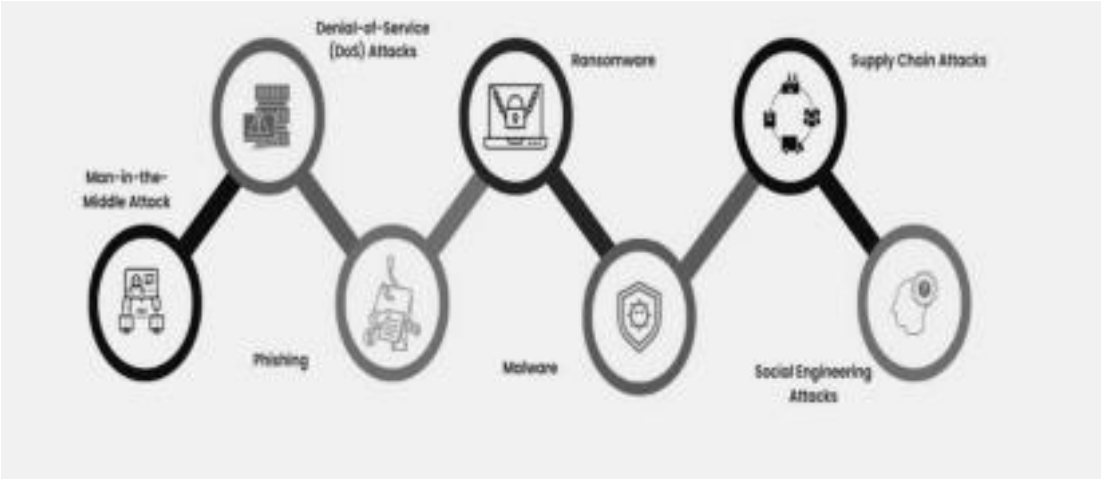

Рис.2.1. Основні типи кіберзагроз [6]

DDoS-атака — це спроба перегрузити обчислювальну систему, таку як сервер, шляхом одночасного відправлення великої кількості запитань. Коли система не може ефективно обробити цей потік, виникає відмова в обслуговуванні (Denial of Service), і система може вийти з ладу. Це особливо загрожує компаніям, що активно використовують Інтернет, наприклад, у сфері електронної комерції, а також операторам зв'язку. Останнім часом зловмисники використовують пристрої Інтернету речей (IoT) для своїх ботів, такі як принтери, розумні колонки та інші, оскільки їх безпека часто залишає бажати кращого. Захист від DDoS-атак включає використання фільтрів, що дозволяють відсікати надмірні запити від ботів, а також розумну конфігурацію системи для мінімізації можливих атак [5].

Інсайдерські загрози. Широка група загроз, викликаних внутрішніми факторами, особливо актуальна в організаціях, де відсутній ефективний контроль за наданням високих рівнів доступу та відсутні обмеження щодо прав доступу до інформаційних ресурсів. Інсайдерські загрози можуть виникати як зловмисний умисел, так і в результаті випадкових дій або людських помилок. Для протидії їм необхідно впроваджувати принцип мінімальної достатності, надавати працівникам лише ті права, які є необхідними для виконання їхніх обов'язків. Також корисними є системи, які
аналізують поведінку користувачів, використовуючи технології штучного інтелекту, щоб виявляти відхилення від звичайних сценаріїв діяльності та вчасно сповіщати службу безпеки.

Фізичні атаки означають, що зловмисник фізично присутній на місці,

виконуючи соціальну інженерну атаку. Тут розглядаються два типи таких атак, які можна здійснити під час червоної команди або тестування на проникнення.

1. Уособлення: Соціальний інженер "прикидається людиною" або грає ролью, якій ви, ймовірно, довіряєте або підкоритесь, щоб отримати доступ до вашого офісу, інформації або інформаційних систем.
2. Консольна атака: Це атаки, які передбачають фізичний доступ до системи, такі як зміна пароля адміністратора, встановлення кейлоггера або отримання доступу до збережених паролів браузера.

Kali також стимулює атаки, коли зловмисник отримує прямий фізичний доступ до систем та мережі. Це може бути ризиковано, оскільки зловмисник може бути помічений. Але винагорода може бути значною, оскільки зловмисник може скомпрометувати конкретні системи з цінними даними. Фізичний доступ, як правило, досягається через соціальну інженерію, особливо використовуючи імітацію. Це може включати такі сценарії, як особа, яка видає себе за співробітника IT, яка швидко потребує доступу для оновлення системи, або продавець, який відвідує клієнта, але виправдовується для зустрічі з іншою людиною або візиту до туалету. Зловмисники можуть також придбати форму кур'єра через Інтернет, однак багато людей припускає, що особа в уніформі Glovo із жовтим рюкзаком є працівником, тому соціальна інженерія не потребує уніформи.

Щодо проникнення в образі важливого менеджера з буфером обміну, це може вразити працівників, які вас не впізнають. Такий тип проникнення зазвичай повідомляється як аудитор, інспектор, що рідко піддається опитуванню. Мета ворожого фізичного доступу полягає в швидкому компрометуванні обраних систем, часто за допомогою встановлення
прихованого або схожого пристрою. Наприклад, зловмисники можуть розмістити USB-ключ та надати системі можливість автоматичного встановлення через автовідтворення. Використання Metasploit дозволяє зловмиснику прикріпити корисне навантаження до виконуваного файлу, такого як заставка, що може бути видається за корпоративну. Коли користувач встановлює програму, встановлюється бекдор, який з'єднує зловмисника з системою [18].

Сучасні зловмисники все частіше використовують передові технології, такі як штучний інтелект, і вдаються до методів соціальної інженерії, використовуючи вразливості людської психології. Це підкреслює важливість перенесення розуміння кіберзагроз з вузької сфери IT-фахівців до загального рівня знань, щоб кожен співробітник мав уявлення про поточні загрози, особливо керівники, які визначають завдання фахівців з кібербезпеки.

Взаємодія з психікою людини - це обширна тема, яка охоплює різноманітні методи впливу або керування думками, почуттями або поведінкою іншої особи. Ці методи можуть застосовуватися як з конструктивною, так і з деструктивною метою. Однак у контексті кібербезпеки вони частіше використовуються зі злочинними намірами.Сучасне життя стало набагато зручнішим завдяки розмаїттю цифрових пристроїв та Інтернету, що їх підтримує. Проте цей технологічний прогрес має свої темні сторони, зокрема, збільшення кількості кібератак. Кібератака - це будь-яка зловмисна діяльність, спрямована на IT-системи або користувачів з метою несанкціонованого доступу до даних.

2.1.1 Методи та техніки проведення атак

Злочинці часто використовують атаки для отримання фінансової вигоди, порушення роботи системи або навіть шпигунства. Суб'єктами загрози можуть бути як окремі особи, які намагаються отримати конфіденційні дані, так і державні структури, що прагнуть завдати шкоду іншим. Незалежно від мотивів, кіберзахист є необхідною складовою для
забезпечення безпеки мереж і даних.Кібератаки можуть призводити до втрати цілісності даних, фінансових втрат, порушення довіри та шкоди репутації. Запобігання цим атакам включає в себе застосування засобів кіберзахисту, таких як антивірусне програмне забезпечення та брандмауери, а також особисту обізнаність щодо фішингових атак та оновлення паролів. Розглянемо деякі з найпоширеніших типів кібератак, з якими стикаємося сьогодні.

1. Malware Attack

Це один з найпоширеніших типів кібератак. "Шкідливе програмне забезпечення" означає шкідливі програмні віруси, включаючи черв'яки, шпигунські програми, програми-вимагачі, рекламні програми та трояни.

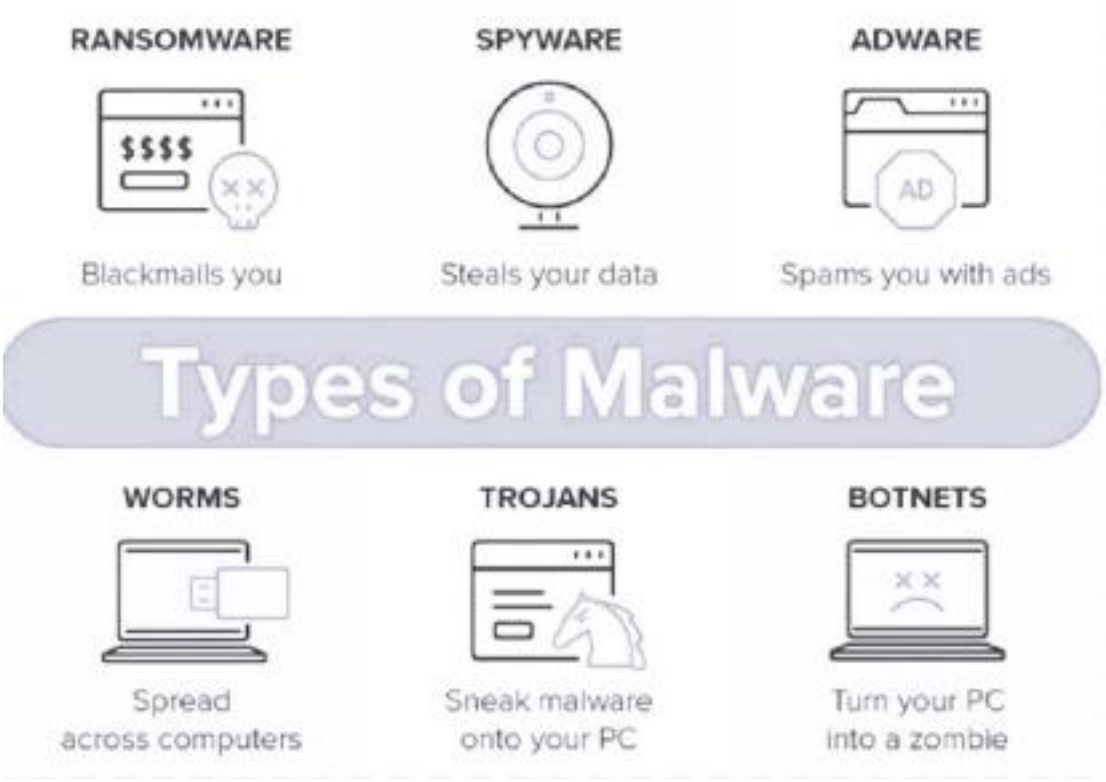

Рис.2.2.Типи Malware attack [12]

Троянський вірус маскується під легальне програмне забезпечення [20]. Програми-вимагачі блокують доступ до ключових компонентів мережі, тоді як шпигунські програми викрадають усі ваші конфіденційні дані без вашого відома. Рекламне ПЗ - це програмне забезпечення, яке відображає на екрані користувача рекламний контент, наприклад, банери. Шкідливе програмне забезпечення проникає в мережу через вразливість. Коли
користувач натискає на небезпечне посилання, завантажує вкладення в електронному листі або використовує заражену флешку.

Як можна запобігти атаці шкідливого програмного забезпечення: · Використовуйте антивірусне програмне забезпечення. Воно може захистити ваш комп'ютер від шкідливого програмного забезпечення. Avast Antivirus, Norton Antivirus та McAfee Antivirus - ось декілька популярних антивірусних програм.

· Використовуйте брандмауери. Брандмауери фільтрують трафік, який може потрапити на ваш пристрій. Windows і Mac OS X мають вбудовані брандмауери за замовчуванням, які називаються Windows Firewall і Mac Firewall.

· Будьте пильні і не переходьте за підозрілими посиланнями. ·

Регулярно оновлюйте операційну систему та браузери. 2. Phishing Attack

Фішингові атаки є одним з найпоширеніших видів кібератак. Це різновид соціальної інженерії, коли зловмисник видає себе за довірену особу і надсилає жертві фальшиві листи. Не знаючи про це, жертва відкриває лист і переходить за шкідливим посиланням або відкриває вкладений файл. Таким чином зловмисники отримують доступ до конфіденційної інформації та облікових даних. Вони також можуть встановити шкідливе програмне забезпечення через фішингову атаку [32]. Фішингові атаки можна запобігти, дотримуючись наведених нижче кроків:

· Уважно перевіряйте електронні листи, які отримуєте. Більшість фішингових листів мають суттєві помилки, такі як орфографічні помилки та зміни формату, які відрізняються від легітимних джерел.

· Використовуйте антифішингову панель інструментів. ·

Регулярно оновлюйте свої паролі.

3. Password Attack

Це форма атаки, при якій хакер намагається отримати доступ до вашого пароля за допомогою різноманітних програм і інструментів для злому паролів, таких як Aircrack, Cain, Abel, John the Ripper, Hashcat і т. д. Існують різні види атак на паролі, такі як атаки грубої сили, атаки за словником та атаки, використовуючи кейлогери. Нижче подано декілька способів запобігти атакам на паролі:

· Використовуйте надійні алфавітно-цифрові паролі зі спеціальними символами.

· Не використовуйте один і той самий пароль для різних веб-сайтів або облікових записів.

· Регулярно оновлюйте свої паролі, що обмежить вашу вразливість до атак.

· Не зберігайте підказки до паролів у відкритому доступі.

4.Man-in-the-Middle Attack

Атака "Man-in-the-Middle" (MITM), також відома як атака на підслуховування, відбувається, коли зловмисник втручається у двосторонню комунікацію між клієнтом і хостом, перехоплюючи зв'язок. Це дозволяє хакерам

отримувати та маніпулювати даними.

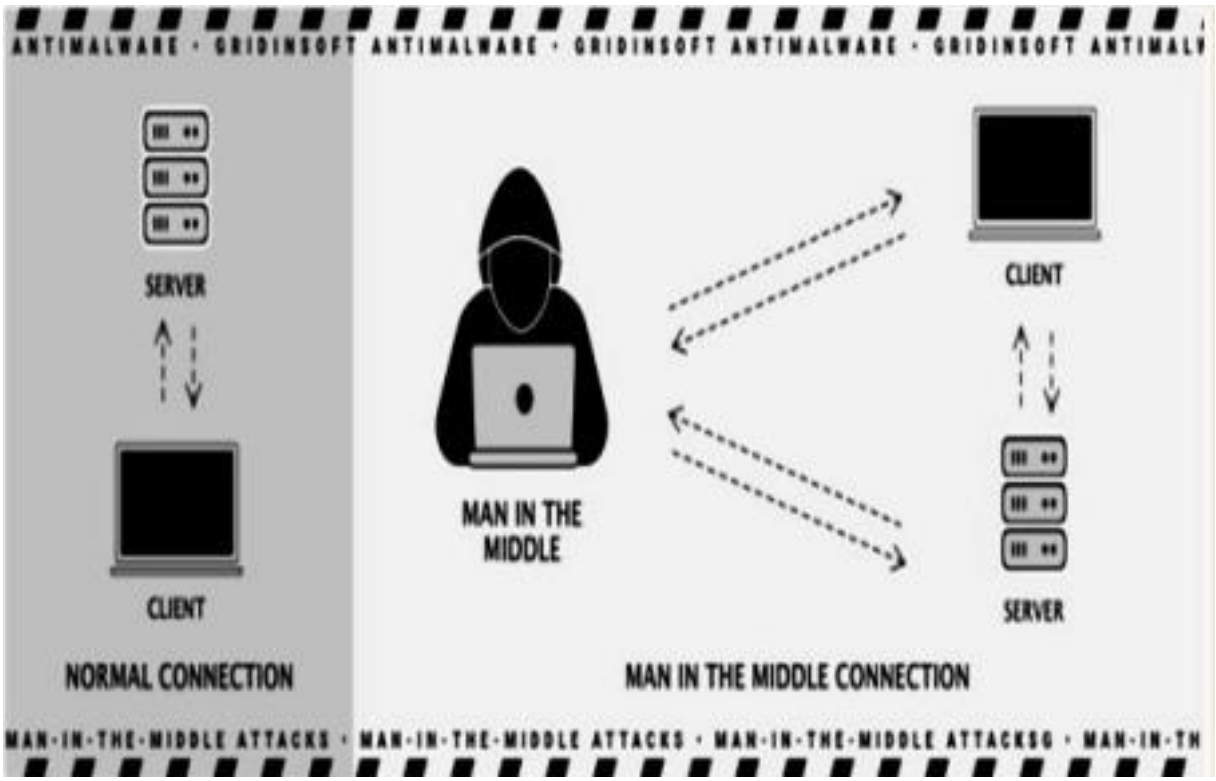

Рис.2.3. Схема атаки MITM [18]

Щоб запобігти атакам MITM, слід:

1. Пам'ятати про безпеку веб-сайтів, використовуваних вами, і використовувати шифрування на своїх пристроях.

2. Утримуйтеся від використання публічних Wi-Fi мереж. 5.

SQL Injection Attack

Атака SQL відбувається на веб-сайті, керованому базою даних, коли хакер маніпулює стандартним SQL-запитом, вводячи шкідливий код у вразливий пошуковий рядок. Це може призвести до втрати важливої інформації та навіть отримання зловмисниками прав адміністратора. Для запобігання атакам SQL-ін'єкції:

1. Використовуйте систему виявлення вторгнень для виявлення несанкціонованого доступу.

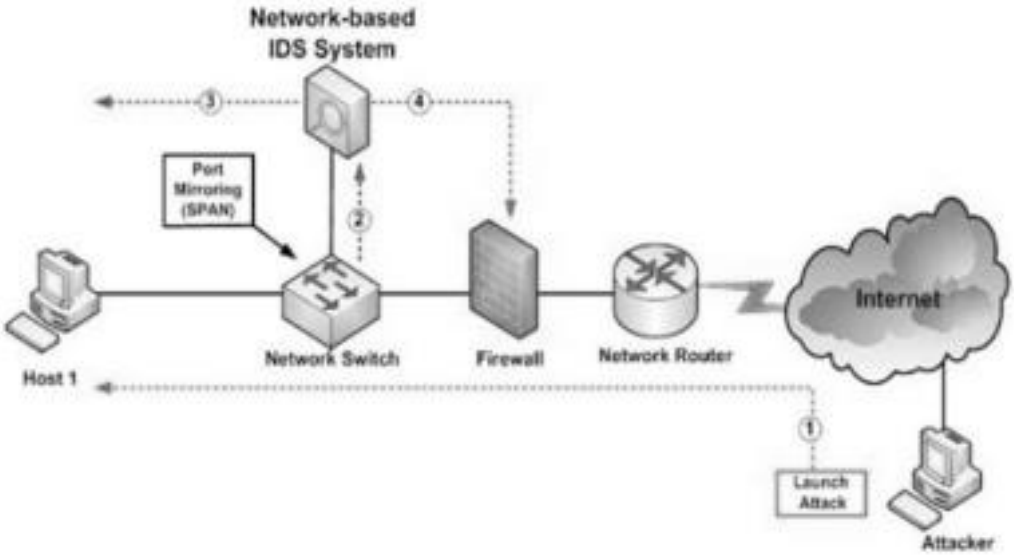

Рис.2.4.Застосування системи виявлення вторгнень[18]

2. Здійснюйте валідацію даних, наданих користувачем, для контролю введених даних.

6.Cross-Site Scripting (XSS)

Атака XSS також включає впровадження шкідливого коду на веб-сайт, але в цьому випадку сам веб-сайт не атакується. Замість цього, шкідливий код запускається в браузері користувача при відвідуванні атакованого веб-сайту. Це може завдати серйозної шкоди репутації веб-сайту та поширити інформацію користувачів без їхнього відома [34].

7. Перехоплення сеансу

Перехоплення сеансу відбувається, коли зловмисник перехоплює сеанс, перехоплюючи унікальний - і приватний - ідентифікатор сеансу і видає себе за комп'ютер, який робить запит, що дозволяє йому увійти в систему як нічого не підозрюючий користувач і отримати доступ до несанкціонованої інформації на веб-сервері. Якщо під час будь-якого сеансу роботи в Інтернеті все йде належним чином, веб-сервери повинні відповідати на ваші різноманітні запити, надаючи вам інформацію, до якої намагаєтеся отримати доступ. Однак існує ряд методів, які зловмисник може використати для викрадення ідентифікатора сеансу, наприклад, міжсайтова скриптова атака, яка використовується для перехоплення ідентифікаторів сеансу. Зловмисник також може перехопити сеанс, щоб вставити себе між комп'ютером, що запитує, і віддаленим сервером, видаючи себе за іншу сторону в сеансі. Це дозволяє перехоплювати інформацію в обох напрямках і

зазвичай називається атакою MITM.

8. Cryptojacking

Термін "криптоджекінг" тісно пов'язаний з криптовалютою. Криптоджекінг відбувається, коли зловмисники отримують доступ до чужого комп'ютера для майнінгу криптовалюти. Доступ отримують шляхом зараження веб-сайту або маніпулювання жертвою, щоб вона натиснула на шкідливе посилання. Вони також використовують для цього онлайн-рекламу з кодом JavaScript. Жертви не знають про це, оскільки код для видобутку криптовалюти працює у фоновому режимі; затримка у виконанні - єдина ознака, яку вони можуть помітити. Криптоджекінгу можна запобігти, виконавши наведені нижче кроки:

· Оновіть своє програмне забезпечення та всі програми безпеки, оскільки криптоджекінг може заразити найбільш незахищені системи.

· Проведіть тренінг для співробітників щодо криптоджекінгу; це допоможе їм виявляти загрози криптоджекінгу.

· Встановіть блокувальник реклами, оскільки реклама є основним джерелом скриптів для криптоджекінгу. Також встановіть розширення на кшталт MinerBlock, яке використовується для виявлення та блокування скриптів для майнінгу криптовалют.

Як уникнути кібератак? Можна висвітлити безліч тактик і рекомендацій для запобігання кібератакам у великому масштабі, але розглянемо кілька ключових прикладів:

1. Тренінг щодо фішингу: Організуйте навчання працівників з виявлення та усвідомлення небезпек фішингових атак. Проводьте імітаційні фішингові кампанії, щоб підвищити обізнаність та вдосконалювати реакції на спроби шахрайства.

2. Виявлення скомпрометованих облікових даних: Використовуйте аналітику поведінки користувачів для встановлення стандартної активності в мережі. Спостерігайте за активністю облікових записів адміністраторів та інших служб, щоб вчасно виявляти потенційні загрози.

3. Захист від програм-вимагачів: Розробіть тривимірний план для мінімізації поверхні атак, зменшення впливу вразливостей та виявлення прогалин. Це включає реагування на виявлені вразливості, блокування

скомпрометованих облікових записів та зміну облікових даних.

4. Захист від XSS-атак: Впроваджуйте політику фільтрації для зовнішніх даних, що пройшли через веб-сайт. Це допомагає виявляти шкідливі скрипти до їх впливу та встановлює широку політику безпеки контенту.

5. Програма розвідки загроз: Створіть центральний вузол, який надає всім функціям організації безпеки необхідні знання та дані про основні загрози. Використовуйте автоматизацію для постійного подання даних про загрози та вдосконалення безпекових процесів.

Розвиток кібербезпеки можна відслідковувати від перших етапів розвитку комп'ютерних технологій, коли заходи безпеки були обмеженими, а розміри Інтернету були відносно скромними. В початковий період 90-х років брандмауери використовувалися як поширений метод захисту мереж і даних від кібератак [14]. Зараз область кібербезпеки охоплює широкий спектр технологій, таких як системи виявлення вторгнень, розвідка загроз та управління інформацією та подіями безпеки (SIEM). З урахуванням зростаючої кількості кіберзлочинів в сучасному світі, знання про кібератаки та засоби захисту вашої мережі стає надзвичайно важливим.

2.1.2 Огляд інструментів впровадження атак

У сфері кібербезпеки інструменти атаки - це спеціалізоване програмне або апаратне забезпечення, що використовується окремими особами або групами для здійснення кібератак. Ці інструменти призначені для використання вразливостей у комп'ютерних системах, мережах і програмних додатках для отримання несанкціонованого доступу, викрадення конфіденційних даних, порушення роботи або заподіяння шкоди. Інструменти атак охоплюють широкий спектр можливостей, від простих інструментів для злому паролів до складних фреймворків для мережевої експлуатації. їх використовують зловмисники, щоб отримати несанкціонований доступ до систем, викрасти дані, порушити роботу або завдати шкоди. Інструменти атаки можна розділити на різні типи залежно від їхнього призначення, функціональності та цільових систем. Деякі поширені

категорії інструментів атаки включають в себе [2]

1. Інструменти експлуатації: Ці інструменти використовуються для використання вразливостей у програмному або апаратному забезпеченні для отримання несанкціонованого доступу до системи. Вони можуть скористатися помилками програмування, неправильною конфігурацією або застарілим програмним забезпеченням, щоб обійти засоби контролю безпеки і виконати шкідливий код.

2. Інструменти сканування та розвідки: Ці інструменти використовуються для сканування мереж або систем на наявність вразливостей, виявлення потенційних цілей і збору інформації про цільове середовище. Вони можуть допомогти зловмисникам виявити слабкі місця в конфігураціях безпеки, розкрити конфіденційні дані або скласти топологію мережі.

3. Інструменти соціальної інженерії: Ці інструменти використовуються для маніпулювання або обману користувачів, щоб змусити їх розкрити конфіденційну інформацію або вжити заходів, які ставлять під загрозу їхню безпеку. Вони можуть включати створення підроблених веб-сайтів, надсилання фішингових електронних листів або створення повідомлень у соціальних мережах, які експлуатують людську психологію.

4. Інструменти для злому паролів: Ці інструменти використовуються для злому захищених паролем систем шляхом спроб вгадати або перебору паролів. Вони можуть використовувати словники, алгоритми або їхні комбінації для генерації та тестування мільйонів паролів проти системи.

5. Інструменти відмови в обслуговуванні (DoS): Ці інструменти використовуються, щоб перевантажити систему або мережу трафіком, роблячи її недоступною для законних користувачів. Вони можуть завалити сервер запитами, споживати пропускну здатність або використовувати вразливості для порушення роботи.

6. Руткіти: Ці інструменти призначені для отримання та підтримки прихованого доступу до системи. Вони приховують себе від виявлення і можуть бути використані для встановлення шкідливого програмного забезпечення, крадіжки даних або віддаленого керування системою.

7. Інструменти для створення шкідливого програмного забезпечення: Ці

інструменти надають зловмисникам основу для створення власного шкідливого програмного забезпечення, або шкідливого ПЗ. Вони можуть включати компілятори, налагоджувачі та бібліотеки коду, які спрощують процес розробки та розгортання шкідливого програмного забезпечення.

Найбільш потужним інструментом для проведення комп'ютерних атак є Social Engineering Toolkit (SET). Розроблений і написаний Девідом Кеннеді та підтримується активною групою співавторів, SET є фреймворком, керованим Python, із відкритим вихідним кодом, спеціально розроблений для полегшення атак соціальної інженерії [20]. SET взаємодіє з Metasploit Framework, забезпечуючи необхідне навантаження для експлуатації, шифрування для обходу антивірусного програмного забезпечення та модуль прослуховування для підключення до скомпрометованої системи.

Для запуску SET в дистрибутиві Kali, перейдіть до Додатків в Kali Linux / Інструменти експлуатації / Набір інструментів соціальної інженерії setoolkit або введіть setoolkit у командному рядку. Головне меню SET виглядає так [22]:

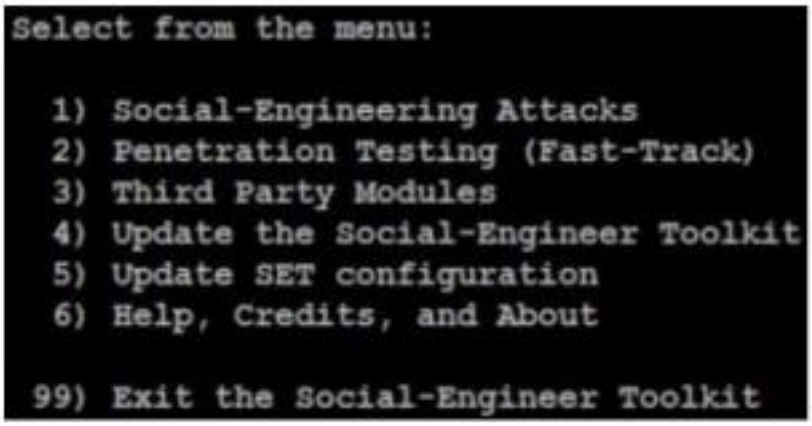

Рис. 2.5. Головне меню SET[20]

Якщо вибрати "Соціально-інженерні атаки", можна побачити наступне підменю, яке включає вектори атак:

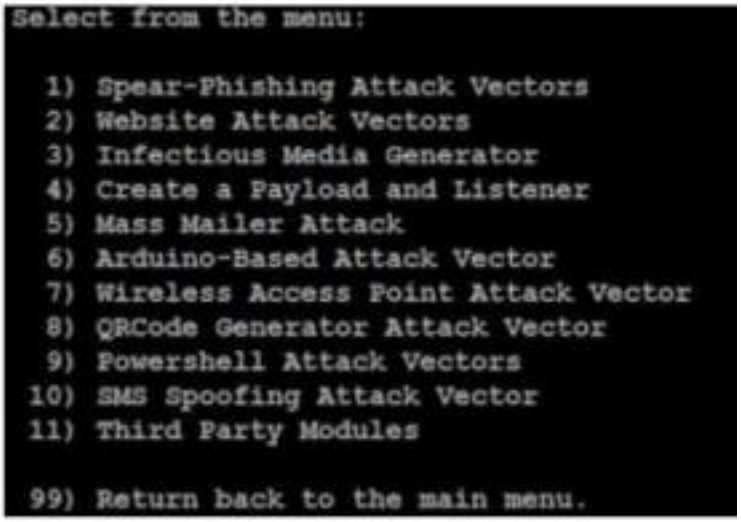

Рис. 2.6.Види атак у підменю[20]

- Веб-сайт атак.
- Інфекційний медіагенератор.
- Створення корисного навантаження і слухача.
- Масова атака.
- Вектор атак на основі Arduino.
- Вектор атак бездротової точки доступу.
- Вектор атак генератора QRCode.
- Вектори атак Powershell.
- Сторонні модулі.

Розділ "Вектори веб-сайтів" детально розглядає різні методи атак, такі як впровадження Java, використання браузера Metasploit, атака на харвестер, таббата, веб-гейдінг та HTA. Ці методи розділені на підрозділи, надаючи зловмисникам гнучкість у виборі стратегії для атак [26].

Wifiphisher - це інструмент соціальної інженерії, який автоматизує фішинг-атаки на мережі Wi-Fi з метою отримання паролів WPA / WPA2 від цільових користувачів. Інструмент може вибрати будь-яку точку доступу Wi Fi поблизу, заблокувати її (скасувати автентифікацію всіх користувачів) і створити точку доступу-клон, до якої не потрібен пароль. Коли людина підключається до цієї мережі, вона сприймається як легітимна, але насправді вона стикається з фішинг-сторінкою, що запитує ввести пароль Wi-Fi.Після того, як цільові користувачі вводять пароль, Wifiphisher відправляє попередження та затримується на час. Потім він відображає підроблений

таймер перезавантаження та підроблений екран оновлення, надаючи час для тестування отриманого пароля. Цей інструмент допомагає в оцінці рівня захисту

від соціальної інженерії на основі Wi-Fi.

Рис.2.7.Інтерфейс Wifiphisher[15]

MSFPC - це зручний інструмент, який спрощує створення базових корисних навантажень, уникнувши довгих команд msfvenom. Цей генератор дозволяє створювати корисні навантаження з мінімум одним аргументом.

MSFPC може створювати корисні навантаження для Windows, Linux і навіть Android. Він економить час, дозволяючи швидко створювати прості корисні навантаження. Хоча він не враховує кодування для обходу антивірусів, це все одно може бути корисним для вивчення.Іноді вам просто потрібно швидко створити корисний товар, доставити його і продовжити виконувати рутинні завдання [20]. У таких випадках msfpc.sh може вам допомогти. Щоб використовувати MSFPC, вам потрібно лише визначити необхідне корисне навантаження за допомогою розширення файлу або платформи, на яку плануєте його впустити. Після введення msfpc в терміналі, можна використовувати інструмент.

2.2 Методи захисту від маніпулювання людьми для отримання доступу до інформації

Обговорення маніпуляцій як соціального явища сьогодні є активною

темою гуманітарних досліджень, спричиненням до цього є політична та економічна обстановка в країні та у світі, поширеність маніпулятивних явищ і доступність методів впливу. Маніпуляції представляють собою систему сценаріїв, алгоритмів і технік, пов'язаних із досягненням цілей зацікавлених осіб, які можуть впливати на діяльність та життя не лише окремої особистості чи соціальної групи, а й зачіпати великі суспільні утворення різних рівнів. У сучасну цифрову епоху маніпулювання людьми з метою отримання доступу до інформації викликає велике занепокоєння. Зловмисники використовують різні тактики, включаючи соціальну інженерію, фішинг та шкідливе програмне забезпечення, щоб використати людські вразливості та отримати конфіденційні дані. Щоб протистояти цим загрозам, люди повинні застосовувати проактивний підхід до захисту своєї інформації [18].

Соціальна інженерія - це хитра тактика, що ґрунтується на людській взаємодії та психологічному маніпулюванні з метою обманом змусити людей розголошувати конфіденційну інформацію або вчиняти дії, що ставлять під загрозу їхню безпеку.

Рис.2.8.Схема впливу в соціальній інженерії [5]

Найпоширеніші методи соціальної інженерії включають в себе введення в оману, фішинг, приманку та послугу за послугу. Під приводом зловмисник створює фальшиву особистість або сценарій, щоб завоювати довіру жертви, тоді як фішинг передбачає надсилання електронних листів або текстових повідомлень, які імітують легітимні джерела, щоб обманом змусити одержувачів перейти за шкідливими посиланнями або розкрити особисті дані. Приманка - це залишення в громадських місцях цінних на перший погляд предметів, таких як USB-накопичувачі, з метою спокусити людей, які нічого не підозрюють, підключити їх до своїх комп'ютерів і ненавмисно інсталювати шкідливе програмне забезпечення. Quid pro quo передбачає пропозицію жертві чогось в обмін на її особисту інформацію або доступ до її пристрою. Дослідження Пітера Шааба, Крістіана Бекерса та Себастьяна Пейпа підкреслює важливість міждисциплінарних підходів до
протидії атакам соціальної інженерії [23]. Вони підкреслюють необхідність поєднання досвіду IT-безпеки зі знанням людської поведінки, що є важливим аспектом, який часто ігнорується в традиційних стратегіях IT-безпеки. Дослідження пропонує цінну інформацію про те, як інтеграція принципів соціальної психології може посилити захисні механізми проти цих типів атак, тим самим покращуючи загальне управління безпекою.

Фішинг, ще один поширений метод маніпуляцій, використовує оманливі електронні листи або текстові повідомлення, які нібито походять від авторитетних організацій, таких як банки або компанії, що видають кредитні картки. Ці повідомлення часто містять посилання, які перенаправляють жертв на фальшиві веб-сайти, дуже схожі на легальні. Після введення на цих шахрайських сайтах особистих даних, таких як імена користувачів і паролі, зловмисники отримують несанкціонований доступ до їхніх облікових записів.

Значну загрозу становить шкідливе програмне забезпечення, призначене для завдання шкоди комп'ютерним системам. Шкідливе програмне забезпечення може проникати на комп'ютер різними способами, включаючи перехід за шкідливими посиланнями, відкриття заражених вкладень або завантаження файлів з ненадійних джерел. Після інсталяції шкідливе програмне забезпечення може викрадати конфіденційну інформацію, встановлювати інші шкідливі

програми або навіть брати під контроль всю систему.

Щоб ефективно захистити себе від маніпуляцій, люди повинні прийняти ряд стратегій. По-перше, дуже важливо бути обізнаним з різними методами маніпуляцій. Розуміння тактики, яку застосовують зловмисники, дає можливість розпізнавати та уникати цих схем. По-друге, дуже важливо бути обережним при обміні інформацією в Інтернеті. Потрібно уникати надання особистих даних особам або платформам, яким не довіряєте, і будьте уважні до того, що публікується в соціальних мережах [14].

По-третє, пильність щодо підозрілих електронних листів або текстових повідомлень має першорядне значення. Якщо в повідомленні запитується особиста інформація або містяться посилання на незнайомі веб-сайти, будьте обережні. Не переходьте за посиланнями, доки не перевірите їхню достовірність. Крім того, дуже важливо підтримувати актуальне програмне забезпечення, оскільки оновлення часто включають виправлення безпеки, які усувають вразливості, що використовуються зловмисниками.

Крім того, встановлення та регулярне оновлення антивірусного та антивірусного програмного забезпечення забезпечує додатковий рівень захисту від зараження шкідливими програмами. Також важливо дотримуватися обережності при завантаженні файлів з Інтернету. Завантажуйте файли лише з перевірених джерел, щоб мінімізувати ризик проникнення шкідливого програмного забезпечення.

Використання надійних паролів та їх регулярна зміна підвищує безпеку облікового запису. Крім того, увімкнення двофакторної автентифікації додає додатковий рівень захисту, оскільки для доступу до облікового запису потрібно не лише пароль, але й додатковий етап перевірки, наприклад, код, надісланий на телефон користувача. Вживаючи таких комплексних заходів, люди можуть ефективно захистити свою особисту інформацію від маніпуляцій і зберегти контроль над своєю цифровою безпекою. Методи захисту від маніпулювання людьми для отримання доступу до інформації включають такі підходи:

1. Освіта і тренування: Навчання співробітників розпізнавати та протидіяти спробам соціальної інженерії є ключовим. Це включає розуміння різних тактик, які можуть використовувати зловмисники, наприклад фішинг,

претендування на іншу особу, та використання емоційного тиску.

2. Політика безпеки і процедури: Встановлення чітких процедур та політик щодо управління інформацією і доступом до неї допомагає зменшити ризики. Це може включати політики паролів, процедури перевірки особи та обмеження доступу до важливої інформації.

3. Регулярні перевірки безпеки: Проведення регулярних аудитів та оцінок безпеки допомагає виявити та усунути потенційні слабкі місця в системах та процедурах.

4. Технічні засоби захисту: Використання антивірусного програмного забезпечення, фаєрволів, фільтрів електронної пошти та інших технологій може допомогти захистити від шкідливих атак і спроб маніпуляції.

5. Контроль доступу та ідентифікація: Обмеження доступу до важливих систем та даних до визначених осіб і ролей у компанії. Використання багатофакторної аутентифікації для підвищення безпеки.

6. Підвищення обізнаності серед співробітників: Регулярне інформування та оновлення співробітників про поточні загрози і шахрайські схеми допомагає їм залишатися пильними.

7. Створення культури безпеки: Заохочення відкритого обговорення питань безпеки та залучення всіх рівнів організації до створення безпечного середовища.

Застосування цих методів може значно підвищити захист інформації від маніпулятивних атак.

2.2.1Цифровий слід і напрями його зменшення

Цифровий слід (Digital Footprint) представляє дані про активність та внесок користувача в онлайн-середовище. Це включає інформацію, яку люди розміщують в інтернеті чи інформацію, яка генерується їхніми онлайн-діями. Зловмисники можуть використовувати цей цифровий слід, наприклад, для створення переконливих фішингових атак або для ідентифікації потенційних жертв соціальної інженерії. Знання та усвідомлення власного цифрового сліду є ключовими для захисту від таких маніпуляцій. Ці дані включають особисті

профілі та аккаунти в соціальних мережах, інформацію про відвідувані веб-сайти, відкриті та створені файли, особисті повідомлення, коментарі, відео, фотографії та іншу особисту інформацію користувача [44].

Цифрові сліди використовуються для дослідження та аналізу різних організацій, включаючи проведення онлайн-опитувань та використання правоохоронними органами для отримання інформації. Соціальні медіа використовують цифровий слід для аналізу інтересів користувачів Інтернету, нерідко збираючи та аналізуючи ці дані без відома самого користувача. В банківській сфері, використання технології Digital Footprint досі є рідкісним, проте його впровадження може значно поліпшити ефективність банківської системи кредитування. Це сприятиме підвищенню якості вихідних даних для скорингових моделей потенційних позичальників.

В епоху повсюдного цифрового зв'язку наша діяльність в Інтернеті залишає по собі незгладимий слід, формуючи унікальний цифровий слід, який охоплює наші взаємодії, внески та комунікації в безмежному просторі Інтернету. Цей цифровий слід, який іноді називають цифровою тінню або електронним слідом, слугує віртуальним відображенням нашої онлайн

персони, формуючи те, як нас сприймають інші, і потенційно впливаючи на різні аспекти нашого життя. Хоча наш цифровий слід може відігравати важливу роль у налагодженні зв'язків, обміні ідеями та доступі до великої кількості інформації, він також несе в собі потенційні ризики та проблеми. Величезна кількість персональних даних, які генеруємо в Інтернеті, може збиратися, аналізуватися і використовуватися різними суб'єктами, в тому числі бізнесом, урядами і навіть окремими особами зі зловмисними намірами. Це викликає занепокоєння щодо приватності, захисту даних і можливості маніпуляцій.

Щоб ефективно орієнтуватися в цифровому ландшафті та захищати нашу присутність в Інтернеті, важливо розуміти природу нашого цифрового сліду та фактори, що сприяють його формуванню. Активні цифрові сліди, такі як пости в соціальних мережах, коментарі в блогах та онлайн-профілі, відображають нашу цілеспрямовану діяльність в Інтернеті. Пасивні цифрові сліди, з іншого боку, створюються без нашої явної згоди, часто за допомогою

технологій відстеження, що використовуються веб-сайтами, брокерами даних

та іншими організаціями.

Хоча наш цифровий слід може бути цінним інструментом для самовираження та зв'язку, він також несе в собі потенційні ризики. Роботодавці можуть ретельно вивчати наші онлайн-профілі, щоб оцінити нашу відповідність посаді, а правоохоронні органи можуть досліджувати нашу цифрову активність у зв'язку з кримінальними розслідуваннями. Більше того, компанії можуть використовувати наш цифровий слід для персоналізованої реклами, потенційно впливаючи на наші рішення щодо купівлі та формуючи наш досвід роботи в Інтернеті. У світлі цих проблем дуже важливо застосовувати проактивний підхід до управління нашим цифровим слідом. Ось кілька важливих кроків, які допоможуть захистити вашу конфіденційність в Інтернеті та зберегти контроль над вашою цифровою ідентичністю:

1. Зрозумійте свій цифровий слід: Ознайомтеся з типами даних, які формують ваш цифровий слід, включаючи активні та пасивні сліди. Активні сліди - це ті, які створюєте навмисно, наприклад, пости в соціальних мережах і покупки в Інтернеті. Пасивні сліди створюються без вашої безпосередньої участі, наприклад, за допомогою файлів cookie та технологій відстеження, що використовуються веб-сайтами.

2. Будьте уважні до того, чим ділитеся в Інтернеті: Перш ніж публікувати або ділитися чимось в Інтернеті, подумайте, хто може це побачити і чи комфортно вам це. Будьте обережні, коли ділитеся особистою інформацією, наприклад, домашньою адресою, номером телефону або даними про роботу.

3. Відрегулюйте свої налаштування конфіденційності: Більшість веб сайтів і платформ соціальних мереж пропонують налаштування конфіденційності, які дозволяють вам контролювати, хто може бачити вашу інформацію. Знайдіть час, щоб переглянути та відкоригувати ці налаштування відповідно до ваших уподобань щодо конфіденційності [38].

4. Використовуйте пошукові системи, орієнтовані на конфіденційність: Подумайте про перехід на пошукову систему, яка ставить конфіденційність користувачів на перше місце, наприклад, DuckDuckGo. Ці альтернативи уникають відстеження вашої історії пошуку та особистих даних, мінімізуючи збір інформації, яка може вплинути на ваш цифровий слід.

5. Будьте обережні з дозволами для веб-сайтів і додатків: Реєструючись на нових веб-сайтах або завантажуючи додатки, уважно переглядайте дозволи, які вони вимагають. Уникайте надання непотрібного доступу до ваших персональних даних, таких як місцезнаходження, контакти або мікрофон, якщо не впевнені в цілях програми та її методах безпеки.

6. Слідкуйте за онлайн-акаунтами: Регулярно перевіряйте онлайн акаунти на наявність будь-якої підозрілої активності, наприклад, спроб несанкціонованого входу або зміни вашої особистої інформації. Якщо помітили щось незвичне, негайно змініть свої паролі та зверніться до відповідних постачальників послуг.

Застосовуючи ці стратегії, можна взяти під контроль свій цифровий слід і захистити свою конфіденційність у постійно мінливому онлайн ландшафті. Пам'ятайте, що ваша цифрова ідентичність - це цінний актив, і дуже важливо відповідально нею керувати. Отже, наш цифровий слід є невід'ємною частиною нашого існування в Інтернеті, формуючи наш досвід і впливаючи на те, як нас сприймають інші. Розуміючи природу нашого цифрового сліду, відповідально ставлячись до поведінки в Інтернеті та застосовуючи ефективні заходи захисту, можемо впевнено орієнтуватися в цифровому ландшафті, зберігаючи конфіденційність і захищаючи нашу онлайн-ідентичність.

Як зменшити свій цифровий слід? Щорічно обсяг особистих даних користувачів в Інтернеті зростає. Інформація з соціальних мереж, онлайн платежі, історії місцезнаходжень, електронні листи та повідомлення через платформи обміну миттєвими повідомленнями складає лише частину вашого цифрового сліду [45]. Розмаїття цього цифрового портрету залежить від ваших звичок розголошення інформації та ставлення до конфіденційності в Інтернеті. Кіберзлочинці можуть використовувати велику кількість ваших даних у злочинних сценаріях або продавати їх на чорних ринках. Навіть якщо вважаєте, що ваші дані нецікаві для інших, в Інтернеті кожен може стати жертвою кіберзлочинців. З великою кількістю доступних ризиків важливо зберігати баланс між приватністю та зручністю використання Інтернет сервісів.

Одним із перших кроків є перевірка основних налаштувань

конфіденційності, визначення того, хто має доступ до вашої інформації. Також важливо ретельно вивчити свій список друзів у соціальних мережах, видаляючи тих, кого не пам'ятаєте, і обмежуючи доступ до особистої інформації. Ваша діяльність в мережі може стати джерелом багатої інформації, яку можна використовувати зловмисно.

Більшість осіб мають десятки, а іноді сотні облікових записів в Інтернеті — на різних веб-сайтах для покупок, фітнес-додатках, кулінарних ресурсах, іграх, додатках та інших сервісах. Кожен з цих ресурсів зберігає різноманітні види особистої інформації, такої як ім'я, дата народження та номер телефону, що може стати предметом інтересу зловмисників. З технологією єдиного входу через облікові записи Google, Facebook або Apple стає легше реєструватися. Оскільки майже ніхто не має повного списку всіх облікових записів, що створені протягом років, можливість єдиного входу може виявитися зручною. Незалежно від того, який обліковий запис використовуєте, всі вони надають можливість переглядати, які додатки мають доступ до вашого облікового запису. Цей перелік можна використовувати для видалення облікових записів, які вам вже не потрібні. Але якщо реєструвалися за допомогою електронної пошти, то можна шукати сервіси за допомогою фраз в поштових листах, таких як "скасувати підписку" або "ласкаво просимо".

Ще один спосіб зменшити свій цифровий слід — це відписування від електронних розсилок новин. Багато підписок додаються автоматично під час реєстрації в різних сервісах та магазинах, які потім надсилають вам електронні листи з новинами та пропозиціями. Часто, зазначаючи при реєстрації, автоматично погоджуємося на отримання рекламних листів. Після очищення пошти від непотрібних підписок, розумною буде створити окрему адресу електронної пошти для покупок. Зменшення цифрового сліду — це не лише ті кроки, що були описані вище. Ще одним важливим інструментом для мінімізації цифрового сліду є використання віртуальної приватної мережі (VPN), яка діє як зашифрований тунель для вашого Інтернет-трафіку і забезпечує захист від відстеження.

Також, можете скористатися інструментами, такими як перевірка конфіденційності Google, для перегляду та, за необхідності, припинення

зберігання відомостей сервісами. Крім того, якщо цікавить, що саме знає Twitter або Facebook, то можна завантажити копію всіх даних, які вони зберігають.

2.2.2 Інформаційна гігієна як захист від маніпулювання

Орієнтуючись у постійно зростаючому цифровому ландшафті, на нас постійно обрушується потік інформації з різних джерел. Цей величезний потік даних може бути приголомшливим, що робить складним завданням відрізнити достовірну інформацію від оманливого або маніпулятивного контенту. Саме тут з'являється концепція інформаційної гігієни як найважливішого інструменту для навігації в цифровому світі. Інформаційна гігієна, подібно до підтримання фізичного здоров'я за допомогою належних гігієнічних практик, передбачає управління потоком інформації в нашому житті, щоб захистити себе від неправдивої інформації, дезінформації та маніпуляцій. Подібно до того, як надається пріоритет фізичній гігієні, щоб захиститися від шкідливих патогенів, повинні дотримуватися інформаційної гігієни, щоб захиститися від згубного впливу помилкової або маніпулятивної інформації. Значення інформаційної гігієни полягає в тому, що вона дає нам
можливість приймати поінформовані рішення, захищати себе від шкоди і виховувати більш поінформованих громадян.

Ухвалення обґрунтованих рішень залежить від доступу до точної та достовірної інформації. Озброєні достовірними даними, можемо робити усвідомлений вибір, який відповідає нашим цінностям і прагненням. І навпаки, вплив неправдивої інформації або дезінформації може призвести до помилкових рішень з потенційно згубними наслідками. Інформаційна гігієна слугує захисним щитом від тактик маніпуляції, які застосовують окремі особи чи групи, що намагаються використати наші вразливості. Застосовуючи практики інформаційної гігієни, можна ефективно виявляти та протистояти спробам вплинути на наші переконання, поведінку чи дії.

У демократичному суспільстві поінформовані громадяни є основою процвітаючої демократії. Активна участь у громадському дискурсі та відповідальне прийняття рішень вимагають доступу до точної та неупередженої

інформації. Інформаційна гігієна дає людям можливість стати поінформованими та активними громадянами, сприяючи розвитку міцної та добре функціонуючої демократії. Щоб розвивати ефективні практики інформаційної гігієни, повинні скептично ставитися до інформації в Інтернеті. Перш ніж сприймати інформацію як достовірну, необхідно поставити під сумнів її джерело та достовірність [26]. Крім того, пошук інформації з різних джерел, включаючи як основні, так і альтернативні ЗМІ, забезпечує ширшу перспективу і допомагає виявити потенційні упередження.

Визнання та усвідомлення власних упереджень є важливим для об'єктивного оцінювання інформації. Наш особистий досвід, переконання та цінності можуть впливати на те, як інтерпретуємо інформацію. Розуміючи свої упередження, можна прагнути до об'єктивності та уникати суджень, що ґрунтуються на упереджених уявленнях. Веб-сайти та інструменти для перевірки фактів пропонують цінні ресурси для перевірки достовірності інформації. Використання цих інструментів дає нам змогу приймати
поінформовані рішення, що ґрунтуються на перевірених фактах, а не на необґрунтованих твердженнях. Утримання від поширення неперевіреної інформації має вирішальне значення для стримування поширення дезінформації та дезінформації. Поширення контенту без перевірки його достовірності сприяє поширенню неточної та потенційно шкідливої інформації.

На додаток до вищезгаданих стратегій, доцільно обмежити вплив соціальних мереж, оскільки соціальні медіа-платформи можуть бути розсадниками дезінформації та дезінформації. Критичне оцінювання джерел інформації та розвиток навичок критичного мислення є важливими для ефективної обробки інформації. Походження терміну "інформація" має латинське коріння (informatio) і вказує на передачу роз'яснень, викладу фактів чи подій. Інформація представляє собою будь-які відомості, створені людиною для передачі у часі та просторі. Процес отримання, обміну та використання інформації називається інформаційним процесом. Коли освоюємо та використовуємо інформацію, вона перетворюється на знання. Процес обробки інформації визначається численними факторами.

Інформація з обмеженим доступом - це та, що складає державну

таємницю, розголошення якої може завдати шкоди державі, суспільству або окремій особі. Інформація сприяє взаємодії різних груп людей, тому інформаційна взаємодія виступає ключовою формою соціальної взаємодії. Всесвітній рівень взаємодії вже визначається єдиною інформаційною системою, що фактично працює в режимі реального часу. Задоволення потреби в інформації грає важливу роль у суспільстві, а дезінформація та інформаційний хаос можуть викликати почуття невпевненості та безсилля.Проблему споживання інформації можна вирішити, упорядковуючи, сортуючи та спеціалізуючись в інформації за допомогою самостійного вибору людиною. Інформація, що виникає разом із суспільством, вважається соціальною інформацією. Основні характеристики соціальної інформації включають кількість, цінність, зміст, об'єктивність, адекватність, вірогідність, точність, оперативність та надійність. **Соціальна інформація** має важливу властивість - вона ніколи не є нейтральною. Соціальну інформацію, що передається через мас-медіа, слід розглядати як процес масової комунікації, що включає в себе зміст, процеси інформаційного обміну, технічні засоби та інше. Терміни "комунікація" та "інформація" в часто використовуються як синоніми в деяких документах міжнародних організацій, і точного загальноприйнятого визначення для них немає. Основна мета масової інформації - відображення реальності. При оцінці інформації звертають увагу на якісні характеристики, такі як адекватність, вірогідність, актуальність, повнота та об'єктивність. Адекватність вказує на відповідність створеного образу реальному об'єкту, явищу або процесу. Актуальність визначає важливість на даний момент часу. Об'єктивність вказує на безпристрасність та незалежність інформації від думок та прагнень людини. Повнота інформації визначається її достатністю для розуміння та прийняття рішень. Дезінформація - це спотворена, свідомо неправдива інформація, яка розповсюджується з метою введення в оману громадськості, політичних опонентів, конкурентів тощо. Також термін використовується для опису процесу поширення у ЗМІ або іншими засобами викривлених або свідомо неправдивих відомостей. У військовій справі це може бути тактичне або стратегічне маскування, яке полягає у планомірному розповсюдженні неправдивих відомостей про власні збройні сили, їх склад, озброєння, боєздатність і військові плани [44].

Ознаки дезінформації включають вплив на конкретну аудиторію через оприлюднення, цілеспрямованість з організатором та умислом, негативні суспільно-небезпечні наслідки, базову "неправдивість", яку можна перевірити, імітаційність, що представлена як правдивий матеріал, "вбудованість" у певні системи поглядів та прив'язку до соціально значущих подій. Види дезінформації включають фейки, маніпулювання, обман конкретних осіб або груп, а також створення необхідної громадської думки.

У світі сучасної інформаційної влади інформаційний вплив стає основним інструментом, який приносить нові виклики та загрози, пов'язані з дезінформацією, фейковими новинами та фальшивою інформацією .У нинішню епоху інформаційного надлишку здатність відрізняти достовірні та надійні джерела від тих, що поширюють неправдиву інформацію та дезінформацію, набуває першочергового значення. Інформаційна гігієна - практика відповідального та розбірливого споживання інформації - слугує важливим захистом від маніпуляцій та поширення шкідливих наративів[38]. Прийнявши принципи критичного оцінювання, аргументації на основі фактів та самосвідомості, люди можуть ефективно орієнтуватися в інформаційному просторі та приймати обґрунтовані рішення.

Ключові принципи інформаційної гігієни:

1. Оцінка джерел: Критично оцінюйте достовірність джерел інформації. Враховуйте досвід автора, його зв'язки та потенційну упередженість. Перевірте репутацію джерела та його історію достовірності.

2. Аргументація на основі фактів: Вимагайте докази на підтримку заяв і тверджень. Шукайте підтверджуючу інформацію з різних джерел. Скептично ставтеся до інформації, наданої без доказів.

3. Усвідомлення упередженості: Розпізнавати та визнавати власні упередження, які можуть впливати на сприйняття інформації. Активно шукайте перспективи, які кидають виклик вашим існуючим переконанням.

4. Відповідальний обмін інформацією: Будьте обережні, коли ділитеся інформацією. Перевірте точність контенту, перш ніж поширювати його. Уникайте поширення інформації з ненадійних джерел або тих, хто має злі наміри [8].

Неправдива інформація, дезінформація, пропаганда та клікбейт є поширеними формами маніпулятивної інформації. Знання їхніх характеристик може покращити вашу здатність розпізнавати достовірну інформацію

1. Дезінформація: Часто ненавмисна дезінформація виникає через помилки у повідомленні, інтерпретації чи комунікації. Вона може бути позбавлена злого умислу, але все одно може призвести до нерозуміння і прийняття дезінформованих рішень.

2. Дезінформація: Свідомо створювана і поширювана, дезінформація має на меті ввести в оману або завдати шкоди окремим особам чи групам. Вона часто використовує сфабриковану або викривлену інформацію для маніпулювання громадською думкою або просування певного порядку денного.

3. Пропаганда: Упереджена та однобока, пропаганда прагне впливати на сприйняття та просувати певну точку зору. Вона часто використовує емоційні заклики, нагнітання страху та демонізацію протилежних поглядів.

4. Клікбейт: Призначена для привернення уваги та генерування кліків, клікбейт часто використовує сенсаційні заголовки, оманливі ескізи або перебільшені заяви. Це може призвести до появи нерелевантного або неточного контенту, що відволікає користувачів від джерел, які заслуговують на довіру.

Інформаційна гігієна - це не просто індивідуальна відповідальність; вона вимагає колективних дій для сприяння розвитку здорової інформаційної екосистеми [3]. Організації можуть відігравати вирішальну роль, застосовуючи відповідальні практики у створенні, поширенні та модерації контенту [1].

· Створення контенту: Надавайте пріоритет точності, прозорості та фактологічно обґрунтованим повідомленням. Чітко визначати джерела та визнавати потенційну упередженість.

· Поширення інформації: Використовуйте відповідальні канали розповсюдження інформації та уникайте поширення неперевіреного або оманливого контенту.

· Модерація контенту: Встановіть чіткі правила модерації контенту, гарантуючи, що шкідлива або маніпулятивна інформація буде видалена або позначена відповідним чином.

Отже, інформаційна гігієна є важливим інструментом для навігації в

сучасному складному інформаційному ландшафті. Розвиваючи навички критичного мислення, проявляючи обережність у споживанні інформації та просуваючи відповідальні практики, окремі особи та організації можуть захистити себе від маніпуляцій і сприяти створенню більш поінформованої та надійної інформаційної екосистеми.Застосовуючи правила інформаційної гігієни, можемо ефективно орієнтуватися в цифровому світі, приймати обґрунтовані рішення, захищати себе від маніпуляцій і сприяти розвитку добре поінформованого суспільства. Інформаційна гігієна дає нам можливість стати вибагливими споживачами інформації, сприяючи створенню більш відповідального та стійкого цифрового ландшафту.

Висновки до другого розділу. У другому розділі дослідження розглянуті основні методи кібератак та заходи захисту від маніпулювання людьми для отримання доступу до інформації. Методи захисту від маніпулювання людьми для отримання доступу до інформації включають освіту та підвищення обізнаності, де навчають індивідів розпізнавати спроби соціальної інженерії та маніпуляції. Важливим аспектом є управління цифровим слідом, тобто обмеження інформації, яку люди діляться в Інтернеті, для ускладнення маніпуляторам збору даних. Також важливою є інформаційна гігієна, яка включає практику безпечного користування цифровими сервісами, включаючи обережне використання соціальних мереж та інтернету. Не менш важливими є політики безпеки, які включають розробку та впровадження корпоративних політик для запобігання витоку інформації, а також технічні засоби, як-то шифрування, двофакторна аутентифікація та інші технологічні рішення. Також досліджено інструменти, які використовуються зловмисниками для здійснення атак, такі як

вірусописні програми, спам-боти та зламні інструменти. Для захисту від маніпулювання людьми наведено методи, такі як зменшення цифрового сліду та інформаційна гігієна.

Цифровий слід та інформаційна гігієна відіграють ключову роль, оскільки інформація, яка вільно доступна в інтернеті, може бути використана маніпуляторами, а також запобігають необдуманому розповсюдженню особистої

інформації.

У контексті подальших досліджень можна зосередитись на розвитку навичок критичного мислення, досліджуючи методи навчання, які допомагають людям критично ставитися до інформації. Важливим є також вивчення нових технологій для виявлення та блокування спроб соціальної інженерії, а також аналіз психології маніпуляції, що включає вивчення методів, які використовують маніпулятори, та розробку стратегій протидії.

РОЗДІЛ 3
РОЗРОБКА РЕКОМЕНДАЦІЙ ПО ЗАХИСТУ ВІД МАНІПУЛЮВАННЯ ЛЮДЬМИ ДЛЯ ОТРИМАННЯ ДОСТУПУ ДО ІНФОРМАЦІЇ

3.1 Аналіз досвіду маніпулювання людьми при доступі до інформації

Можливість доступу до інформації та її обробки має важливе значення для прийняття поінформованих рішень та ефективної участі в житті суспільства. Однак зростаюча доступність інформації в Інтернеті також полегшує маніпулювання людьми. У цьому розділі проаналізуємо досвід маніпулювання людьми під час доступу до інформації, зосередившись на таких аспектах:

· Різні методи, що використовуються для маніпулювання людьми · Фактори, які роблять людей більш вразливими до маніпуляцій · Наслідки маніпуляцій

· Рекомендації щодо захисту від маніпуляцій

· Техніки маніпуляції

Існує безліч методів, які можуть бути використані для маніпулювання людьми при отриманні доступу до інформації. Деякі з найпоширеніших методів включають[38]:

1. Дезінформація: Це поширення неправдивої або оманливої інформації з наміром ввести в оману. Дезінформація може поширюватися різними каналами, включаючи соціальні мережі, новинні веб-сайти і навіть "сарафанне радіо".
2. Фреймінг: Це подання інформації в такий спосіб, щоб вплинути на думки чи переконання людей. Наприклад, новинна стаття може виставляти політичного кандидата в позитивному або негативному світлі, вибираючи, які факти включити або підкреслити.
3. Повторення: Це повторення висловів, лого тощо знову і знову, щоб зробити його більш запам'ятовуваним і переконливим. Наприклад, політична кампанія може повторювати гасло знову і знову, щоб підвищити ймовірність того, що виборці його запам'ятають.
4. Відомі люди: Тут використовується той факт, що люди з більшою ймовірністю повірять тому, кого вони сприймають як експерта або авторитетну особу. Наприклад, для того, щоб переконати людей купити товар, можна використати схвалення знаменитостей.
5. Пропаганда: Це інформація, яка подається таким чином, щоб вплинути на

думки чи поведінку людей. Пропаганда може використовуватися для просування певної політичної ідеології, продукту або послуги. 6. Нагнітання страху: Це використання страху для маніпулювання людьми з метою спонукання їх до певних дій. Залякування може використовуватися для продажу товарів, отримання підтримки певного політичного кандидата або просто для контролю над поведінкою людей.

Існує низка факторів, які можуть зробити людей більш сприйнятливими до маніпуляцій, зокрема

· Когнітивні упередження: Це ментальні ярлики, які можуть призвести до помилок у мисленні. Деякі поширені когнітивні упередження, які можуть зробити людей більш вразливими до маніпуляцій, включають евристику доступності, упередження підтвердження та ефект фреймінгу.

· Брак навичок критичного мислення: Навички критичного мислення - це здатність об'єктивно аналізувати інформацію та формувати власні судження. Люди, яким бракує навичок критичного мислення, більш схильні до маніпулювання інформацією, яка апелює до їхніх емоцій або упереджень.

· Довіра до авторитетних осіб: Люди часто більш схильні вірити інформації, яка надходить від авторитетних осіб, таких як політики, знаменитості чи експерти. Це може зробити людей більш вразливими до маніпуляцій з боку тих, хто має владу або вплив.

· Емоційна вразливість: Люди, які переживають сильні емоції, такі як страх, гнів або смуток, більш схильні до маніпуляцій. Це пов'язано з тим, що емоції можуть затьмарювати судження людей і робити їх більш сприйнятливими до переконань.

Наслідки маніпуляції можуть бути значними і далекосяжними. Ось деякі з потенційних наслідків маніпуляції:

· Дезінформоване прийняття рішень: Коли людьми маніпулюють, вони більш схильні приймати рішення на основі неправдивої або оманливої інформації[15]. Це може призвести до низки негативних наслідків, таких як фінансові втрати, репутаційні збитки або навіть фізична шкода.

· Соціальний поділ і конфлікт: Маніпуляції можуть бути використані для того, щоб посіяти розбрат і розкол між людьми. Це може призвести до соціальних

заворушень, насильства і навіть війни.

· Недовіра: Коли люди піддаються маніпуляціям з боку можновладців, це може підірвати їхню довіру до таких інституцій, як уряд, засоби масової інформації та бізнес. Це може призвести до руйнування соціального порядку і зниження громадянської активності.

Розвивати навички критичного мислення: Навички критичного мислення необхідні для об'єктивної оцінки інформації та формування власних суджень. Існує низка ресурсів, які допоможуть людям розвинути навички критичного мислення, наприклад, онлайн-курси, книги та семінари.

Когнітивні упередження можуть зробити людей більш вразливими до маніпуляцій. Знаючи про поширені когнітивні упередження, люди можуть навчитися їх розпізнавати та уникати[43]. Те, що хтось має владу чи вплив, не означає, що він завжди говорить правду. Важливо скептично ставитися до інформації від авторитетних осіб і об'єктивно оцінювати її, перш ніж прийняти.Емоції можуть затьмарювати судження людей і робити їх більш вразливими до маніпуляцій. Коли відчуваєте сильні емоції, важливо бути особливо уважними до інформації, яку споживаєте. Один з найкращих способів захиститися від маніпуляцій - шукати різноманітні джерела
інформації. Це допоможе вам отримати більш повне і збалансоване уявлення
про світ.

Маніпулювання людьми під час доступу до інформації може мати негативний вплив на окремих осіб та суспільство в цілому. Ось деякі з можливих наслідків:

· Дезінформація: Люди, якими маніпулюють, можуть бути більш схильні вірити дезінформації, що може призвести до прийняття ними неправильних рішень.

· Поляризація: Маніпуляції можуть бути використані для поляризації людей і ускладнення для них цивілізованого обговорення важливих питань.

· Ерозія довіри: Маніпуляції можуть підірвати довіру до інституцій та ускладнити співпрацю між людьми.

Отже, маніпуляція - це поширена проблема, яка може мати значні наслідки для окремих людей, суспільств і світу в цілому. Аналізуючи досвід

маніпулювання людьми при доступі до інформації, можна відзначити кілька реальних випадків. Наприклад, були випадки, коли фінансові установи та банки ставали мішенями фішингових атак. Шахраї надсилали електронні листи, що імітували офіційну кореспонденцію від банку, з метою отримання конфіденційної інформації, такої як дані кредитних карток або паролі від банківських рахунків.

У сфері електронної комерції також були випадки, коли споживачі отримували електронні листи, які здавалися від популярних роздрібних торговців. Ці листи могли містити шкідливі посилання або вкладення, які вимагали від користувачів ввести свої особисті дані або платіжну інформацію. Щодо криптовалют, відомі випадки фішингових атак на користувачів криптовалютних бірж та гаманців, де шахраї створювали фальшиві веб-сайти або відправляли електронні листи, імітуючи офіційні повідомлення від цих сервісів, з метою вкрасти криптовалюту.

Ці приклади демонструють, як маніпуляція може бути використана для отримання доступу до конфіденційної інформації в різних секторах.Згідно з дослідженням компанії "IRONSCALES", починаючи з березня 2020 року, близько 81% компаній по всьому світу зіткнулися зі зростанням кількості фішингових атак через електронну пошту[29]. Незважаючи на серйозну загрозу, яку фішинг становить сьогодні для компаній та користувачів, більшість компаній проводять тренінги з протидії фішингу для своїх співробітників лише один раз на рік. Така недостатня освіта є ключовим чинником, через який фішинг залишається основною загрозою, що може призвести до витоку даних. За даними "Dbir Verizon" за 2021 рік, приблизно 25% усіх витоків даних мають зв'язок з фішингом, а 85% витоків даних пов'язані з людським фактором. Це підтверджується дослідженнями Центру скарг на злочини в Інтернеті (IC3), який зафіксував рекордну кількість скарг від американських громадян у 2020 році. У США того року 241 342 людини стали жертвами фішингу, що призвело до невиплати або недоставки товарів, вимагань, витоків персональних даних, та крадіжки особистих даних[30].

Середній показник спроб компрометації корпоративної електронної пошти (BEC) значно зріс на 15% між другим і третім кварталами року. Частіше

спостерігаються витоки даних, спричинені крадіжкою облікових даних, а не інсталяцією шкідливого програмного забезпечення[31]. За інформацією від "IBM", кожна компанія, що зазнала витоку даних у 2021 році, постраждала від втрати або крадіжки облікових даних, при цьому 17% були атаковані через безпосередні фішингові атаки[32]. Однак дані "Google Safe Browsing" свідчать, що зараз у Інтернеті майже в 75 разів більше фішингових сайтів, ніж шкідливих [33]. За даними, представленими на рис. 3.1, спостерігається значне збільшення фішингових атак у фінансовому секторі, зокрема в банківській сфері, які становили 23,2% від загальної кількості фішингових атак. Щодо криптовалюти, атаки на криптовалютні біржі та гаманці складали близько 6,5% від усіх атак. Рисунок 3.1. також
показує зростання фішингових атак у сфері електронної комерції, особливо в роздрібній торгівлі.

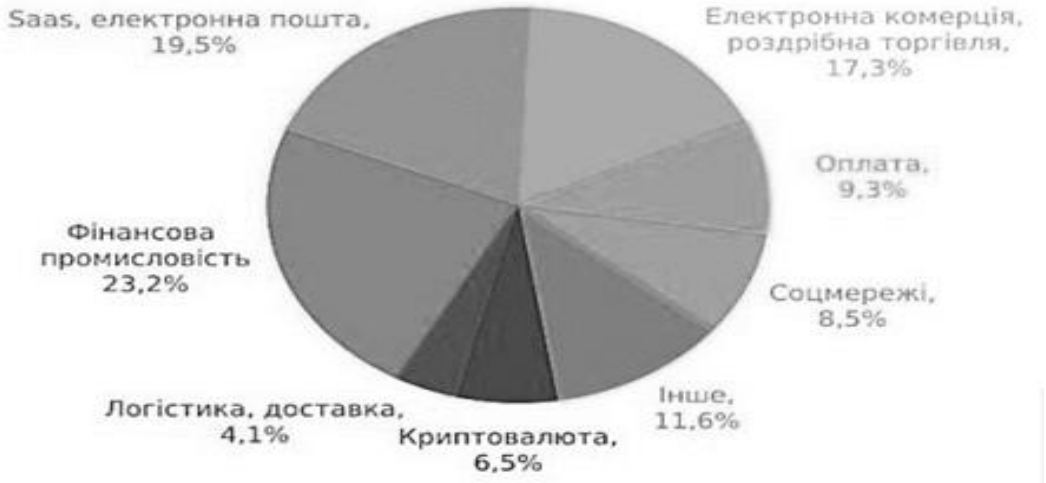

Рис.3.1. Найбільш вразливі промислові галузі

Розуміючи методи, які використовуються для маніпулювання людьми, фактори, які роблять людей вразливими, та потенційні наслідки маніпуляцій, можемо краще підготуватися до того, щоб захистити себе та інших від їхнього шкідливого впливу. Можемо розвивати навички критичного мислення, усвідомлювати когнітивні упередження, скептично ставитися до інформації від

авторитетних осіб, звертати увагу на свої емоції та шукати різноманітні джерела інформації. Здійснюючи ці проактивні кроки, приймати поінформовані рішення, брати участь у конструктивному діалозі та будувати більш стійке і справедливе суспільство.

3.2 Методика захисту від маніпулювання людьми для отримання доступу до інформації

Методика: Сукупність прийомів і способів, які використовуються для досягнення певної мети. Методика може включати в себе різні методи, такі як психологічні прийоми, технічні інструменти, і організаційні заходи.

Методи: Конкретні дії, які використовуються в рамках методики. Методи можуть бути як простими, так і складними, і можуть залежати від конкретної ситуації і мети, яку необхідно досягти. Таким чином, методика може бути розкрита через методи, як послідовність кроків для виконання такої важливої задачі як дослідження визначеної мети відповідно до її теми.

Методика захисту від маніпулювання людьми для отримання доступу до інформації охоплює **комплексний підхід**, що включає **розробку стратегії безпеки, освіту та підвищення обізнаності співробітників, технічні заходи безпеки, політику доступу до даних та планування відповіді на інциденти**[32]. Цей підхід передбачає **визначення ключових інформаційних активів і потенційних загроз**, а також ***розробку політик і процедур для управління ризиками***. Особливий акцент робиться на регулярне навчання персоналу з питань безпеки інформації, включаючи навички розпізнавання фішингових атак та інших методів маніпуляції.

В технічному плані важливими є впровадження шифрування даних, двофакторної аутентифікації, використання брандмауерів та антивірусного програмного забезпечення, а також налагодження систем моніторингу та виявлення вторгнень. Важливу роль відіграє і політика доступу до даних, яка базується на принципі найменшого привілею, із строгим контролем та періодичним переглядом доступу до систем і даних. І, нарешті, розробка ефективного плану реагування на інциденти, що включає процедури

повідомлення, ізоляції загроз та відновлення систем, є ключовим для мінімізації наслідків в разі витоку або маніпуляції даними.

У **розробці стратегії захисту** для компанії на кшталт "Monobank" від маніпулювання людьми з метою отримання доступу до інформації, важливо зосередитись на комплексному підході, який охоплює як організаційні, так і технічні заходи. Враховуючи, що Monobank є цифровим банком, особлива увага має бути приділена захисту онлайн транзакцій і зберігання даних клієнтів.

Першочергово, важливо **створити міцну корпоративну культуру**, де кожен співробітник усвідомлює свою роль і відповідальність у забезпеченні безпеки інформації. Регулярні тренінги і освітні програми з безпеки інформації допомагають підвищити рівень обізнаності персоналу щодо потенційних кіберзагроз, таких як фішинг, шахрайство чи інші види маніпулювання. Особливу увагу слід приділити навчанню працівників розпізнавати спроби соціальної інженерії та адекватно на них реагувати[43].

З технічного боку, важливо забезпечити впровадження надійних заходів безпеки, таких як багатофакторна аутентифікація для доступу до корпоративних систем і клієнтських акаунтів. Використання сильного шифрування для захисту даних, які передаються та зберігаються, є ключовим у запобіганні витоків інформації. Також необхідно **регулярно проводити аудити безпеки та оновлювати захисні системи, щоб вони відповідали сучасним викликам у сфері кібербезпеки**. Розробка ефективного плану реагування на інциденти також має велике значення. Це включає в себе чітке визначення процедур для виявлення, реагування та відновлення після інцидентів безпеки. Важливо, щоб усі співробітники були обізнані з цими процедурами і знали, як діяти в разі виявлення підозрілої активності або потенційної атаки.

Крім того, в контексті цифрового банкінгу, необхідно **регулярно інформувати клієнтів про потенційні ризики та навчати їх основам кібергігієни.** Це може включати комунікації щодо безпечного використання онлайн банкінгу, розпізнавання шахрайських схем і важливості збереження конфіденційності їхніх даних. Інтегруючи ці заходи в загальну стратегію безпеки, Monobank може значно знизити ризики, пов'язані з маніпулюванням людьми для отримання доступу до інформації, та підвищити рівень довіри та

безпеки як серед своїх співробітників, так і серед клієнтів.

Говорячи про безпеку інформації в університетському навчанні, часто маємо на увазі **технічні засоби захисту**, але занадто часто забуваємо про найуразливіший елемент цієї системи – людину [43]. У дослідженні прагнемо розглянути це питання, дослідити можливості отримання інформації з індивіда за різними шляхами, проаналізувати їх і розробити методи протидії.

Вважається, що ці методи є важливими для керівників різних компаній, які мають навчити своїх співробітників, або принаймні ознайомити їх із можливими загрозами. Крім комерційного використання, отримана інформація також буде корисною для звичайних громадян.

У більшості випадків індивід просто не розуміє, що надає цінну або потенційно цінну інформацію. Будь-яка перспективна особа, яка володіє цікавою інформацією, може виступати як об'єкт використання. Індивід, демонструючи певні реакції, піддається впливу спонукань, і розуміння цього дає можливість використовувати його слабкі місця для отримання необхідних даних, навіть без його усвідомлення.

Професійний маніпулятор, подібний до детектива, використовує **різноманітні методи**, такі як **спостереження, експерименти та аналіз, для виявлення слабких місць своєї жертви**. Виходячи з цього, обирається **оптимальний спосіб маніпуляції**, а **об'єкт вивчається** таким чином, щоб **виявити його слабкі сторони**. **Мотиви**, що можуть слугувати ключами до об'єкта, включають ***жадібність, страх, фактор болю, сексуальну емоційність, байдужість, внутрішній авантюризм, рахунки з конкретними особами, націоналізм, громадянський обов'язок, загальнолюдську мораль, підсвідому потребу в самоповазі, симпатію до одержувача або його справи, марнославство.*** **Маніпуляція** - це важкий метод, використовуваний для впливу на щось під час ручної роботи. У вузькому сенсі це може бути витівкою або махінацією, але таке визначення

не охоплює всю сутність цього явища. **Маніпуляція** завжди гра на наших почуттях та емоціях, спрямована на досягнення конкретної мети. **Об'єктами маніпуляції** часто стають[27]:

- Наша неінформованість або нерозуміння маніпуляцій;

- Наші мрії, бажання та цілі;

- Почуття провини, страху та заздрості;

- Наші слабкості та нестійкість особистості;

- Стереотипи;

- Особливості психології людської поведінки.

Існують **три види маніпуляцій**: навіювання, переконання та шантаж. Переконання спрямоване на раціональне мислення, навіювання проникає в субсидію обійти свідомість, а шантаж викликає стрес, спрямовуючи свідомість в нестабільний стан.

Якщо виявили спроби маніпуляції, важливо запитати: "Навіщо ви це говорите?" або "Чого ви хочете досягти своїми словами?" Це допомагає розкрити маніпуляцію. Важливо бути непередбачуваним, оскільки маніпулятор вивчає свою жертву та розкривається раціональним

осмисленням. Слід зберігати спокій та холодний розум, не піддаватися психологічному тиску, не відкривати душу незнайомим людям та навчатися говорити "ні". Важливо витрачати зусилля на підготовку до протидії маніпуляціям, так само як і на захист інформації від технічних загроз[16]. Але жодні **технічні заходи захисту інформації** не забезпечать ефективного захисту від соціальної інженерії. Причина полягає в тому, що **соціальні інженери використовують невразливість нетехнічних інструментів та "людський фактор".** У цьому контексті неперервна та відповідна робота з персоналом є єдиним ефективним засобом протистояння соціальним інженерам.

Для підвищення безпеки організації важливо систематично проводити спеціальну підготовку, постійно контролювати рівень знань працівників, виконувати тести та внутрішні саботажі для виявлення рівня підготовки працівників в реальних умовах.

Суттєвим аспектом у навчанні користувачів є усвідомлення, що **навчання - це циклічний процес, який слід регулярно повторювати з часом**.

Форма навчання може включати теоретичні заняття, практикуми, онлайн-семінари та рольові ігри (моделювання атак). Для розробки методології навчання персоналу важливо розуміти, чому люди вразливі до атак. Обговорення цих тенденцій може допомогти працівникам усвідомити, як соціальні інженери

можуть маніпулювати людьми.

Маніпуляція, як метод впливу, вивчається соціологами протягом 50 років. Роберт Чалдіні, відомий експериментальний соціальний психолог, визначив шість "рис людської природи", які соціальні інженери успішно використовують для маніпуляцій. **Ключові методи включають використання авторитету та можливостей групового впливу для задоволення попиту людини або створення видимої схожості.**

Люди мають тенденцію дотримуватися своїх обіцянок (**наприклад,** зловмисник може звертатися до нового співробітника, раджуючи йому прочитати політику та процедури безпеки, позначаючи це як обов'язковий крок для отримання доступу до інформаційних систем компанії. Коли користувач видає свій пароль, абонент пораджує йому створити більш надійні паролі, діючи, як інструктор[32]. Працівник може також припускати, що той, хто телефонує, вже погодився дотримуватися угоди). Зазвичай люди відчувають себе частиною своєї соціальної групи. Дії інших членів групи служать гарантією дійсної поведінки (наприклад, абонент пропонує перевірити та назвати імена інших членів служби, які з ним спілкуються. Жертва припускає, що інші імена належать дійсним працівникам служби. Зловмисник може потім ставити будь-які питання та використовувати отриману інформацію для злочинних цілей).

Розробка стратегій протидії соціальній інженерії має початися зі створення групи, відповідальної за безпеку. Ці співробітники повинні нести відповідальність за розробку політики та процедур безпеки для захисту окремих працівників та мережі організації. Група повинна представляти різні відділи.

Обов'язки цієї групи повинні включати:

1) Забезпечення підтримки політики та процедур безпеки.

2) Допомога в розробці навчальних матеріалів для персоналу.

Відповідальний за розробку програм інформаційної безпеки повинен визначити конкретні вимоги для різних груп працівників, які мають справу з обробкою даних в організації. Тренінги повинні бути проведені для різних категорій працівників, таких як менеджери, IT-персонал, користувачі комп'ютерів, обслуговуючий персонал тощо. Посібники з технічного навчання повинні включати демонстрацію соціальної інженерії через рольові ігри та перегляд

повідомлень у ЗМІ про останні атаки на інші організації.Відповідальний за розробку програми інформаційної безпеки повинен визначити конкретні вимоги для різних груп співробітників, які працюють з інформацією організації. Навчання повинно охоплювати такі групи персоналу[42]:

1. Менеджери;
2. IT співробітники;
3. Користувачі ПК;
4. Обслуговуючий персонал;
5. Адміністратори та їх асистенти;
6. Охоронці (з коротким навчальним курсом).

Технічні засоби навчання повинні включати:

- Демонстрацію соціальної інженерії через рольові ігри;
- Огляд подій ЗМІ щодо останніх атак на інші організації;
- Обговорення стратегій запобігання втраті інформації.

Організація має не лише встановлювати політику безпеки, але й заохочувати співробітників, які працюють з інформацією компанії чи комп'ютерними системами, ретельно вивчати та дотримуватися цієї політики. Забезпечення розуміння причин прийняття певних положень у регламенті допоможе уникнути обходу правил з метою особистого вигоди. Технічний захист може включати засоби запобігання отриманню та використанню інформації, і він поділяється на групи залежно від реалізації.Технічний захист може включати різноманітні засоби для запобігання отриманню та використанню інформації. З точки зору запобігання навмисним діям, ці заходи можна класифікувати в різні групи.

До технічних (апаратних) засобів входять різні пристрої, такі як механічні, електромеханічні та електронні, які розв'язують проблему захисту даних шляхом використання апаратних рішень. Ці пристрої можуть запобігати фізичним вторгненням або, якщо втручання вже сталося, обмежувати доступ до інформації та приховувати її. Наприклад, замки, решітки на вікнах та охоронні сигналізації розв'язують перший аспект проблеми, тоді як генератори шуму, мережеві фільтри та інші пристрої "блокують" потенційні канали витоку інформації або виявляють їх. Технічні засоби мають переваги в надійності, незалежності від

суб'єктивних факторів та високій стійкості до модифікацій. Однак вони можуть бути менш гнучкими, великими та важкими, і їм може бракувати гнучкості, а також вони можуть вимагати значних витрат.

До програмних засобів належать програми для ідентифікації користувачів, контролю доступу, шифрування інформації, видалення залишкової інформації тощо. Програмне забезпечення має переваги універсальності, гнучкості, надійності та простоті установки, і його можна легко модифікувати та розвивати. Однак у нього може бути обмежена функціональність мережі, висока чутливість до випадкових або навмисних змін, і воно може залежати від типів комп'ютерів та їх обладнання.

Актуальні проблеми соціальної інженерії в організації ПрАТ "НЕК "Укренерго".

Соціальна інженерія - це тип атаки, який спирається на людську взаємодію, щоб обманом змусити жертву розкрити конфіденційну інформацію або вчинити дії, які ставлять під загрозу її безпеку. Організації будь-якого розміру вразливі до атак соціальної інженерії, і ПАТ "НЕК "Укренерго" не є винятком.

За даними веб-сайту ПАТ "НЕК "Укренерго", в компанії працює понад 20 000 співробітників. Така велика кількість працівників робить її першочерговою мішенню для атак соціальної інженерії.

ПАТ "НЕК "Укренерго" є організацією критичної інфраструктури, яка відповідає за передачу електроенергії в Україні. Це робить організацію високоцінною мішенню для кібератак, в тому числі і для атак соціальної інженерії.

ПАТ "НЕК "Укренерго" протягом останніх років зазнало низки атак соціальної інженерії. Ці атаки призвели до викрадення конфіденційних даних, порушення операційної діяльності та втрати грошових коштів.Серед найпоширеніших методів соціальної інженерії, що застосовуються проти ПАТ "НЕК "Укренерго", можна виділити наступні:

· Фішингові електронні листи: Фішингові листи - це електронні листи, які надсилаються з начебто легітимного джерела, щоб обманом змусити одержувачів перейти за шкідливим посиланням або відкрити заражене вкладення.

· Вішинг: Вішинг - це різновид соціальної інженерії, який використовує телефонні дзвінки, щоб обманом змусити жертву розкрити конфіденційну інформацію або вжити заходів, які ставлять під загрозу її безпеку.

· Претекстинг (від англ. pretexting): Це метод соціальної інженерії, який полягає у створенні хибного приводу для отримання доступу до конфіденційної інформації або для того, щоб переконати когось здійснити дію, яку він не зробив би за інших обставин.

Компанія зробила деякі кроки для зменшення ризику атак соціальної інженерії, зокрема:

1. Навчання співробітників тому, як виявляти та уникати атак соціальної інженерії.

2. Впровадження засобів контролю безпеки для захисту конфіденційних даних.

3. Проведення регулярних аудитів безпеки.

Однак компанія все ще стикається з низкою викликів у запобіганні атакам соціальної інженерії. До таких викликів відносяться: Велика кількість співробітників, яких компанія повинна навчити. · Складність відстеження нових методів соціальної інженерії. Той факт, що соціальні інженерні атаки часто покладаються на людський фактор, який буває важко контролювати. ПАТ "НЕК "Укренерго" має продовжувати інвестувати в навчання та заходи безпеки, щоб захиститися від атак соціальної інженерії. Компанія також має розглянути можливість впровадження додаткових заходів безпеки, таких як багатофакторна автентифікація, для подальшого посилення свого захисту. Методика захисту від маніпулювання людьми для отримання доступу до інформації включає в себе два основних напрямки:

· Зменшення цифрового сліду

· Інформаційна гігієна

Зменшення цифрового сліду

Цифровий слід - це інформація про користувача, яку він залишає в Інтернеті. Цифровий слід може включати в себе такі дані:

· Імена користувачів та паролі

· Історія відвідувань веб-сайтів

· Фотографії та відео

· Коментарі та пости в соціальних мережах

Зловмисники можуть використовувати цифровий слід для маніпулювання людиною. Наприклад, вони можуть використовувати інформацію про імена користувачів та паролі для отримання несанкціонованого доступу до облікових записів користувача. Або вони можуть використовувати інформацію про інтереси та уподобання користувача для створення персоналізованих атак.

Для зменшення цифрового сліду користувач може вжити таких заходів:

· Використання різних імен користувачів та паролів для різних веб-сайтів і додатків

· Відключення функції автозаповнення в браузері

· Використання анонімних мереж, таких як Tor

· Видалення непотрібної інформації з соціальних мереж

Інформаційна гігієна

Інформаційна гігієна - це комплекс заходів, спрямованих на захист від шкідливої інформації. До заходів інформаційної гігієни відносяться такі: · Критичне ставлення до інформації, отриманої з Інтернету · Не поширювати інформацію, джерело якої невідомо

· Не відкривати електронні листи або інші повідомлення від незнайомих відправників

· Не публікувати в Інтернеті особисту інформацію, яка може бути використана для маніпулювання

Критичне ставлення до інформації означає, що користувач повинен бути обережним і не довіряти всім джерелам інформації. Користувач повинен перевіряти інформацію з різних джерел, перш ніж її використовувати.

Не поширення інформації, джерело якої невідомо, також є важливим заходом захисту від маніпулювання. Зловмисники можуть поширювати неправдиву інформацію з метою дезінформації людей. Користувач повинен бути обережним і не поширювати інформацію, джерело якої невідомо.

Не відкриття електронних листів або інших повідомлень від незнайомих відправників також є важливим заходом захисту від маніпулювання. Зловмисники можуть використовувати електронні листи або інші повідомлення

для розповсюдження шкідливого програмного забезпечення або для обману людей з метою отримання їх особистої інформації.

Не публікація в Інтернеті особистої інформації, яка може бути використана для маніпулювання, також є важливим заходом захисту. Зловмисники можуть використовувати особисту інформацію людей для створення персоналізованих атак. Користувач повинен бути обережним і не публікувати в Інтернеті особисту інформацію, яка може бути використана для маніпулювання.

Виконання цих заходів може допомогти користувачам захиститися від маніпулювання людьми для отримання доступу до інформації.

Висновки до третього розділу. Висновки до третього розділу "Розробка рекомендацій по захисту від маніпулювання людьми для отримання доступу до інформації" відображають глибоке розуміння складності проблеми та потреби в інтегрованому підході. Аналіз досвіду показав, що маніпулювання людьми є значною загрозою в сучасному цифровому світі, особливо у сфері кібербезпеки. Це вимагає постійної уваги та адаптації стратегій безпеки.

Розроблені методики та рекомендації наголошують на важливості комплексного підходу, що включає як організаційні, так і технічні аспекти. Освітні програми для співробітників, ефективні технологічні рішення для захисту даних, регулярний моніторинг та аудит систем, а також розробка детальних планів реагування на інциденти є ключовими елементами захисту від маніпулювання. З огляду на це, кожна організація, включаючи "Monobank", повинна розробляти та впроваджувати цілісну стратегію захисту від маніпуляцій, що враховує як внутрішні, так і зовнішні виклики сучасного цифрового ландшафту.

ВИСНОВКИ

У результаті дослідження визначено, що маніпулювання для отримання доступу до інформації є актуальною та серйозною проблемою у сучасному світі. Зловмисники використовують різноманітні методи, такі як соціальна інженерія та використання шкідливих програм, щоб досягти своїх цілей. Це може призвести до серйозних наслідків, таких як витік конфіденційної інформації чи фінансові збитки.

В рамках проведеного дослідження були визначені методи атак та розроблені стратегії захисту від маніпулювання людьми для отримання доступу до інформації. Методи атак включають експлуатацію вразливостей у людській

психології, використання шкідливих програм та соціальну інженерію. Ці атаки можуть спричинити надзвичайно негативні наслідки, такі як втрата конфіденційності чи фінансові втрати.

Мета дослідження полягала в розробці методів атаки та захисту від маніпулювання людьми для отримання доступу до інформації. У результаті дослідження були розроблені рекомендації щодо захисту від маніпулювання людьми для отримання доступу до інформації. Ці рекомендації включають в себе такі заходи, як зменшення цифрового сліду, дотримання правил інформаційної гігієни та підвищення обізнаності користувачів про методи і техніки маніпулювання людьми.

Завдання дослідження були наступними:

Проаналізувати теоретичні основи дослідження маніпулювання людьми. Це завдання було досягнуто, оскільки в дослідженні було проаналізовано теоретичні основи дослідження маніпулювання людьми.

Охарактеризувати типи загроз для кібербезпеки та види атак, які можуть використовуватися для маніпулювання людьми. Це завдання було досягнуто, оскільки в дослідженні було охарактеризовано типи загроз для кібербезпеки та види атак, які можуть використовуватися для маніпулювання людьми.

Розглянути методи захисту від маніпулювання людьми для отримання доступу до інформації. Це завдання було досягнуто, оскільки в дослідженні було розглянуто методи захисту від маніпулювання людьми для отримання доступу до інформації.

Розробити рекомендації щодо захисту від маніпулювання людьми для отримання доступу до інформації. Це завдання було досягнуто, оскільки в дослідженні було розроблено рекомендації щодо захисту від маніпулювання людьми для отримання доступу до інформації.

Серед запропонованих заходів захисту від маніпулювання, важливість зменшення цифрового сліду визначається обережним ставленням до особистої інформації в Інтернеті. Крім того, інформаційна гігієна та освіта важливі для формування критичного мислення та усвідомленості щодо методів маніпуляції.

Захист від маніпулювання людьми для отримання доступу до інформації є

критично важливим аспектом загальної безпеки, і подальші дослідження можуть сприяти розробці ефективних заходів захисту та вдосконаленню відповідних стратегій. Аналіз досвіду показав, що виклики в кібербезпеці вимагають як організаційних, так і технічних стратегій. Наголошується на значенні освітніх програм для співробітників, застосуванні передових технологій для захисту даних, та розробці ефективних планів реагування на інциденти. Цілісна стратегія захисту є ключовою для організацій у сучасному цифровому середовищі.

Рекомендації щодо захисту від маніпулювання людьми для отримання доступу до інформації:

· Зменшення цифрового сліду: користувач повинен бути обережним у тому, яку інформацію він залишає в Інтернеті.

· Інформаційна гігієна: користувач повинен критично ставитися до інформації, яку він отримує з Інтернету, і не поширювати інформацію, джерело якої невідомо.

· Освіта: користувачі повинні бути поінформовані про методи і техніки маніпулювання людьми, щоб бути більш обережними і не піддаватися обману.

· Використання надійних антивірусних програм: антивірусні програми можуть допомогти захистити комп'ютер від шкідливих програм, які можуть використовуватися для маніпулювання людьми.

· Використання брандмауерів: брандмауери можуть допомогти захистити комп'ютер від несанкціонованого доступу.

· Оновлення програмного забезпечення: зловмисники часто використовують вразливості в програмному забезпеченні для проведення атак. Важливо регулярно оновлювати програмне забезпечення, щоб усунути ці вразливості.

Перспективи подальших досліджень:

· Розробка більш ефективних методів захисту від маніпулювання людьми для отримання доступу до інформації.

· Дослідження впливу маніпулювання людьми на кібербезпеку. · Розробка освітніх програм для підвищення обізнаності про методи і техніки маніпулювання людьми.

Проведене дослідження є актуальним і важливим для підвищення рівня

кібербезпеки. Розроблені рекомендації можуть допомогти користувачам захиститися від маніпулювання людьми для отримання доступу до інформації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Сугестивні технології маніпулятивного впливу : навч. посіб. / [В.М.Петрик, М.М.Присяжнюк, Л.Ф.Компанцева та ін.] ; за заг. ред. Є.Д.Скулиша. – К., 2010.С 10
2. Бабак В.П., Корченко О.Г. Інформаційнабезпека та сучаснімережевітехнології. Англ.-укр.- рос. слов. термінів. − К.: НАУ, 2003. − 670 с.
3. Бурячок В. Л., Корченко О. Г., Бурячок Л. В. Social engineering as a method of information and telecommunication systems intelligence. *Ukrainian information security research journal*. 2012. Vol. 14, no. 4 (57). URL: https://doi.org/10.18372/2410-7840.14.3471 (date of access: 30.11.2023).

4. Ванацький Д. І. Соціальна інженерія. *Вісник Київського інституту бізнесу та технологій*. 2018. Вип. № 2 (36). С. 26.

5. Гелюх М. Інформаційна гігієна: навіщо потрібна та як не стати жертвами фейків. *UA.NEWS*. URL: https://ua.news/ua/technologies/informatsionnaya-gigiena-zachem-nuzhna-i-kak-ne-stat-zhertvami-fejkov (дата звернення: 29.11.2023).

6. Думчиков М. О., Думчиков М. А., Dumchykov M. O. Кібератаки як новітня загроза інформаційній безпеці : thesis. 2020. URL: https://essuir.sumdu.edu.ua/handle/123456789/77915 (дата звернення: 03.12.2023).

7. Інформаційна безпека : thesis / А. В. Булашенко та ін. 2010. URL: http://essuir.sumdu.edu.ua/handle/123456789/21090 (дата звернення: 30.11.2023).

8. Інформаційна гігієна : thesis / Л. О. Колісник та ін. 2011. URL: http://essuir.sumdu.edu.ua/handle/123456789/13171 (дата звернення: 30.11.2023).

9. Кавун С. В. Інформаційна безпека : підручник. Харків : ХНЕУ, 2009. 368 с.

10. Конхіді Ш. Соціальна інженерія в галузі IT-безпеки: інструменти, тактика та методи / Конхіді Ш. – McGraw-Hill Education, 2014. – 272 с.

11. Класифікація методів соціальногоінжинірингу / О.Г. Корченко, Є.В. Паціра, Д.А. Горніцька // Захист інформації. – 2007. – №4 (36). – С.37-45.

12. Мітник К. Мистецтво обману / К. Мітник. – John Wiley& Sons, 2002. – 304 с.

13. Оніщенко Н. Інформаційна безпека як складова розвитку сучасного інформаційного суспільства: питання правового забезпечення. *Problemas y perspectivasde la aplicaciónde la investigacióncientíficainnovadora*. 2021. URL: https://doi.org/10.36074/logos-11.06.2021.v1.19 (дата звернення: 30.11.2023).

14. Суббот А. Інформаційна безпека суспільства. *Віче*. 2015. № 8 (388). С. 29–31.

15. Сучасні аспекти кібербезпеки в контексті глобальних загроз : thesis / М. О. Думчиков та ін. 2020. URL: https://essuir.sumdu.edu.ua/handle/123456789/78666 (дата звернення: 30.11.2023).

16. Соціальна інженерія [Електронний ресурс] - Режим доступу: http://studies.in.ua/lekciisociologija/4443-socalna-nzhenerya.html

17. СОЦІАЛЬНА ІНЖЕНЕРІЯ - МЕТОДИКА МАНІПУЛЮВАННЯ ШИРОКИМИ МАСАМИ ЛЮДЕЙ [Електронний ресурс] - Режим доступу: http://uk.ruarrijoseph.com/obschestvo/ 72810- socialnaya-inzheneriya-metodika-manipulirovaniya-shirokimi-massami-lyudey.html

18. Шалопутов В. Д., Шурхно С. Цифровий слід людства : thesis. 2010. URL: http://essuir.sumdu.edu.ua/handle/123456789/21122 (дата звернення: 30.11.2023).

19. Російські кібероперації аналітика за перше півріччя 2023року.- Режим доступу: https://cip.gov.ua/ua/news/zmina-taktik-cilei-i-spromozhnostei-khakerskikh-grup-uryadu-rf-ta-kontrolovanikh-nim-ugrupovan-prognozi.

20. ClassificationMethod for Network Security Data Based on Multi-featuredExtraction / Y. Kangetal. *International Journal on Artificial Intelligence Tools*. 2021. Vol. 30, no. 01. P. 2140006. URL: https://doi.org/10.1142/s0218213021400066 (date of access: 30.11.2023).

21. CristoperHadnagy. Social Engineering. The art of Human Hacking. Wiley Publishing, Inc.,2011 – 477 p

22. Kotukh Y. Types of power relations in cybersecurity strategy. *Investytsiyi: praktykatadosvid*. 2021. No. 11. P. 98. URL: https://doi.org/10.32702/2306-6814.2021.11.98 (date of access: 30.11.2023).

23. Krebs B. StateGovts. WarnedofMalware-Laden CD SentViaSnailMailfromChina [Електронний ресурс] / BrianKrebs // KrebsonSecurity. – 2018. –

Режим доступу до ресурсу: https://krebsonsecurity.com/2018/07/state-govts-warned-of-malware-laden-cd-sent-via-snail-mail-from-china/.

24. Lee T., Jia C. Curse or cure? The role of algorithm in promoting or countering information disorder. *Information disorder*. London, 2023. P. 29–45. URL: https://doi.org/10.4324/9781003299936-2 (date of access: 30.11.2023).

25. Legal Support of Cybersecurity of Critical Information Infrastructure of Ukraine / M. Kovalivetal. *Path of Science*. 2021. Vol. 7, no. 4. P. 2011–2018. URL: https://doi.org/10.22178/pos.69-12 (date of access: 30.11.2023).

26. Maymí F. J. Cybersecurity. *SIGITE '19: The 20th Annual Conference on Information Technology Education*, Tacoma WA USA. New York, NY, USA, 2019. URL: https://doi.org/10.1145/3349266.3355613 (date of access: 30.11.2023).

27. Method engineering as a social practice / B. Henderson-Sellersetal. *Situational method engineering*. Berlin, Heidelberg, 2013. P. 53–68. URL: https://doi.org/10.1007/978-3-642-41467-1_3 (date of access: 30.11.2023).

28. Model of transformation of the national cybersecurity system in the conditions of hybrid threats / R. M. Boyarchuketal. *Modern information security*. 2020. Vol. 41, no. 1. P. 6–10. URL: https://doi.org/10.31673/2409-7292.2020.010610 (date of access: 30.11.2023).

29. Roy J. Cybersecurity. *Public Administration and Information Technology*. New York, NY, 2013. P. 59–68. URL: https://doi.org/10.1007/978-1-4614-7221-6_5 (date of access: 30.11.2023).

30. Robust Email Security Requires Alignment Between Security Practitioners and Decision Makers [Електронний ресурс] // Osterman Research.– 2020. – Режим доступу до ресурсу: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWIy Sx.

31. DBIR 2021 Data Breach Investigation Report [Електронний ресурс] // Verizon. – 2021. – Режим доступу до ресурсу: https://www.verizon.com/business/resources/reports/2021-data-breach-investigations- report.pdf.

32. Abonormal Security Quarterly BEC Report. [Електронний ресурс] / Evan Reiser // Abnormal Security. – 2020. – Режимдоступу до ресурсу: https://info.abnormalsecurity.com/rs/231IDP139/images/AS_Qtrly_BEC_Report_Q3_2 020.pdf.

33. Cost of a Data Breach Report 2021 [Електронний ресурс] // IBM Security. – 2020. – Режим доступу до ресурсу: https://www.ibm.com/downloads/cas/OJDVQGRY.

34. Google Safe Browsing Service of Google that helps protect devices. [Еле- ктронний ресурс] // Google. – 2022. – Режим доступу до ресурсу: https://transparencyreport.google.com/safe-browsing/overview.

35. Sokolovsky S. P. Information systems proactive protection suiteagainstnetwork reconnaissance. *Vestnikkomp'iuternykh i informatsionnykhtekhnologii*. 2021. No. 209. P. 53–62. URL: https://doi.org/10.14489/vkit.2021.11.pp.053-062 (date of access: 30.11.2023).

36. T. Aston. Modeling the socialreinforcement of misinformationdissemination on socialmedia. *SCIRP*. URL: https://www.scirp.org/journal/paperinformation.aspx?paperid=121022#:~:text=The%20magnitude%20of%20false%20intel,intent%20to%20deceive%20[3]. (date of access: 29.11.2023).

37. Thakur K., Pathan A.-S. K. Types of computer malware. *Cybersecurityfundamentals*. 2020. P. 77–97. URL: https://doi.org/10.1201/9781003035626-5 (date of access: 30.11.2023).

38. Thakur K., Pathan A.-S. K. Types of cyberattacks. *Cybersecurityfundamentals*. 2020. P. 41–57. URL: https://doi.org/10.1201/9781003035626-3 (date of access: 30.11.2023).

39. United States. Congress. House. Committee on Homeland Security. Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology. Addressing the nation'scybersecuritychallenges: Reducingvulnerabilitiesrequiresstrategicinvestment and immediateaction

:hearingbefore the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology of the Committee on Homeland Security, House of Representatives, One HundredTenthCongress, April 25, 2007. Washington : U.S. G.P.O., 2009. 47 p.

40. Wang S., Wang H. Opportunities and Challenges of Cybersecurity for Undergraduate Information Systems Programs. *International Journal of Information and Communication Technology Education*. 2019. Vol. 15, no. 2. P. 49–68. URL: https://doi.org/10.4018/ijicte.2019040104 (date of access: 30.11.2023).

41. Watson G. The techniques of manipulation. *Social engineeringpenetration testing*. 2014. P. 39–63. URL: https://doi.org/10.1016/b978-0-12-420124-8.00003-x (date of access: 30.11.2023).

42. Ways to reduce the «carbonfootprint» of diesel vehicles / A. Rossokhinetal. *Transportation research procedia*. 2022. Vol. 61. P. 224–228. URL: https://doi.org/10.1016/j.trpro.2022.01.037 (date of access: 30.11.2023).

43. Zukis B. Information Technology and CybersecurityGovernance in a Digital World. *The Handbook of Board Governance*. Hoboken, NJ, USA, 2016. P. 555–573. URL: https://doi.org/10.1002/9781119245445.ch28 (date of access: 30.11.2023).

44. Andress J., Winterfeld S. Computer networkattack. Cyberwarfare. 2011. P. 167–178. URL: https://doi.org/10.1016/b978-1-59749-637-7.00009-5 (date of access: 05.12.2023).

45. Balzacq T., Cavelty M. D. A theory of actor-network for cyber-security. Europeanjournal of international security. 2016. Vol. 1, no. 2. P. 176–198. URL: https://doi.org/10.1017/eis.2016.8 (date of access: 03.12.2023).

46. Digital medialiteracy: what is clickbait?. GCFGlobal.org. URL: https://edu.gcfglobal.org/en/digital-media-literacy/what-is-clickbait/1/#:~:text=They're%20just%20a%20small,to%20your%20emotions%20and%20curiosity. (date of access: 04.12.2023).

47. ENISA threat landscape 2020: cyber attacks becoming more sophisticated, targeted, widespread and undetected. ENISA. URL: https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-

2020#:~:text=During%20the%20pandemic,%20cyber%20criminals,This%20is%20not%20new. (date of access: 03.12.2023).

48. Fakiha B. Business organization security strategies to cybersecurity threats. International journal of safety and securityengineering. 2021. Vol. 11, no. 1. P. 101–104. URL: https://doi.org/10.18280/ijsse.110111 (date of access: 02.12.2023).

49. Hryshchuk O. M., Hryshchuk R. V., Okhrimchuk V. V. The verification of generalizeddifferential-game model of potentially dangerous pattern of cyber-attack. Telecommunication and information technologies. 2020. Vol. 66, no. 1. P. 53–67. URL: https://doi.org/10.31673/2412-4338.2020.015367 (date of access: 02.12.2023).

50. Information security threat assessment using socialengineering in the organizational context – literature review / A. Lopesetal. Information systems and technologies. Cham, 2022. P. 233–242. URL: https://doi.org/10.1007/978-3-031-04819-7_24 (date of access: 02.12.2023).

51. Information technologies and social transformation / ed. by G. B. R, N. A. o. Engineering. Washington, D.C : National Academy Press, 1985. 173 p.

52. Kosiński J., Gontarz T., Kośla R. Cybersecurity and the handling of cyberincidents. Internal security. 2019. Vol. 10, no. 2. P. 107–128. URL: https://doi.org/10.5604/01.3001.0013.4219 (date of access: 03.12.2023).

53. Malware. VirginiaInstitute of Marine Science. URL: https://www.vims.edu/intranet/itns/gettingstarted/itsecurity/securitytips/malware/index.php#:~:text=What%20is%20it?,annoying%20software%20or%20program%20code. (date of access: 03.12.2023).

54. Pech J. Aplikacezákona a vyhlášky o kybernetickébezpečnosti na úřadechstátnísprávy : master'sthesis. 2016. URL: http://www.nusl.cz/ntk/nusl-203989 (date of access: 05.12.2023).

55. Phishing: fraudulentemails, text messages, phone calls &socialmedia | umassamherst information technology | umassamherst. UMassAmherst. URL: https://www.umass.edu/it/security/phishing-fraudulent-emails-text-messages-

phone-calls#:~:text=These%20messages%20claim%20to%20come,a%20trusted%20friend%20or%20colleague. (date of access: 05.12.2023).

56. Social engineering attacks / Y. S. Sainietal. Emerging technologies in data mining and information security. Singapore, 2022. P. 497–509. URL: https://doi.org/10.1007/978-981-19-4193-1_49 (date of access: 05.12.2023).

57. Social engineering: definition& examples | knowbe4. SecurityAwareness Training | KnowBe4. URL: https://www.knowbe4.com/what-is-social-engineering/#:~:text=Defining%20Social%20Engineering,CEO%20Fraud%20are%20all%20examples. (date of access: 05.12.2023).

58. Stapleshit with disruption after cyber-attack. InfosecurityMagazine. URL: https://www.infosecurity-magazine.com/news/staples-hit-disruption-cyberattack/#:~:text="It%20is%20important%20for%20businesses,ever-changing%20threat%20landscape." (date of access: 03.12.2023).

59. The growing need for cybersecurityriskmanagement - Difenda. Difenda. URL: https://www.difenda.com/the-growing-need-for-cybersecurity-risk-management/#:~:text=This%20includes%20both%20technical%20solutions,for%20cyber%20criminals%20to%20succeed. (date of access: 03.12.2023).

60. What is misinformation | IGI global. IGI Global: International Academic Publisher. URL: https://www.igi-global.com/dictionary/misinformation/18690#:~:text=Misinformation%20refers%20to%20false%20or,not%20recognize%20it%20as%20false.&text=Information%20that%20is%20inaccurate.&text=The%20person%20who%20spreads%20wrong,that%20the%20information%20is%20wrong.&text=An%20unintentionally%20false,%20wrong%20information. (date of access: 03.12.2023).

61. Year C. Cybersecurity year: hackingattackawarenessevery organization every person. Independently Published, 2020.

62. Đekić M. Incident response as a key factor of defense. Tehnika. 2020. Vol. 75, no. 6. P. 809–813. URL: https://doi.org/10.5937/tehnika2006809d (date of access: 05.12.2023).