Міністерство освіти і науки України

Чорноморський національний університет імені Петра Могили
(повне найменування вищого навчального закладу)

навчально-науковий медичний інститут
(повне найменування інституту, назва факультету (відділення))

кафедра психології
(повна назва кафедри (предметної, циклової комісії))

«ДОПУЩЕНО ДО ЗАХИСТУ»
Завідувач кафедри психології
_____ А. І. Яблонський
“____” листопада 2024 року

УДК: 159.922.2-053.9:004.738.5

**КВАЛІФІКАЦІЙНА РОБОТА**
на здобуття ступеня вищої освіти
магістр
(ступінь вищої освіти)

на тему: **ВПЛИВ МЕТОДІВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ НА ОСОБЛИВОСТІ ПСИХІКИ КОРИСТУВАЧІВ ІНТЕРНЕТУ ТРЕТЬОГО ВІКУ ДОРОСЛОСТІ**

Керівник: д. пед. н., професор Терентьєва Наталія Олександрівна
(вчене звання, науковий ступінь, П.І.Б.)

Рецензент: д. пед. н., професор, професор кафедри психології Національного університету біоресурсів і природокористування України Яшник Світлана Валеріївна
(посада, вчене звання, науковий ступінь, П.І.Б.)

Виконав: студентка VI курсу групи 666 М Фалько Наталія Іванівна
(П.І.Б.)

Спеціальності: 053 «Психологія»
(шифр і назва спеціальності)

ОПП: «Психологія»

Миколаїв – 2024 рік

Чорноморський національний університет імені Петра Могили
( повне найменування вищого навчального закладу )

| | |
|---|---|
| Інститут, факультет, відділення | навчально-науковий медичний інститут |
| Кафедра, циклова комісія | кафедра психології |
| Рівень вищої освіти | другий (магістерський) |
| Спеціальність | 053 «Психологія» |
| ОПП / ОНП | «Психологія» |

ЗАТВЕРДЖУЮ
Завідувач кафедри психології
_____ А. І. Яблонський
“ ” 2024 року

**З А В Д А Н Н Я**
**НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ**

**Фалько Наталії Іванівні**
(прізвище, ім’я, по батькові)

1. Тема проєкту (роботи) Вплив методів соціальної інженерії на особливості психіки користувачів Інтернету третього віку дорослості

керівник роботи: Терентьєва Наталія Олександрівна, д.пед.н., професор
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)

затверджені наказом закладу вищої освіти
від«20» вересня 2024 року № 249/1.

2. Строк подання студентом проєкту (роботи) «22 листопада 2024 року

3. Вихідні дані до кваліфікаційної роботи: вступ, основна частина, висновок, список використаних джерел та літератури, додатки.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) згідно з планом кваліфікаційної роботи магістра.

5. Перелік графічного матеріалу (з точним зазначенням обов’язкових креслень)

не планується

6. Консультанти розділів проєкту (роботи)

| Розділ | Прізвище, ініціали та посада консультанта | Підпис | |
|---|---|---|---|
| | | завдання видав | завдання прийняв |
| Вступ | Терентьєва Н.О. | | |
| Розділ 1 | Терентьєва Н.О. | | |
| Розділ 2 | Терентьєва Н.О. | | |
| Розділ 3 | Терентьєва Н.О. | | |
| Висновки | Терентьєва Н.О. | | |

7. Дата видачі завдання 26.09.2024

**КАЛЕНДАРНИЙ ПЛАН**

| № з/п | Назва етапів кваліфікаційної роботи | Строк виконання етапів проєкту (роботи) | Примітка |
|---|---|---|---|
| 1. | Вступ до кваліфікаційної роботи | вересень 2024 | |
| 2. | Розділ 1. Теоретичні основи вивчення впливу методів соціальної інженерії на особливості психіки користувачів Інтернету. | жовтень 2024 | |
| 3. | Розділ 2. Дослідження впливу соціальної інженерії на поведінку користувачів Інтернету. | жовтень 2024 | |
| 4. | Розділ 3. Теоретико-експериментальне застосування тренінгової роботи з користувачами Інтернету третього віку дорослості. | жовтень 2024 | |
| 5. | Висновки | листопад 2024 | |
| 6. | Передкваліфікаційна практика | 11.11 – 24.11. 2024 | |
| 7. | Оформлення списку використаних джерел та літератури, додатків | листопад 2024 | |
| 8. | Попередній захист | 26.11.2024 | |
| 9. | Рецензія на кваліфікаційну роботу | 17.11.2024 | |
| 10. | Захист кваліфікаційної роботи | 19.12 2024 | |

**Студент** _____ **Фалько Н.**
(підпис) (прізвище та ініціали)

**Керівник проєкту (роботи)** _____ **Терентьєва Н.О.**
(підпис) (прізвище та ініціали)

# АНОТАЦІЯ

**Фалько Н.І**. Вплив методів соціальної інженерії на особливості психіки користувачів Інтернету, зокрема третього віку дорослості

Кваліфікаційна робота на здобуття освітньо-кваліфікаційного рівня магістра за спеціальністю 053 «Психологія» Чорноморського національного університету імені Петра Могили 2024 року.

Кваліфікаційну роботу присвячено аналізу впливу методів соціальної інженерії (фішинг, вішинг, претекстинг тощо) на психологічні особливості користувачів Інтернету, досліджуються їх вразливості до маніпуляцій залежно від емоційного стану, вікових і когнітивних характеристик. Емпірично підтверджено вплив цих методів на довіру, емоційну стійкість і ухвалення рішень. Запропоновано та проведено тренінгову програму "Твій цифровий щит" для підвищення обізнаності користувачів онлайн-середовища пенсійного віку.

Об'єктом дослідження є психологічний вплив методами соціальної інженерії на користувачів Інтернету, зокрема третього віку дорослості.

В першому розділі розкрито поняття соціальної інженерії, охарактеризовані методи соціальної інженерії, здійснено аналіз наукової літератури щодо особливостей психіки та методів соціальної інженерії. Особлива увага приділена вивченню взаємозв'язку між особливостями психіки користувачів та їх вразливістю перед маніпулятивними методами, які використовуються в онлайн-середовищі. В другому розділі представлена емпірична частина теми, описані обрані методики дослідження та їх результи. Розроблені для користувачів рекомендації щодо розпізнавання та запобігання соціально-інженерним атакам. У третьому розділі розглянуто методологічні засади, зміст і процедура соціально-психологічного тренінгу. Проаналізовані та інтерпретовані результати проведення тренінгової програми “Твій цифровий щит” для користувачів Інтернету третього віку дорослості.

Практичне значення роботи полягає у розробці та апробації тренінгової програми «Твій цифровий щит», яка може бути впроваджена у навчальні курси, тренінги та консультаційні заходи для підвищення рівня цифрової безпеки користувачів пенсійного віку.

Ключові слова: соціальна інженерія, методи соціальної інженерії, психологічний вплив, користувачі Інтернету, пенсіонери, вразливості психіки.

## SUMMARY

Falko N.I. Influence of social engineering methods on the peculiarities of the psyche of Internet users, in particular the third age of adulthood

Qualification work for obtaining a master's degree in specialty 053 “Psychology” at Black Sea National University named after Petro Mohyla in 2024.

The qualification work is devoted to the analysis of the impact of social engineering methods (phishing, vishing, pretexting, etc.) on the psychological characteristics of Internet users, investigates their vulnerability to manipulation depending on their emotional state, age and cognitive characteristics. The impact of these methods on trust, emotional stability, and decision-making is empirically confirmed. The training program “Your Digital Shield” was proposed and implemented to raise awareness of users of the online environment of retirement age.

The object of the study is the psychological impact of social engineering methods on Internet users, in particular, the third age of adulthood.

The first section defines the concept of social engineering, characterizes the methods of social engineering, and analyzes the scientific literature on the peculiarities of the psyche and methods of social engineering. Particular attention is paid to the study of the relationship between the peculiarities of the psyche of users and their vulnerability to manipulative methods used in the online environment.

The second section presents the empirical part of the topic, describes the selected research methods and their results. Recommendations for users to recognize and prevent social engineering attacks are developed.

The third chapter discusses the methodological foundations, content and procedure of social and psychological training. The results of the training program “Your Digital Shield” for Internet users of the third age of adulthood are analyzed and interpreted.

The practical significance of the work lies in the development and testing of the training program “Your Digital Shield”, which can be implemented in educational courses, trainings and consulting activities to improve the level of digital security of retirement age users.

Keywords: social engineering, methods of social engineering, psychological influence, Internet users, pensioners, mental vulnerabilities.

**ЗМІСТ**

# ВСТУП

**Актуальність теми дослідження**. Сучасне суспільство переживає надзвичайно швидкий розвиток інформаційних технологій, що значно змінює спосіб комунікації та взаємодії людей. Інтернет, як один із ключових аспектів цього розвитку, став важливим чинником в побуті і діяльності сучасного індивіда. За даними дослідження, проведеного корпорацією Google, у 2023 році зафіксовано 5,18 млрд користувачів Інтернету, що відповідає 64,6% людства [4, с. 65]. Водночас, разом із зростанням використання Інтернету, зростає і вплив соціальної інженерії на особливості психіки користувачів. Соціальна інженерія, визначена як маніпулювання людськими діями, зокрема через психологічні методи, набуває нових форм та вимагає уваги як з боку дослідників, так і з боку суспільства загалом.

Спостерігається зростаюча залежність усіх сфер життєдіяльності людини від Інтернету, збільшенні кількості і видів онлайн-шахрайств, кіберзлочинів та розробки ефективних стратегій захисту. Розуміння того, які механізми використовуються в соціальній інженерії, дозволяє розробити рекомендації та інструменти для захисту користувачів від психологічних маніпуляцій, використовуючи знання та дослідження різних галузей науки, таких як психологія, соціологія, ІТ-технологія, кібербезпека. За матеріалами прес-реліза конференції «Підсумки платіжного шахрайства у 2023 році в Україні: статистика, тренди» (25 січня 2024 року) у 2023-му році відбулося 209 382 звернення громадян щодо шахрайства. Серед найпоширеніших схем онлайн-шахрайства: недоставка товару після передплати в мережі, дзвінки від імені банків, фішинг, прохання про допомогу через соцмережі [17]. Зазначене і спричинило вибір теми дослідження «Вплив методів соціальної інженерії на особливості психіки користувачів Інтернету третього віку дорослості».

**Метою** дослідження визначаємо вивчення впливу методів соціальної інженерії на особливості психіки користувачів Інтернету з подальшою

розробкою заходів для захисту та підтримки психологічного благополуччя в онлайн-середовищі для користувачів Інтернету третього віку.

**Завданнями** дослідження відповідно до мети виокремлюємо:

1. вання користувачами в Інтернеті та схарактеризувати особливості вразливостей психіки перед маніпулятивними методами.

2. Здійснити емпіричнОкреслити види методів соціальної інженерії, які використовуються для маніпулює дослідження впливу методів соціальної інженерії на поведінку та реакції користувачів, зокрема, на емоційну стійкість, емпатію, довіру та стиль ухвалення рішення користувачів Інтернету.

3. Розробити та апробувати тренінгову програму для користувачів Інтернету третього віку дорослості, спрямовану на підвищення обізнаності про методи соціальної інженерії та формування стійкості до маніпуляцій у цифровому середовищі та запропонувати рекомендації захисту від маніпулятивних методів в онлайн-просторі.

**Об’єктом дослідження** є явище психологічного впливу соціальної інженерії на користувачів Інтернету.

**Предметом дослідження** є специфіка впливу психологічних методів соціальної інженерії на користувачів Інтернету третього віку дорослості за допомогою інструментів інтернет-технологій.

**Методи дослідження:** Для розв’язання поставлених завдань застосовано комплекс взаємопов’язаних методів дослідження: *теоретичні* (аналіз, синтез та порівняння); *емпіричні* (інтерв’ю, бесіди, анкетування та опитування, психодіагностичні та проективні методики; експеримент (констатувальний, формувальний)); *методи математично-статистичної обробки даних* (описові статистики для узагальнення результатів дослідження; коефіцієнт кореляції Пірсона для дослідження взаємозв’язку між застосуванням методів соціальної інженерії та вразливостей користувачів) з унаочненням.

**Наукова новизна** одержаних результатів визначається тим, що вперше на основі наукових джерел здійснено аналіз впливу методів соціальної інженерії на користувачів Інтернету третього віку з виокремленням особливостей психіки та

поведінки людей похилого віку в контексті кіберзагроз з акцентуванням уваги на ключові фактори, які підвищують вразливість пенсіонерів до маніпуляцій в Інтернеті; *удосконалено* підґрунтя цифрової безпеки користувачів пенсійного віку як важливого компоненту загальної безпеки суспільства з окресленням мети і завдань; *подальшого розвитку* дістали наукові положення щодо розробки тренінгової програми навчання та профілактики кіберзлочинності серед осіб похилого віку.

**Практична значущість** полягає у розробці та апробації тренінгової програми «Твій цифровий щит», яка може бути впроваджена у навчальні курси, тренінги та консультаційні заходи для підвищення рівня цифрової безпеки користувачів пенсійного віку; можуть бути використані соціальними працівниками, психологами та організаціями, що працюють із літніми людьми. Рекомендації, сформульовані на основі проведеного дослідження, сприяють вдосконаленню навичок розпізнавання маніпуляційних технік в онлайн-середовищі, що знижує ризики потрапляння в шахрайські схеми.

**Апробація результатів дослідження** здійснена на XXVII Всеукраїнській щорічній науково-практичній конференції «Могилянські читання - 2024: досвід та тенденції розвитку суспільства в Україні: глобальний, національний та регіональний аспекти» (6-10 листопада 2024 року, Миколаїв).

Окремі положення кваліфікаційної роботи опубліковані в: 1) Терентьєва Н., Фалько Н. Взаємозалежність особливостей психіки користувачів Інтернет-середовища та методів соціальної інженерії. *Габітус*. Одеса: Гельветика. 2024, № 66. (фахове видання, ISSN: 2663-5216, наукометричне видання, Index Copernicus International); 2) Фалько Н. Соціальна інженерія: зброя масового психологічного впливу в цифрову епоху. *Науково-інформаційний супровід професійної підготовки фахівців в умовах невизначеності: тези науково-практичного семінару з міжнародною участю* (25 квітня 2024 року, м. Миколаїв). С. 171-176.

**Структура та обсяг роботи**. Кваліфікаційна робота складається зі вступу, трьох розділів, висновків до них, висновків та списку використаних джерел (114

найменувань) та 7 додатків на 21 сторінках. У тексті містяться 8 таблиць, 11 рисунків. Загальний обсяг кваліфікаційної роботи – 124 сторінrb, з яких основного тексту – 85 сторінок.

# РОЗДІЛ 1
# ТЕОРЕТИЧНІ ОСНОВИ ВИВЧЕННЯ ВПЛИВУ МЕТОДІВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ НА ОСОБЛИВОСТІ ПСИХІКИ КОРИСТУВАЧІВ ІНТЕРНЕТУ

## 1.1. Сутність поняття соціальної інженерії та її роль у сучасному суспільстві

*При соціальній інженерії «зламують» людину, а не пристрій*

*з сайту "Nadiyno"*

Ефективне дослідження сучасних проблем соціальної інженерії можливе лише з точки зору мультинаукового підходу, а саме на межі психології, соціології, політології, інформаційних технологій, менеджменту, економіки, кібербезпеки та ін. Адже всі ці сфери діяльності значною мірою сфокусовані на емоційному впливі на соціум, індивіда. А можливості Інтернету в цілому та соцмереж безпосередньо дають продукувати будь-яку емоцію в необмежених масштабах, а отже, вести особу чи суспільство (його частину) в потрібному маніпулятору руслі.

Лише розуміння тенденцій розвитку соціуму та інструментів управління ним як зі знаком плюс, так і мінус (маніпулювання) може дати відповіді і щодо розвитку впливів на конкретного індивіда в такому потужному ресурсі, як Інтернет. На нашу думку, сьогодні є кілька напрямків такого інтересу для науки та практиків: визначити та структурувати інструменти впливу соціальної інженерії на особу за допомогою ШІ; дослідити можливості практичного психолога зрозуміти суть проблеми клієнта, постраждалого від інтернет-шахрайства; на державному рівні визначити методи залучення якомога більшої частини суспільства до навчання протидії соціальній інженерії та удосконалення правового регулювання з цього питання.

Аналіз останніх публікацій показав, що питаннями формування нового суспільства, психологічним портретом сучасної людини займалося багато філософів, науковців, психологів, серед яких можна відмітити таких як:

Дж. Акерлоф, А. Коваль, М. Кастельс, І. Лапченко, Н. Чепелєва, Р. Шиллер тощо. Незважаючи на досить широкий спектр проведених досліджень, питання використання соціальної інженерії для сучасної моделі сучасного фішингу, пов'язаного із заволодінням даних, а саме – персональних даних, чутливої інформації та номерів банківських карток, виступає частиною загальної проблеми, котрій присвячується багато наукових статей у різних галузях науки [58, с. 260].

Як зазначає Г. Ржевський, останнім часом активізувалися дослідження впливу віртуальної комунікації на психіку людини, на розвиток особистості, повсюдно вивчаються й інші потенційно небезпечні психологічні наслідки проникнення комп'ютерів в повсякденне життя людей [53, с. 148].

Інтернет, з одного боку, таїть певні загрози державі через свою відкритість, некерованість, демократичну природу функціонування й потребує пильної уваги, реґулювання та контролю з боку владних, силових структур. З іншого боку, Інтернет має неосяжні можливості для впливу на громадянина, на електорат, що призвело до появи й значно поширення маніпулятивних стратегій і технологій в онлайн-середовищі, які зараз широко використовуються як на місцевому, регіональному та державному, так і на міждержавному, глобальному рівні [8, с. 414].

Українське законодавство визначає інтернет-шахрайство як один з видів шахрайства, а саме – заволодіння майном або майновим правами за допомогою обману або зловживання довірою, що регулюється статтею 190 Кримінального кодексу України [36].

Для розслідування такої категорії злочинів потрібно врахувати, що існують деякі особливості, а саме: особистого контакту між потерпілим і злочинцем немає, все здійснюється дистанційно. А це означає, що робота слідства ускладнена ще встановленням особистості шахрая; переказ грошей здійснюється дистанційно – в цілому, це більше плюс, оскільки через інформацію з банку можна встановити точну суму збитку [59].

Поширення кіберзагроз на усі сфери життєдіяльності та вдосконалення інструментарію їх реалізації зумовлює необхідність зміни стратегії і тактики протидії ним. Набуває значимості максимально швидке виявлення вразливостей і кібератак, реагування та поширення інформації про них для мінімізації можливої шкоди [32, с. 76].

У такій ситуації актуальною є Стратегія кібербезпеки України, яка затверджена Указом Президента України від 26 серпня 2021 року № 447/2021 [50]. З огляду на всю специфіку кібер-злочинів створено Департамент кіберполіції в складі Національної поліції України, який супроводжує справи даної категорії [52]. На жаль, на законодавчому рівні проблема захисту інформації користувача недостатньо опрацьована [43, с. 15].

У сучасному світі найбільшу цінність та значимість несе інформація, а найслабкішим місцем у її захисті є ж самі люди. Технології стрімко розвиваються, а разом з ними збільшується чисельність злочинів у кіберпросторі. Все більше хакерів намагаються отримати дані з осіб, фірм та різних організацій у своїх інтересах. І з кожним разом вони застосовують різні підходи для отримання бажаного результату. Існують безліч методів та способів пов’язаних з шахрайством в цифровому середовищі, проте одним з найнебезпечніших та найбільш ефективних вважається соціальна інженерія [56].

У ширшому розумінні соціальною інженерією можна вважати будь-які маніпуляції, пов’язані з психологією поведінки. Однак це поняття не завжди пов’язане зі злочинною чи шахрайською діяльністю. Насправді соціальна інженерія широко використовується і вивчається в різних контекстах, в таких областях, як соціальні науки, психологія й маркетинг [75].

А. Селіванова та Ю. Левитський у роботі «Дослідження методів соціальної інженерії. Частина І. Вплив на здоров’я людини» зазначають: “цей термін є синонімом диктатури й тоталітарної тиранії. Ідея полягає у тому, щоб поводитися з людськими істотами так само, як інженер поводиться з матеріалом, з якого він будує мости, дороги і машини. Воля соціального інженера має

замінити волю багатьох людей, яких він планує використати для побудови своєї утопії» [57, с. 57].

Соціальна інженерія – це термін, який використовується для позначення широкого спектра зловмисних дій, що здійснюються за допомогою людської взаємодії. Він використовує психологічні маніпуляції, щоб змусити користувачів робити помилки безпеки або надавати конфіденційну інформацію [90].

Науковці з Китаю Ван Цзогуан (Z. Wang), Сан Лімін (L. Sun), Чжу Хунсон (H. Zhu) у своїх працях детально проаналізували поняття соціальної інженерії саме з позиції вразливостей людської психіки в кібербезпеці. На основі еволюційного аналізу вони запропонували нове визначення соціальної інженерії в кібербезпеці, яке усуває концептуальні невідповідності, охоплює основні концептуальні конотації, уточнює концептуальні межі тощо [113, с. 85102].

М. Ганченко зазначає, що соціальна інженерія (social engineering) або «атака на людину» – це сукупність психологічних і соціальних прийомів, методів та технологій, які дозволяють отримати конфіденційну інформацію [11, с. 16].

Доктор філософії Кембриджського університету Джозеф М. Хетфілд у дослідженні «Social engineering in cybersecurity: The evolution of a concept» розкриває концептуальний набір сучасних конотацій через аналіз 134 визначень терміну «соціальна інженерія», знайденого в наукових статтях, написаних про кібербезпеку з 1990 по 2017 рік [95, с. 103].

Соціальна інженерія продовжує залишатися одним з популярних та важливих інструментів для кіберзлочинців. Адже ці методи є ефективними та економічно вигідними. Це дає змогу розширювати спектр атак, роблячи їх більш різноманітними та використовуючи нові сучасні технології. Глобальна поширеність та використання методів соціальної інженерії у повсякденному житті базується на твердженні, що люди завжди були й залишаються найбільш вразливою ланкою у захисті інформації [111, с. 4].

Науковці Л. Половенко та С. Мерінова стверджують, що психологічною передумовою застосування технологій соціальної інженерії виступають когнітивні упередження – тенденції думати певним чином, шаблонність,

стереотипність мислення, що дає змогу навіювати відповідні «стандарти», диктувати відповідний тип поведінки У сфері інформаційної безпеки термін використовується для опису науки і мистецтва психологічної маніпуляції з метою несанкціонованого доступу до інформаційних ресурсів [49, с. 184].

На нашу думку, доречно згадати і найвідомішого хакера світу. Кевін Мітнік, хоч і не мав професійної освіти в галузі психології, виявився відмінним спостерігачем та аналітиком людської поведінки через його вміння використовувати соціальну інженерію для здійснення взломів [111, с. 31]. Він досліджував психологічні слабкі місця та тенденції в людському мисленні і використовував цю інформацію для маніпуляцій та отримання доступу до конфіденційної інформації [102, с. 3]. Його роботи, такі як «Мистецтво обману» та «Мистецтво вторгнення», демонструють його розуміння особливостей психіки людини, здатність адаптувати свої методи до різних ситуацій і особистостей. Визнаний майстер соціальної маніпуляції, який використовував знання про людську психологію для досягнення своїх цілей у сфері кібербезпеки (як зі знаком плюс, так зі знаком мінус) [103, с. 12].

Соціальна інженерія намагається використати притаманні людям слабкості, наприклад: квапливість, жадібність, альтруїзм чи страх перед офіційною установою, з метою отримання конфіденційної інформації та подальшого доступу до системи [90].

В. Яковенко і Н. Казеян розглядають соціальну інженерію як метод несанкціонованого доступу до інформації або системам зберігання інформації завдяки взаємодії з людиною. Вона стала універсальним способом управління діями людини з мінімальним використанням технічних засобів. Метод заснований на використанні слабкостей людського фактора з впливом на психіку об’єкта, і тому представляє найбільшу загрозу для інформаційної безпеки [77, с. 183].

В основу соціальноїх інженерії покладено психологічне управління людиною, а саме емоційний стан: зацікавленість, стурбованість, страх, довіра тощо [111, с. 30]. Основною метою соціальної інженерії є отримання допуску до

конфіденційної інформації, паролів, електронної пошти, банківських даних і інших захищених систем [30, с. 64].

Цю думку підтримує дослідник Г. Харл який описував соціальну інженерію як мистецтво і науку змусити людей виконувати бажання шахрая з точки зору психології. [94, с. 2]

Суть соціальної інженерії полягає в тому, щоб використати людську природу та вразливості, заманити їх у пастку та переконати здійснити небезпечні дії. Це може бути здійснено через використання маніпулятивних технік, які базуються на довірі, необережності або незнанні людей [88].

Поширеність методів соціальної інженерії пояснюється тим, що психіка людини є більш вразливою, ніж захисні технології, і часто злочинцям набагато простіше отримати доступ до закритих даних через комунікацію, ніж через зламування систем захисту [35, с. 3].

Науковці Техаського університету Rosana Montanez, Edward Golob, Shouhuai Xu визначають кібератаки соціальної інженерії як різновид психологічної атаки, яка використовує слабкі місця в когнітивних функціях людини [104, с. 1].

Отже, соціальна інженерія є складним феноменом, який характеризується різноманіттям методів – від простих маніпуляцій до складних соціальних інженерних атак. Її успішність залежить від розуміння людської психології та вміння будувати довіру. Встановлено, що вивчення поняття соціальної інженерії науковцями охоплює широкий спектр дисциплін – від психології та соціології до кібербезпеки, набуває більшої актуальності через зростання кількості цифрових взаємодій у сучасному онлайн-просторі.

### 1.2. Основні методи та стратегії, які використовуються для здійснення впливу на користувачів Інтернету

За оцінками експертів, до 2025 року атаки соціальної інженерії будуть коштувати світові витрати в 10,5 трильйонів доларів США на рік. «Людська помилка» пов’язана приблизно з 95% кібератак, а це означає, що соціальна

інженерія, яка ґрунтується на людському елементі дій і поведінки, бере участь у більшості кібератак.[114, с. 6]

Атаки соціальної інженерії охоплюють широкий спектр методів, які використовують людську психологію для маніпулювання особами, змушуючи їх розкривати конфіденційну інформацію, виконувати певні дії або приймати рішення, які приносять користь зловмиснику.

На сьогодні накопичено, досліджено і проаналізовано значний досвід маніпуляцій із свідомістю та введення в оману людей, напрацьовано величезний обсяг матеріалів стосовно психології поведінки як тих, хто маніпулює, так і тих, хто попадає в тенета, розставлені спритними маніпуляторами, які гарно розбираються в людях та уміють читаючи психологічний портрет людини та знаходити найбільш психологічно нестійких та тих, хто піддані впливу різних методів, заходів та інструментів соціальної інженерії індивідів [111, с. 5]. Відмінністю таких «ловців на простаків» є те, що вони працюють без використання грубої сили та насильства, використовуючи лише психологічні тенета (соціальну інженерію) для «ловлі простаків», чим і входять у довіру [84, с. 30]. Змінюються лише інструменти та сам «предмет бажання» – інформація, яка в умовах інформаційного та постінформаційного суспільства набула ознаки товару та стратегічного ресурсу. Насамперед це персональні дані, чутлива інформація для бізнесу, уряду та особливо – номери банківських карток для подальшого зняття коштів із них [113, с. 85099].

Соціальна інженерія стала невід’ємною частиною кібер-шахраїв. Йдеться про спеціальну методику маніпуляції, яка допомагає змусити людину віддати зловмисникам необхідні дані використовуючи людські слабкості – тобто емоції та природну поведінку жертви [84, с. 23]. У контексті кібербезпеки соціальна інженерія – це тип атаки, при якій зловмисник використовує вразливі місця людини за допомогою соціальної взаємодії для порушення кібербезпеки безпеки, з використанням або без використання технічних засобів та технічних вразливосте. [113, с. 85-105]. Маніпуляції передбачають використання людської доброти, жадібності та цікавості для отримання доступу до будівель з

обмеженим доступом або спонукання користувачів до встановлення бекдорного програмного забезпечення [111, с. 26]. Сьогодні існує чимало методів використання соціальної інженерії. В основі – маніпуляція людськими страхами, зацікавленістю або довірою [76].

Один із найвідоміших хакерів світу Кевін Мітник у книзі «The Art of Deception: Controlling the Human Element of Security» підкреслює: «Люди виявляють себе більш вразливими до маніпуляції, коли вони несвідомі того, що вони маніпульовані» [103, с. 25]. Ця цитата підкреслює важливість свідомого розуміння та виявлення маніпуляцій, щоб захистити себе від них. Маніпулятори можуть використовувати різні техніки, щоб приховати свої наміри та залучити своїх жертв у пастку. Тому важливо вивчати це питання, бути уважними та освіченими щодо можливих загроз та методів захисту від них [103, с. 78].

Дослідники методів соціальної інженерії (соціального інжинірингу) за маніпулюванням рисами людської натури поділяють на авторитетністні, прихильністні, взаємністні, відповідальністні, соціальністні та обмежувальністні [31, с. 200]. Такі ознаки вони визначають шляхом узагальнення результатів соціальних досліджень щодо впливів (маніпуляцій) на людей, де виділено шість рис людської натури, які можна використовувати для отримання потрібної інформації: взаємність, послідовність, соціальне схвалення, симпатія, авторитет і дефіцит [85, с. 76].

Ю. Чаплінська виокремлює вісімнадцять ризиків кіберсоціалізації, джерела якого лежать у технологічній площині, але вони мають психологічні аспекти реалізації, які втілюються як на індивідуальному рівні чи на рівні малої групи, так і на загальносвітовому рівні [72, с. 163].

Суть здійснення маніпуляції полягає в тому, щоб створити певний дисбаланс у жертви і викликати внутрішній дискомфорт. Окрім того, щоб жертва не встигла знайти способи вирішення поданої ситуації, маніпулятор попередньо надає ці способи вирішення, зазвичай надаючи вибір, котрий можна назвати «вибір без вибору» [63, с. 144]. У основі усіх шахрайських схем полягає

маніпуляція свідомістю людини, де вона стає об’єктом, засобом досягнення цілей одних людей за рахунок маніпулювання іншими [9, с. 76].

У працях американських науковців J. Dawson, R. Thomson проаналізовано психологічні аспекти стійкості до шахрайських дій в Інтернеті [35, с. 3].

Розглянемо основні методи соціальної інженерії, визначимо їх особливості, приклади використання, способи і ймовірність впливу на особу.

Фішинг – це метод обману, заснований на неуважності користувача, спрямований на отримання конфіденційної інформації, такої як імена користувачів, паролі, дані банківських карток або номери телефонів [82, с. 414]. Зловмисники маскуються під представників відомих організацій, брендів, магазинів чи банків, створюючи ілюзію довіри та правдивості, щоб спонукати користувача надати необхідні дані. Атака здійснюється з використанням електронної пошти або sms-розсилки, куди надсилається лист з пропозицією перейти за посиланням. Усе відбувається поспіхом та обмеженням часу на виконання з боку користувача. Це спричиняє вихід людини з рівноваги, подальше прийняття неправильних та необдуманих рішень. У результаті відбувається перехід на підроблений зловмисником сайт для вводу даних, необхідних для авторизації користувача. Таким чином конфіденційні дані стають доступними та відомими шахраю [11, с. 19]. Тож фішинг спрямований на керування діями потерпілого базуючись на наївності та неуважності останнього.

Жертви також можуть додатково зателефонувати із проханням відкрити цей додаток або ж перейти за посиланням. Вважається, що таке «живе» спілкування додає ситуації чималої правдоподібності і зазвичай змушує людей відкривати вкладення [56].

Цю думку підтримують дослідники Д. Беседа та О. Сорочинський: фішингові сайти – це веб-ресурси, які візуально ніяк не відрізняються від офіційних сайтів, але при вводі особистих даних: логіни і паролі наприклад для авторизації у державних ресурсах, у електронних скриньках або реквізити своїх платіжних карток – це все переходить у руки кіберзлочинців [6, с. 12].

Претекстинг – атака, проведена за заздалегідь підготовленим сценарієм, для здійснення якої шах-рай видає себе за іншу особу та вивідує у жертви необхідну інформацію. [49, с. 185]. Для правдоподібності шахрай на момент атаки уже володіє деякою правдивою інформацією, котру повідомляє, щоб увійти в довіру, зблизитись або ввести людину у знервований чи стан переживання, та дізнатись ще більше необхідних даних. Претекстинг засвідчує, що люди схильні довіряти, коли мова йде про знайоме, близьке, рідне, підсилене емоційним забарвленням [11, с. 20, 21].

Дослідники K. Chetioui, B. Bah, A. Ouali, A. Bahnasse. серед найбільш популярних методів соціальної інженерії виділяють такі: Бейтинг або лов “на живця” це атака, в якій використовуються "приманки" для того, щоб зацікавити жертву, викликавши її цікавість [86, с. 659]. У приманці зловмисник обіцяє щось в обмін. Наприклад, хакер може обіцяти безкоштовну музику, телефони, грошові призи тощо, і для отримання цього користувач повинен не тільки увійти на сторінку, а й поділитися певною особистою інформацією [101, с. 388]; фішинг (масове розсилання електронної пошти великій групі адресатів, що спонукає до відкриття вкладення до переходу за посиланням на веб-сторінку з метою є виманювання персональних даних) [69, с. 162], вішінг (зловмисники використовують канали голосового зв’язку, наприклад телефонні дзвінки, щоб обманом змусити жертв розкрити конфіденційну інформацію або виконати дії, що загрожують їхній безпеці) [82, с. 411] або лже-антивірус (це шкідливе програмне забезпечення, яке змушує користувачів відвідувати веб-сайт, заражений шахрайським шляхом) [89]. Найслабша ланка захисту будь-якої системи – самі користувачі.

Одна з поширених схем шахраювання сьогодні в Україні, зважаючи на повномасштабну агресію росії, – це фейкові волонтери, військові та священники. Зловмисники беруть пости реальних людей, але вставляють свої картки для переказу [17]. Інша схема – так звана допомога з грошовою допомогою. Під виглядом міжнародних організацій, соціальної платформи “єДопомога”, порталу державних послуг “Дія” шахраї пропонують громадяни, що постраждали від

війни пропонують фінансову допомогу, далі перейти на фішинговий сайт, де мають можливість викрасти реквізити карток та облікові записи користувачів [45].

Восени 2023 року широкого поширення набув шахрайський метод під назвою «Гроші за лайки». Зловмисники пропонували користувачам виконувати прості дії: ставити лайки на товари, відео в YouTube або TikTok, оцінювати об’єкти чи переглядати фільми, обіцяючи за це виплату грошей. Завоювавши довіру, вони починали вимагати від жертв здійснювати покупки дорогих товарів або бронювати готелі за власний рахунок, після чого зникали без сліду [15].

Розглянемо такі особливості, пов’язані з атаками соціальної інженерії: особистість, досвід, індивідуальні відмінності, культура, робоче навантаження, стрес і пильність. Ці атрибути впливають на сприйнятливість людини до атак соціальної інженерії [104, с. 9]. Що стосується особистості, то немає консенсусу щодо її зв’язку з її сприйнятливістю до атак соціальної інженерії в кіберпросторі.

Особливості психіки користувачів, на які впливають методи соціальної інженерії, можна охарактеризувати п’ятьма основними сферами, а саме невротизм, відкритість, екстравертність, свідомість і приємність [105, с. 2]. Окреслимо сучасне розуміння їхнього зв’язку з атаками соціальної інженерії. Що стосується невротизму дослідження показують, що високий рівень його пов’язаний із нижчою самоефективністю (тобто впевненістю користувача в управлінні кіберризиком) і підвищенням сприйнятливості до фішингу, але дослідження на фішинг припускає, що високий невротизм знижує сприйнятливість до фішингових атак [93, с. 318]. Що стосується відкритості, одне дослідження припускає, що висока відкритість підвищує сприйнятливість до атак на конфіденційність, але інші дослідження припускають, що висока відкритість знижує сприйнятливість до фішингових атак [87, с. 7]. Що стосується екстраверсії, одне дослідження припускає, що висока екстравертність підвищує сприйнятливість людини до фішингових атак, але інше дослідження припускає, що висока екстравертність знижує сприйнятливість до фішингових атак [105, с. 2].

Досить цікавою спробою переосмислити сучасний стан справ у царині маніпуляцій на рівні свідомості та вплив на психологічний стан людини є книга нобелівських лауреатів з економіки Джорджа Акерлофа та Роберта Шиллера, які спробували на основі численних прикладів з різних сфер економіки показати гігантські масштаби зловживань людською довірою, викликаних нераціональністю і нелогічністю певних вчинків для врахування іншими для уникнення потрапляння у аналогічні ситуації [1, с. 68].

Автори використовують термін "phishing" – метод соціальної інженерії, спрямований на отримання конфіденційної інформації шляхом обману людей. "Phishing" є метафорою для широкого спектру практик, що включають в себе маніпуляцію та обман у різних сферах економіки, використання психологічних трюків для збільшення продажів [111, с. 9]. Дослідники закликають до більшого розуміння психологічних механізмів, які використовуються для впливу на економічне поведінку, та до впровадження заходів для захисту людей від недобросовісних практик [1, с. 68].

Звичайні фішингові електронні листи, як правило, не адресовані якомусь конкретному одержувачу. Замість цього вони відправляються на величезні списки адрес електронної пошти, куплених шахраями і злочинцями [88]. Найбільш розповсюдженою формою кібератаки в світі є різний вид фішингу, що передбачає вироблення важливої інформації за допомогою електронних листів із застосуванням соціальної інженерії та обману. Щодо України, то в 2022 році офіційно зареєстровано 415 кіберінцидентів, що в 2,8 рази більше порівняно з роком 2021 року [37, с. 3].

Техніки соціальних інженерів різноманітні, але їх об’єднує одне – в основі лежать когнітивні спотворення (тобто людська дурість і неуважність). Крім цього останнім часом почастішали випадки шахрайства за допомогою соціальної інженерії – метод незаконного отримання доступу до певної інформації, не використовуючи технічні обладнання та засоби. Головним чином використовуються слабкості людського фактора, і полягає в маніпулюванні поведінкою людини [28, с. 24].

Д. Мехед доводить, що серед існуючих загроз інформаційній безпеці вже котрий рік поспіль перші позиції займають методи соціальної інженерії [42,с.249]. Виділено найбільш поширені інструменти і методи однієї зі складових соціальної інженерії – фішингу [97, с. 7]. Серед низки сформованих рекомендацій щодо захисту окреме місце займає підвищення обізнаності працівників в питаннях інформаційної безпеки, регулярне навчання персоналу правилам безпечної роботи в Інтернеті, пояснення методів атак і способів захисту тощо [42, с. 247].

Цю думку підхоплює науковець О. Кушнерьов, зазначивши, що найбільш розповсюдженою формою кібератаки в світі є різний вид фішингу, що передбачає вироблення важливої інформації за допомогою електронних листів із застосуванням соціальної інженерії та обману [37, с.52].

Дослідник Е. Окайвеле характеризує претекстинг – як тип соціальної інженерії, коли зловмисники створюють сфабрикований сценарій або привід, щоб маніпулювати жертвами, щоб вони надали інформацію. Наприклад, зловмисник може видавати себе за колегу та запитувати конфіденційні дані [107]. Використовують це з метою завоювати довіру жертви та отримати доступ до безпечних зон або інформації.

Атаки Honeytrap – «медова пастка» – використовуються зловмисниками, які створюють фальшиві профілі, щоб обманом змусити жертв поділитися грошима, інформацією або доступом до мережі [46]. Цю тактику часто використовують у сценаріях шпигунства чи шантажу.

Ще одним із методів є зворотна соціальна інженерія, за якої особа сама звертається до шахрая та повідомляє свої конфіденційні дані. Одним із можливих сценаріїв є, коли шахрай надсилає співробітникам компанії нібито нові номери телефонів служби технічної підтримки. Цілком імовірно, що через певний час хтось із співробітників зателефонує і шахрай зможе вивідати інформацію, яка його цікавить [13, с. 22]. Жертва вважає, що вона ініціювала взаємодію, і може бути більш охочою виконувати запити або розголошувати інформацію.

Романтичні онлайн-шахрайства передбачають створення зловмисниками підроблених профілів на веб-сайтах знайомств для встановлення романтичних стосунків із жертвами. Згодом вони емоційно та фінансово експлуатують жертв [107].

Американські дослідники R. Montanez, A. Atyabi, Xu S поділяють методи атак соціальної інженерії в кіберпросторі на чотири категорії: контекстуалізація, маскування, фізичний доступ і цифрова зворотна інженерія [104, с. 11].

Контекстуалізація – це техніка формування повідомлення, за якої зловмисник представляє себе як члена «внутрішньої групи» або спільноти інтересів, включаючи в повідомлення деталі, що стосуються групи. Прикладами деталей можуть бути поточні події або теми, специфічні для спільноти. Окрім підвищення довіри до зловмисника, контекстуалізація також дає підстави для зниження сприйняття ризику [104, с. 12].

Маскування – це набір методів, за допомогою яких зловмисник припускає себе онлайн-персоною, щоб продемонструвати довіру та надійність. До нього належить один із методів соціальної інженерії – випадковий одержувач. Суть якого полягає у намаганні зв’язатися з великою кількістю потенційних жертв випадковим чином. Застосовуються чотири специфічні методи атак: фішинг, SMiShing, вішинг і шахрайство електронною поштою [105, с. 9]. По-перше, фішинг є найпоширенішим методом атаки через електронну пошту. Типовий фішинговий електронний лист містить посилання, яке спрямовує жертву на шахрайський веб-сайт для завантаження зловмисного програмного забезпечення (наприклад, програми-вимагача) або викрадення облікових даних жертви. Мета повідомлення полягає в тому, щоб мотивувати одержувача натиснути посилання, для чого широко присутні стимули та підказки терміновості. У той же час стимули можуть відрізнятися залежно від групи, термінові запити використовуються, щоб спонукати користувача натиснути посилання для уникнення втрати послуг [105, с. 11].

За інформацією Cybertalk фішинг – це тактика номер один, яку використовують хакери, щоб отримати дані, необхідні для більш масштабних

атак. Коли фішинг налаштовано для цільової особи чи компанії, цей метод називається «фішингом», і близько 65% хакерів використовували цей тип атаки. Щодня надсилається близько 15 мільярдів фішингових листів [2].

Цю думку підтверджує науковець М. Гуцалюк: один з найбільш успішних форматів атак, які кіберзлочинці регулярно використовують для проведення атак соціальної інженерії, – це фішингові електронні листи [16, с.85].

Детально досліджували психологічні вразливості під час фішингу науковці університету Олбані Goel, Williams, Dincelli [92, с. 22]. Результати показали, що контекстуалізація повідомлень для звернення до психологічних слабкостей одержувачів підвищує їх сприйнятливість до фішингу. Страх втратити чи очікування отримати щось цінне підвищував сприйнятливість до обману та вразливість до фішингу [92, с. 37].

Дослідника А.Козар аналізує метод соціальної інженерії – квіпрокво: шахраї дзвонять за випадковим номером телефону компанії і представляються співробітниками технічної підтримки, метою є введення певних команд самим потерпілим, що дозволяють запустити шкідливе програмне забезпечення [28, с. 24].

Проаналізуємо зв’язок між почуттями (емоціями) та маніпулятивними діями шахраїв та представимо їх у вигляді таблиці (Табл.1.1)

*Таблиця 1.1.*

**Взаємозв’язок між емоціями та методами соціальної інженерії**

| **Почуття, на яке впливають** | **Додаткові деталі** | **Приклади методів соціальної інженерії** | **Мета шахраїв** | **Додаткові деталі** |
|---|---|---|---|---|
| Довіра | Використання легітимних логотипів, доменів, створення відчуття безпеки | Фішинг, вішінг, іммітація брендів, спам | Отримання конфіденційної інформації | Використання легітимних логотипів, доменів, створення відчуття безпеки |

| | | | | |
|---|---|---|---|---|
| | | від імені знайомих [56]. | | |
| Страх | Гра на емоціях, використання термінів "терміново", "останній шанс" | Шантаж, вимагання, повідомлення про блокування акаунтів | Змусити жертву діяти швидко і бездумно | Гра на емоціях, використання термінів "терміново", "останній шанс" |
| Жадібність | Використання слів "безкоштовно", "виграш", "інвестиція" | Бейтинг, фішинг з привабливими пропозиціями | Отримання фінансової вигоди | Використання слів "безкоштовно", "виграш", "інвестиція" |
| Гордість | Використання слів "ексклюзивний", "особливий", "престижний" | Маніпуляція авторитетом, ексклюзивні пропозиції | Схилити жертву до співпраці | Використання слів "ексклюзивний", "особливий", "престижний" |
| Цікавість | Використання сенсаційних заголовків, незвичайних фактів | Клікбейт, поширення фейкових новин, виклик на дуелі | Залучення жертви на шкідливі ресурси | Використання сенсаційних заголовків, незвичайних фактів |
| Співчуття | Використання фотографій, відео, історій про хворих дітей, тварин | Благодійні шахрайства, фейкові збори коштів | Отримання грошових коштів | Використання фотографій, відео, історій про хворих дітей, тварин |
| Сором | Використання компрометуючої інформації, погрози | Шантаж, викриття особистих таємниць | Змусити жертву виконати | Використання компрометуючої інформації, погрози |

| | | | | |
|---|---|---|---|---|
| | розголошення секретів | | вимоги шахраїв | розголошення секретів |

Як бачимо, найслабша ланка захисту будь-якої системи – самі користувачі. Соціальна інженерія намагається використати притаманні людям слабкості, напр. квапливість, жадібність, альтруїзм чи страх перед офіційною установою, з метою отримання конфіденційної інформації та подальшого доступу до програм [90].

На відміну від систем і мереж, користувачі не можуть бути захищені від соціальної інженерії за допомогою дорогих інструментів, таких як брандмауери і антивірусні програми. Вони завжди відкриті і видають інформацію, яка може бути використана зловмисниками для нанесення по ним удару, коли цього найменше очікують [68, с.5].

## 1.3. Взаємозалежність особливостей психіки користувачів інтернет-середовища та методів соціальної інженерії

Динаміка і ритм сучасного життя, прагнення до успіху вимагають від людини постійною зібраності, концентрації уваги, мобілізації усіх сил. Це, у свою чергу, є причиною виникнення у людини численних стресів, депресій, коливань психоемоційного стану. Стреси займають значне місце в житті людей. Вони впливають на здоров’я, поведінку людини, взаємовідносини з іншими людьми, стосунки в сім’ї, працездатність, а отже, на досягнення або недосягнення людиною успіху [111, с. 38]. Війна, яка триває вже понад 2 роки, ще більш додали напруженості, психіка людини приходить в стресовий стан і

запускаються адаптаційні процеси. Організм використовує резерви, які в нормі не задіяні, когнітивні функції стають обслуговуючими і реагують на емоційний стан, тому пам’ять і увага на якийсь період часу погіршуються. Наслідком цього може стати підвищена схильність до впливу шахраїв або соціальних інженерів. Якщо в звичайному стані людина не схильна вірити в "підозрілі транзакції", про які повідомляють з незнайомого номера, в стані стресу тривожність перемагає, і людина стає жертвою [57, с. 57].

Соціальна інженерія опирається на психологічні особливості людини, такі як: я повинен зробити так, бо більшість так би і зробили (ми оцінюємо свою поведінку на фоні поведінки більшості); повага до авторитетних людей чи державних установ (ми будемо більше довіряти поліцейському, банківському працівнику, лікарю тощо аніж пересічній людині) [105, с. 10].

Усі види методів соціальної інженерії спираються на слабкість людської психології. Шахраї використовують емоції, щоб маніпулювати та обманювати своїх жертв. Людський страх, жадібність, цікавість і навіть готовність допомагати іншим обертаються проти них різними методами [75].

Ми розглядаємо установки, пов’язані з атаками соціальної інженерії: ставлення довіри, ставлення підозрілості та ставлення до ризику. Ці установки впливають на сприйнятливість людини до атак соціальної інженерії. Що стосується ставлення довіри, то високий рівень довіри створює високу сприйнятливість до атак соціальної інженерії і шахрайства [111, с. 20]. Для підозрілого ставлення особа з високою підозрілістю менш сприйнятлива до атак соціальної інженерії. Що стосується ставлення до ризику, то високе сприйняття ризику знижує сприйнятливість до атак соціальної інженерії, а низьке сприйняття ризику підвищує сприйнятливість до шахрайства [105, с. 3].

Науковець з Китайської школи кібербезпеки Zuoguang Wang наголошує на вразливостях людської психіки під час дії методів соціальної інженерії: «Ці задіяні людські елементи не тільки вразливі, але й уразливі настільки, що затьмарюють більшість інших заходів безпеки. Це означає, що цей недолік безпеки є універсальним і не залежить від платформи, програмного

забезпечення, мережі чи віку обладнання. Люди могли б витратити всі статки, купуючи технології та послуги..., однак мережева інфраструктура все ще може залишатися вразливою до старомодних маніпуляцій» [113, с. 85-101].

На думку науковців М. Руденко та С. Власової соціальна інженерія базується на досить простих психологічних характеристиках людини, таких як: принцип взаємності («ти мені – я тобі»), принцип соціальної перевірки (ви оцінюєте свою поведінку в контексті поведінки більшість), повага до влади (ви довірятимете лікарю та поліції більше, ніж звичайній людині). Усі ці правила стосуються «офлайнового» шахрайства, але вони мають свої особливості, коли вчиняються онлайн [55, с. 316].

Щоб підвищити шанси на успіх, такі психологічні методи можуть бути використані для створення повідомлень: переконання, шахрайство, стимул і мотивація, а також інтуїтивний тригер. Переконання – це акт представлення аргументу, який спонукає індивіда поводитися бажаним чином [111, с. 25]. Шахрайство (або обман) – це акт подання аргументу з наміром створити хибне переконання. Стимули та мотиватори заохочують співпрацю, де стимули використовують зовнішні винагороди, а мотиватори – внутрішні психологічні властивості [98, с. 189]. Вісцеральні тригери – це мотиваційні маніпуляції, які викликають емоційну реакцію шляхом використання потреб і бажань [105, с. 6].

Аферисти в основному використовують фактор часу – вмовляють жертву швидко прийняти рішення, не залишаючи їй можливості раціонально оцінити ситуацію; а також фактор поваги, авторитету. Навіть наша доброта нерідко стає мішенню для маніпуляцій, як-от листи з проханнями про допомогу, які приховують нещирі наміри. Фактор стадності базується на нашій схильності копіювати поведінку друзів або людей, які поруч з нами, з метою присипання нашої пильності [111, с. 29].

В основі шахрайства лежить принцип маніпуляції нашою вірою. Але взагалі нікому не вірити не вихід. Потрібно вірити, але не бути занадто легковірними. Не слід бути занадто відвертими. Шахраї дуже вміло використовують будь-яку інформацію, щоби втертися в довіру. Особливо

обережними потрібно бути з інформацією, яку користувачі повідомляють про себе в інтернеті, у соціальних мережах. Найбільше шансів у аферист тоді, коли користувач знаходиться у стані емоційного спаду [111, с. 34]. Психологи рекомендують не квапитися, раціонально осмислити те, що відбувається.

Пильність – це процес виділення когнітивних ресурсів для виконання складного завдання, такого як виявлення ознак, які можуть вказувати на оманливі наміри в повідомленні [105, с. 6]. Варто підкреслити, що на пильність впливає підозрілість.

Більшість людей асоціюють довіру в онлайн-просторі з поверхневими атрибутами, такими як професійний вигляд веб-сайту або наявність високоякісного та насиченого контенту [104, с. 12]. Довіра зменшує підозри, покращує переконливість повідомлення і підвищує сприйнятливість жертв до атак соціальної інженерії. Довіра до зловмисника характеризується такими атрибутами: спільність, репутація та надійність, які описані далі [111, с. 25].

Спільність можна легко встановити в Інтернеті, оскільки зловмисник може використовувати інформацію в соціальних мережах і на веб-сайтах, щоб побудувати спільну мову з жертвою. Така інформація, як упередження, вірування, норми та діалекти спільноти, корисна для зловмисника. Використовуючи таку інформацію, зловмисник може видати себе за учасника спільноти або знайомого на онлайн-форумах або в групах соціальних мереж [104, с. 12].

Репутація (авторитет) часто базується на мережі партнерів. Одним із методів покращення репутації зловмисника в кіберпросторі, яку сприймають інші, є збільшення зв’язків зловмисника в соціальних мережах із авторитетними особами. Шахрай може спиратися на сприйману спільність, щоб спонукати поважних осіб прийняти запрошення підключитися. Ще однією спокусою для залучення авторитетних людей у соціальних медіа є розмір соціальної мережі. Зловмисник може створювати широку соціальну мережу за допомогою ботів і підроблених персонажів [105, с. 10]

Надійність – це уявлення про те, що інша сторона діє добросовісно. Щоб показати надійність, зловмисник може включити в повідомлення артефакти (наприклад, посилання, зображення, графіку). Інтернет-середовище впливає на довіру жертви та сприйняття ризику [97, с. 4].

Сприйняття ризику – це індивідуальна оцінка ризику, пов’язаного з дією, і сприйняття ризику впливає на те, який ризик людина готова прийняти. Жертва в кіберпросторі також характеризується такими атрибутами: знання предметної області, пильність [111, с. 35].

По-перше, знання в сферах, відмінних від кібербезпеки, не зменшує сприйнятливість до атак соціальної інженерії в кіберпросторі. Це пояснюється тим, що вони часто покладаються на візуальні елементи та емоції, коли приймають рішення, пов’язані з ризиком [104, с. 12]. Крім того, сприйняття онлайн-ризику неекспертами формується передбачуваною вигодою від діяльності, а онлайн-діяльність, яка вважається корисною, сприймається як менш ризикована та виконується частіше [105, с. 11].

По-друге, застосування знань предметної галузі для розпізнавання атак соціальної інженерії в кіберпросторі є когнітивно вимогливим, оскільки розвиток знань про предметну область часто передбачає шаблони навчання, які вказують на зловмисні наміри [111, с. 33]. Загальні методи ідентифікації шаблонів (наприклад, розбір URL-адрес) вимагають вирішення технічних складнощів, що є когнітивно вимогливим, схильним до помилок і може сприяти надмірній довірі. Це розумно, оскільки коли ризик високий, але ситуацію важко оцінити, довіра є альтернативою для зменшення складності прийняття рішень [112, с. 154].

По-третє, пильність вимагає уваги, на яку впливають два компоненти, а саме перемикання та збереження уваги. Переключення уваги – це процес перенаправлення уваги з одного завдання на інше, тоді як підтримка уваги – це процес виділення когнітивних ресурсів для обробки інформації [108, с. 197]. Переключення уваги є попередником підтримки уваги та призводить до центральної обробки. Виразні подразники викликають переключення уваги.

У звичайних обставинах увага людини спрямована на виконання основного завдання, яке підтримує його цілі (наприклад, керування електронною поштою, відвідування веб-сайтів або пошук інформації в Інтернеті). Щоб виявити ознаки обману в повідомленні соціальної інженерії, потрібно перенаправити свою увагу, щоб помітити невідповідності в повідомленні, де невідповідності мають бути достатньо помітними, щоб їх виявити та запустити перемикання. Як наслідок, пильність "присипається" та впливають індивідуальні характеристики (наприклад, комп'ютерні звички) [105, с. 7].

Шахрайство відносно фізичних осіб можна розділити на три групи. Відносно найменш захищених верств населення, що мають низький рівень фінансового достатку і кіберграмотності (пенсіонери, жителі невеликих міст) [28, с. 24]. Для економічно активної частини населення, яка користується інтернетом, шахраї вибирають спам-розсилки листів, що містять інформацію про уявні знижки, отримання пільг, компенсацій, соціальних виплат. Такі повідомлення містять шкідливі програми або посилання на фішингові сайти, в результаті використання яких відбувається зараження пристрою і компрометація платежів його власника [112, с. 148]. До останньої групи можна віднести осіб, які активно користуються сучасними мобільними пристроями з операційними системами Android та IOS. Зловмисники використовують шкідливе програмне забезпечення для отримання доступу до встановлених на пристрої додатків, які містять конфіденційні дані. Це дозволяє їм здійснювати фінансові операції, такі як перекази грошових коштів з карт жертви. Такий підхід до шахрайства з використанням соціальної інженерії має різні варіації і полягає у використанні людських слабкостей [28, с. 27]. Висока поширеність таких атак підкреслює важливість своєчасного інформування про загрози, що є ключовим моментом у захисті користувачів віртуального середовища.

На думку О. Федоренко у ситуації, коли психологічний вплив здійснюється приховано, люди не завжди можуть чітко усвідомлювати суть загрози перебуваючи під впливом страху, не розуміючи що саме відбувається. На цій підставі у людей виникають панічні стани, які знижують критичність мислення,

і дозволяють маніпулювати їхньою поведінкою, стимулюючи до виконання тих чи інших дій [67, с. 328].

Соціальна інженерія нематеріальна, її неможливо усунути фізично. Найдієвіший спосіб не стати жертвою шахрайства – це не втрачати пильності і не дозволяти шахраєві себе провести [28, с. 25]. Соціальні інженери використовують ці вразливості, щоб змусити людей розголошувати конфіденційну інформацію, виконувати певні дії або приймати рішення, які приносять користь зловмиснику.

Підтримуємо думку видатного вченого-біхевіориста Томаса Еріксона: «Будь-який комунікативний контакт включає реціпієнта – саме за ним остаточне рішення» [20, с. 8], яка прекрасно ілюструє ключовий аспект психологічного впливу методів соціальної інженерії. Незалежно від того, наскільки досконало спланована маніпуляція або переконання, кінцевий вибір завжди залишається за людиною, яка отримує інформацію. Цим підкреслюється роль особистої відповідальності та здатності критично мислити [99, с. 71].

Ґрунтовний аналіз ключових вразливих місць людини, на які соціальні інженери часто орієнтуються, зустрічається у праці адвоката з кібербезпеки Еммануеля Окайвеле (E. Okaiwele) [107].

Процес використання психологічних вразливостей під час соціальної інженерії ми представили у блок – схемі «Модель взаємодії зловмисника та жертви в рамках соціальної інженерії» (рис. 1.2.).

Дослідник Murtaza Ahmed Siddiqi зазначає, що одна атака соціальної інженерії може бути проведена з використанням кількох методів впливу. Один метод впливу може використовувати кілька вразливих місць людини. Цей багатовимірний взаємозв’язок між атаками соціальтної інженерії, методами впливу та вразливими місцями людини робить кібератаки складними та загрозливими для безпеки [110, с. 10].

Науковці Техаського університету розмірковують про розвиток нової підгалузі, яку можна назвати «когнітивна психологія кібербезпеки», яка адаптує

принципи когнітивної психології до сфери кібербезпеки, одночасно охоплюючи нові поняття та концепції, унікальні для сфери кібербезпеки [104, с. 1].

Кевін Мітник у книзі "Ghost in the Wires: My Adventures as the World's Most Wanted Hacker" зазначає про важливість захисту від маніпуляцій: "Хочете знати найкращий спосіб захистити себе від маніпуляцій? Пам’ятайте, що найпотужніший інструмент у вашій арсеналі – це ваш розум. Завжди ставте під сумнів будь-яку ситуацію, в якій вас просять виконати щось, що вас не зручно, або в якій вам пропонують щось, що здається надзвичайно вигідним або легким. Навчіться розрізняти справжні можливості від обману. Пам’ятайте, що кращий захист – це свідомість [102, с. 256].

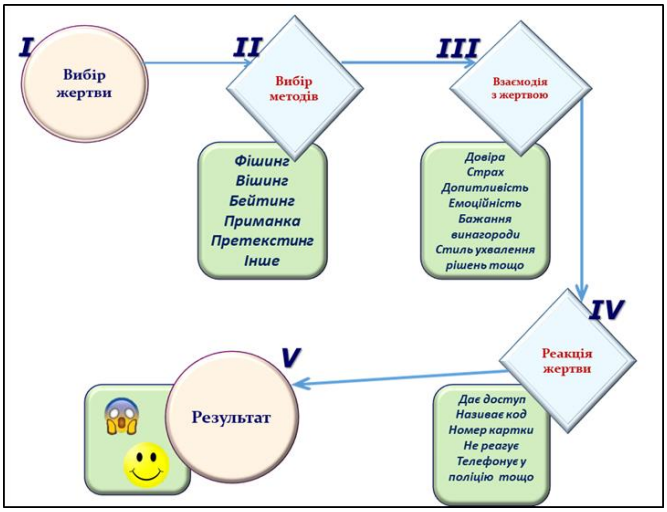



Рис. 1.2. Модель взаємодії зловмисника та жертви в рамках соціальної інженерії

Аналіз наукових джерел вказує на тісний взаємозв'язок між особливостями психіки користувачів Інтернету та ефективністю методів соціальної інженерії. Психологічні аспекти, такі як довіра, емоційність, бажання допомогти, когнітивні упередження є ключовими факторами, що впливають на успішність шахрайських дій.

Таким чином, розуміння психологічних особливостей користувачів є невід'ємною частиною забезпечення ефективної кібербезпеки в сучасному цифровому світі.

## Висновки до першого розділу

Техніки соціальної інженерії різноманітні, але їх спільною рисою є використання когнітивних спотворень, таких як людська наївність та неуважність. Останнім часом спостерігається збільшення випадків шахрайства за допомогою соціальної інженерії, що передбачає незаконний доступ до інформації без використання технічних засобів. Це передбачає маніпулювання поведінкою людини, яке змушує її здійснити дії, що сприяють крадіжці коштів або отриманню особистих даних. Такі методи включають фальшиві SMS-розсилки, злом даних для входу на популярні інтернет-ресурси, фішинг, квіпрокво і інші.

За даними офіційного сайту Кіберполіції Національної поліції України за вісім місяців 2024 року за оперативного супроводження кіберполіції до суду направлено 1897 кримінальних проваджень. У 2023 році цей показник за аналогічний період становив 1546 кримінальних проваджень. Але спостерігається загальне зменшення кількості звернень громадян через онлайн-шахрайства. Така динаміка зумовлена, зокрема, постійним інформуванням населення, а також нашими діями щодо протидії шахрайствам [24].

Високий рівень розповсюдженості цього виду шахрайства підкреслює важливість своєчасного інформування про загрози як ключового захисного механізму для користувачів сучасних комунікаційних засобів. Хоча соціальна інженерія являє собою нематеріальну загрозу, уникнути стати її жертвою можна, утримуючи пильність і не дозволяючи шахраям провести себе.

Атаки соціальної інженерії є постійною загрозою в цифровому світі, але розуміння психології цих тактик може допомогти окремим особам і організаціям захиститися від них. Визнаючи психологічні тригери та тривожні сигнали, пов’язані із соціальною інженерією, ми можемо зміцнити свій захист і захистити наше цифрове життя від маніпулятивних кіберзлочинців.

Людина не може одразу виявити, що перед нею шахрай через те, що істинний аферист – віртуоз своєї справи. Він ні до чого не змушує, а робить вас співучасниками власного краху. Він не краде – користувач віддає. Він не випитує – люди самі розповідають йому свою історію. Ми віримо, бо хочемо повірити. Тому проаналізувавши основні методики, що використовує соціальна інженерія в онлайн-просторі, виявлені взаємозв’язки між особливостями людської психіки та методами соціальної інженерії.

Для застосування методів соціальної інженерії не потрібні технічні знання, але негативні наслідки можуть бути значні. Інфраструктура й мистецтво їх застосування постійно удосконалюються та набувають тенденцію до активізації. Враховуючи розширення масштабів діяльності організованої злочинності все більше застосовуються методи “м’якої сили” [27, с. 97].

З’ясовано, що шахраї активізуються саме у складні, кризові періоди життя суспільства, оскільки критичне мислення людини знижується, вона втрачає пильність і через занурення у свої думки не помічає небезпеки. Єдине, що може допомогти у цій ситуації – самоконтроль. Шахраї розраховують якраз на емоційну незрілість. Вони тиснуть на слабкі місця людей. А ще вони дуже спостережливі: відстежують у соціальних мережах, що зараз актуально, на що реагують люди. Відповідно до цього створюють контент – зі зворушливою історією та вразливою картинкою, щоб це було емоційно.

Зазначимо, що у третьому кварталі 2023 року компанія Vade виявила значне збільшення кількості фішингових і шкідливих атак. Обсяги фішингу зросли на 173% порівняно з попереднім кварталом (493,2 млн проти 180,4 млн). Malware також спостерігалося стрімке зростання порівняно з кварталом (110%), досягнувши 125,7 мільйонів електронних листів порівняно з 60 мільйонами у другому кварталі [74]. Це свідчить про важливість питань, розглянутих у першому розділі.

# РОЗДІЛ 2.
# ДОСЛІДЖЕННЯ ВПЛИВУ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ НА ПОВЕДІНКУ КОРИСТУВАЧІВ ІНТЕРНЕТУ

## 2.1. Організація і методи дослідження впливу соціальної інженерії на поведінку користувачів інтернету

З метою виявлення впливу методів соціальної інженерії на особливості психіки користувачів було проведено дослідження. На основі проведеного аналізу, описаного у розділі першому, було розроблено анкети для опитування користувачів Інтернету.

У якості сервісу для опитування було обрано Google Forms. Це зручний сервіс для швидкого створення якісних та інформативних форм для опитування, яким можуть користуватися усі бажаючі без будь-яких проблем, враховуючи, що дослідження проводиться під час збройного конфлікту з рф [54]. Відсутність необхідності у реєстрації та її швидке завантаження дозволяє охопити велику аудиторію. Вибірку склали 76 громадян України, які проживають у Миколаївській області, Німеччині, Фінляндії та США. За результатами початкового анкетування “Інтернет-поведінка користувачів” виділено дві групи: які ймовірно можуть постраждати від методів соціальної інженерії та ті, хто вже мають такий гіркий досвід. У опитуванні взяли участь за статтю: жінки (64,9%) та чоловіки (35,1%) (рис. 2.1).

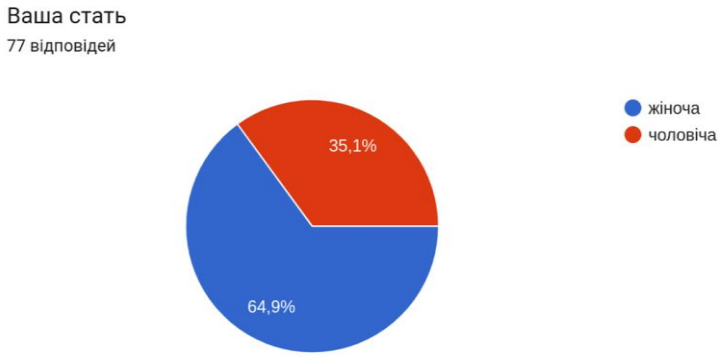



Рис. 2.1. Розподіл респондентів за статтю

Вікова категорія учасників розподілилася так: від 18 до 25 років – 13 чол. (16,9%), від 26 до 45 років 19 чол. (24,7%), від 46 до 60 років – 30 чол. (40,3%), від 61 до 75 років – 14 чол. (18,2%). Респонденти від 75 років не брали участь в анкетуванні, хоча така категорія була представлена в анкеті (рис. 2.2).

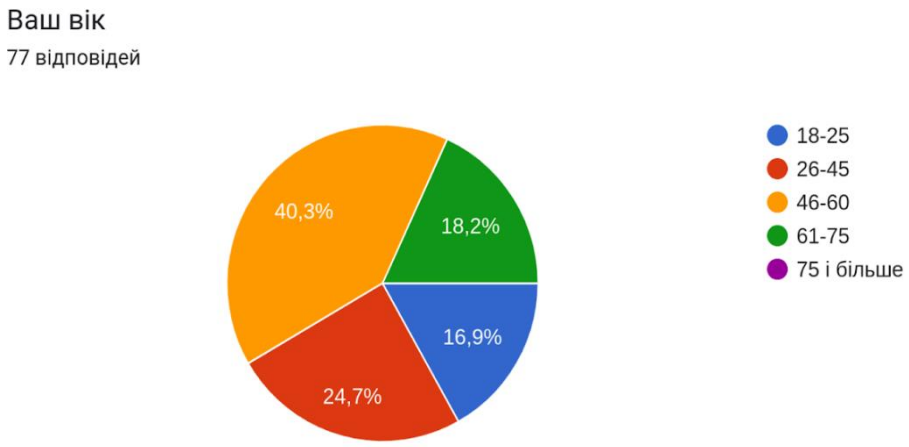



Рис. 2.2. Вікова категорія респондентів

У вибірці за зайнятістю респонденти розподілилися так: “працюю” перша група 48,78%, друга – 71,42%, навчаються у першій групі 21, 95% респондентів, у другій – 5,71%. Тимчасово не працюють 17,07% у першій групі опитуваних, 8,57% – у другій групі опитуваних. Пенсіонерами є у першій групі 2,44% респондентів, у другій – 11,43%. Є категорія респондентів, які є пенсіонерами і продовжують працювати. Ці дані представлені у табл. 2.1.

*Таблиця 2.1*

**Зайнятість користувачів Інтернету, які взяли участь в анкетуванні**

| Вид зайнятості | Користувачі Інтернету, які ймовірно можуть постраждати від онлайн шахрайства, перша група, (n =41) | | Користувачі Інтернету, які постраждали від онлайн шахрайства, друга група (n=35) | |
|---|---|---|---|---|
| | n | % | n | % |
| працюю | 22 | 53,66 | 25 | 71, 42 |
| навчаюся | 9 | 21,95 | 2 | 5, 71 |

| | | | | |
|---|---|---|---|---|
| тимчасово не працюю | 7 | 17,07 | 3 | 8,57 |
| пенсіонер | 1 | 2,44 | 4 | 11,43 |
| працюю і пенсіонер | 2 | 4,88 | 1 | 2,86 |

Серед показників зайнятості у респондентів, які постраждали від онлайн шахрайства найбільший відсоток працюючих, на другому місці – пенсіонери. Це дає нам припустити, що професійна діяльність та вік може вплинути на вразливість до впливу методів соціальної інженерії.

Цікавими є результати щодо вибору популярної соціальної мережі. Користувачам Інтернету було запропоновано 9 соціальних мереж: одним із питань було вибрати соціальні мережі, де зареєстровані, інше – у якій найбільше проводите часу. Найбільш популярними у користувачів Інтернету, які можуть ймовірно постраждати від онлайн шахрайства є: Facebook (19,51%), Telegram 24,39%), Instagram (21,95%), WhatsApp (14,63%), YouTube (14,63%), У користувачів Інтернету, які постраждали від онлайн шахрайства показники розподілилися: Facebook (31,43%), Telegram (17,14%), Instagram (17,14%), YouTube(14,29%). Отже, можна припустити, що Facebook може бути причиною того, що найбільша кількість постраждалих від шахрайства є користувачами саме цієї платформи.

Facebook має величезну аудиторію користувачів по всьому світу. Чим більше користувачів, тим більше потенційних жертв для шахраїв, які можуть спрямовувати свої атаки на цю платформу; дозволяє користувачам ділитися величезним обсягом особистої інформації, включаючи деталі про своє особисте життя, інтереси, місце роботи та навчання, фотографії тощо. На Facebook можна створювати підроблені сторінки або розміщувати підроблену рекламу, яка може виглядати автентично. Це може призвести до того, що користувачі будуть вважати шахраїв за довірені джерела або продукти. Завдяки своїм особливостям та широкому користувацькому базису, ця платформа може бути середовищем, де

багато користувачів можуть стати жертвами шахрайства через різноманітні маніпуляції та атаки.

За результатами комплексного тестування “Психоемоційний вимір взаємодії соціальної інженерії в Інтернеті” виявлено 31 постраждалого від шахрайства в онлайн-середовищі, з переважною більшістю проведено з ними бесіди та інтерв’ю.

Для констатувального етапу нашого емпіричного дослідження були використані наступні психодіагностичні методики:

Визначено ступінь управління своїми емоціями та адаптування до стресових ситуацій за допомогою психодіагностичної методики – тесту “Рівень емоційної стійкості” (автор Т. Тарасов, кандидат психологічних наук, психотерапевт вищої категорії). До тесту включено 10 тверджень, за результатами якого визначається  рівні емоційної стійкості (Додаток Б).

Методика Н. Холла – це психодіагностична методика для визначення здатності розуміти відносини особистості, що репрезентуються в емоціях і управляти емоційною сферою на основі прийняття рішень (Додаток А). Тест складається з 30 тверджень і містить 5 шкал: 1) емоційна обізнаність; 2) управління своїми емоціями (емоційна чуйність, емоційна неригідність); 3) самомотивація (довільне керування своїми емоціями); 4) емпатія; 5) розпізнавання емоцій інших людей (вміння впливати на їхній емоційний стан) [29, с. 29].

Найважливішими перевагами даної методики є її зручність, універсальність, інформативність, надійність, експрес-характер, можливість класифікації та зіставлення отриманих показників.

## 2.2 Аналіз варіативності поведінки та реакцій користувачів на різні методи соціальної інженерії

У ході констатувального етапу експериментального дослідження було отримано результати, узагальнення яких дало змогу визначити вплив методів соціальної інженерії на особливості психіки користувачів Інтернету.

Під час аналізу насамперед звертали увагу на сприймання та розуміння емоцій: емоційну обізнаність, усвідомлення емоцій; управління емоціями; самомотивацію; емпатію; розпізнавання і управління емоціями інших людей. Ці показники розглядалися за методикою Н. Холла [29, с. 30].

*Таблиця 2.2.*

**Результати діагностики за тестом Холла**

| Шкали | | Користувачі Інтернету, які ймовірно можуть постраждати від онлайн шахрайства (перша група) (n=45) | | Користувачі Інтернету, які постраждали від шахрайства в онлайн середовищі (друга група) (n=31) | |
|---|---|---|---|---|---|
| | | n | У % | n | у % |
| ЕмО | Н | 15 | 33,33 | 11 | 35,48 |
| | С | 22 | 04,89 | 14 | 45,16 |
| | В | 8 | 17,78 | 6 | 19,35 |
| УпрВЕ | Н | 32 | 71,11 | 18 | 58,06 |
| | С | 11 | 24,44 | 9 | 29,03 |
| | В | 2 | 04,44 | 4 | 12,90 |
| СамМ | Н | 20 | 44,44 | 13 | 41,92 |
| | С | 20 | 44,44 | 13 | 41,92 |
| | В | 5 | 11,11 | 5 | 16,13 |

| | | | | | |
|---|---|---|---|---|---|
| Е | Н | 18 | 40,00 | 13 | 41,94 |
| | С | 22 | 48,89 | 15 | 48,39 |
| | В | 15 | 33,33 | 3 | 09,68 |
| РозпЕІЛ | Н | 25 | 55,56 | 8 | 25,80 |
| | С | 17 | 37,77 | 19 | 61,29 |
| | В | 3 | 06,67 | 4 | 12,90 |

*Прим*.: 1) шкали за тестом Холла: ЕмО – емоційна обізнаність; УпрВЕ – управління власними емоціями; СамМ – самомотивація; Е – емпатія; РозпЕІЛ – розпізнавання емоцій інших людей; 2) рівні за тестом Холла: Н –низький рівень; С – середні рівень; В – високий рівень.

У табл. 2.2. наведені результати діагностики за тестом Холла, з якої ми бачимо, що в користувачів Інтернету обох груп рівні емоційної обізнаності є подібними. Проаналізувавши результати виявили, що найбільше респондентів мають середній рівень: у першій групі він склав 48,89%, у другій – 45,16%, низький рівень – 33,33% та 35,48% відповідно. Високий рівень емоційної обізнаності виявився у 17,78% та 19,35% опитуваних відповідно. На нашу думку, це свідчить про здатність розпізнавати, розуміти і керувати власними емоціями, а також емоціями інших людей. Можна припустити, що можуть виникнути труднощі у повному розумінні того, що спричиняє ці емоції, і вмінні керувати ними для досягнення позитивних результатів у взаємодії з іншими, в умінні захистити себе від впливу методів соціальної інженерії та в інтернет-просторі.

Порівнюючи респондентів обох груп, ми бачимо, що показник низького рівня шкали “Управління власними емоціями” у користувачів, які постраждали від шахрайства є істотно нижчим (58,06%), ніж у користувачів, які ймовірно можуть постраждати від шахрайства (71,11%).

За шкалою «Самомотивація» в першій групі респондентів низький рівень мають 44,44%, в другій – 41,92%, середній рівень склав – 44,44% та 41,92% відповідно. Це свідчить, що у користувачів Інтернету обох груп можуть зустрічатися проблеми з самомотивацією, з встановленням цілей, зосереджуванням на завданнях і працювати над їх виконанням, навіть коли зустрічає труднощі чи перешкоди (наприклад, вплив методів соціальної інженерії).

Шкалу “Емпатія” високий рівень представили користувачі інтернету першої групи – 33,33%, другої групи користувачів – 09,68%. Показники середнього і низького рівнів є подібними. Низький рівень емпатії показали третину респондентів першої групи, показники другої групи склали 41,94%. Це дає змогу зробити припущення, що такий показник як емпатія є важливим аспектом у житті користувачів Інтернету та відображає здоровий рівень співпереживання та соціальної компетентності.

Шкала “Розпізнавання емоцій інших людей” ми бачимо, що 55,56% користувачів першої групи мають низький рівень, а серед користувачів другої групи таких – 25,80 %. За цією ж шкалою 37,77% користувачів першої групи мають середній рівень, серед учнів користувачів другої групи таких більше – 61,29 %. Високий рівень визначився як: респонденти першої групи – 6,67%, респонденти другої групи – 12,90%. Отже, користувачі Інтернету, які ймовірно можуть постраждати від онлайн шахрайства є краще обізнаними у розпізнаванні емоцій інших людей порівняно з користувачами Інтернету, які постраждали від онлайн шахрайства. Результати дослідження за методикою Н. Холла представлені у діаграмі (рис. 2.3).


Рис. 2.3. Результати дослідження за методикою Н. Холла

Отже, можна припустити, що учасники нашої вибірки мають певні труднощі у розпізнаванні своїх і чужих емоцій, через це вони можуть не завжди адекватно реагувати на емоційні вияви у віртуальному середовищі. Їм може бути складно контролювати інтенсивність та зовнішні прояви своїх емоцій. Також можна припустити, що в них не вистачає вміння гармонійно взаємодіяти в міжособистісних відносинах, адекватно інтерпретувати емоції оточуючих, проявляти толерантність і соціальну адаптивність, досягаючи гармонії у своєму внутрішньому світі.

Тест “Рівень емоційної стійкості” (автор Т. Тарасов) (Додаток Б) проводився з двома зазначеними групами респондентів, складався з десяти питань. За результатами тестування середній рівень емоційної стійкості мають респонденти першої групи – 82, 93%, другої групи – 60,00%. Підвищений рівень емоційності показали результати користувачів, які ймовірно можуть постраждати від онлайн шахрайства – 17,17%, значно вищий цей показник у користувачів, які постраждали від онлайн шахрайства і склав 40%. Високого рівня емоційної стійкості, який базується на стабільній психіці не виявлено (табл. 2.3).

*Таблиця 2.3.*

**Результати тесту «Рівень емоційної стійкості» (автор Т. Тарасов)**

| Рівні емоційної стійкості | | Користувачі Інтернету, які ймовірно можуть постраждати від онлайн шахрайства (перша група), (n=45) | | Користувачі Інтернету, які постраждали від онлайн шахрайства (друга група), (n=31) | |
|---|---|---|---|---|---|
| | | n | у % | n | у% |
| | низький рівень емоційної стійкості | 0 | 0 | 0 | 0 |
| | середній рівень емоційної стійкості | 34 | 82,93 | 21 | 60,00 |
| | високий рівень емоційності | 11 | 17,17 | 10 | 40,00 |

Зазначимо, що нашу думку, однією із вразливістю до впливу методів соціальної інженерії за результатами тесту може бути висока емоційність, яка пригнічувати здатність людини до логічного мислення і аналізу ситуації. У таких випадках людина може діяти ірраціонально або бездумно, не враховуючи потенційні наслідки своїх дій.

Розвиток емоційної стійкості пов’язаний з формуванням прийомів саморегуляції, які відповідають індивідуальним особливостям людини [73, с. 380]. Результати цього дослідження дають змогу припустити, що більшість користувачів онлайн-спільноти, які постраждали від онлайн шахрайства мають високий рівень емоційності, що впливає на вразливість до маніпуляції через соціальну інженерію, оскільки знижує її здатність до аналізу та критичного мислення, а також підвищує схильність до впливу з боку інших.

За результатами тесту за картинками «Довіра» (Додаток В) респонденти розподілені на чотири рівня довіри. Високий рівень довіри спостерігається у більшості респондентів другої групи 54,29%, а у респондентів першої групи він значно нижчий, склав 36,58%, але це найбільший показник за рівнями у групі. Рівень, що визначається: обережний, не поспішає довіряти незнайомцям

розподілився так: респонденти першої групи – 19,51%, другої групи – 5,71% і є найнижчим показником за рівнями (табл. 2.4).

Тобто, можемо припустити, що у користувачів Інтернету, які мають високий рівень довіри значно збільшується вразливість до методів соціальної інженерії. Коли людина довіряє комусь або чомусь, вона схильна приймати інформацію та пропозиції цієї сторони без достатнього обміркування.

*Таблиця 2.4*

**Результати тесту за картинками «Довіра»**

| Рівні довіри | | Користувачі Інтернету, які ймовірно можуть постраждати від онлайн шахрайства (перша група), (n=45) | | Користувачі Інтернету, які постраждали від онлайн шахрайства (друга група), (n=31) | |
|---|---|---|---|---|---|
| | | n | у % | n | у% |
|  | Високий рівень довіри | 15 | 36,58 | 19 | 54,29 |
| | Довіра заробляється чесністю і взаємною повагою | 13 | 31,70 | 8 | 22,86 |
| | Обережний,не поспішає довіряти незнайомцям | 8 | 19,51 | 2 | 5,71 |
| | Вірить у добрі наміри оточуючих | 5 | 12,20 | 6 | 17,14 |

Після аналізу результатів тесту за картинками «Стиль ухвалення рішення» (Додаток Г) було визначено (табл. 2.5), що у користувачів, що ймовірно можуть постраждати від онлайн шахрайства спостерігаються більш високі показники «ретельного аналізу і розмірковування» та показники «рівня спокою у стресових ситуаціях», ніж у користувачів Інтернету, що постраждали від онлайн шахрайства. У відсоткових значеннях: 36,58% та 54,29% відповідно. На противагу, показник «спокій у стресовій ситуації» виявився значно нижчим у користувачів Інтернету, що постраждали від онлайн шахрайства (5,71%), ніж у

користувачів, що ймовірно можуть постраждати від онлайн шахрайства (19,51%).

*Таблиця 2.5.*

**Результати тесту за картинками «Стиль ухвалення рішень»**

| Рівні | | Користувачі Інтернету, які ймовірно можуть постраждати від онлайн шахрайства (перша група), (n=45) | | Користувачі Інтернету, які постраждали від онлайн шахрайства (друга група), (n=31) | |
|---|---|---|---|---|---|
| | | n | у % | n | у% |
|  | швидке ухвалення рішень | 15 | 36,58 | 19 | 54,29 |
| | ретельний аналіз і розмірковування | 13 | 31,70 | 8 | 22,86 |
| | спокій у стресових ситуаціях | 8 | 19,51 | 2 | 5,71 |
| | вдумливість та стратегічний підхід до життя | 5 | 12,20 | 6 | 17,14 |

Як бачимо, за результатами тесту швидке ухвалення рішення може бути супроводжене емоційною реакцією, яка робить людину більш схильною до впливу: може не врахувати всі можливі наслідки своїх дій, приймати інформацію на віру без аналізу або перевірки її достовірності, втрачена увага до деталей або підозрілих ознак, які вказують на спробу маніпуляції.

З метою збору інформації, діагностики методів соціальної інженерії, застосовувався такий інструмент як бесіда. Здійснена у двох варіантах: особиста зустріч та розмова по телефону. Учасниками стали ті користувачі Інтернету, які у початковій анкеті «Інтернет – поведінка користувачів» відповіли «так» на питання: Чи стикалися Ви з випадками шахрайства в мережі Інтернет? У ході особистої бесіди зафіксовані наступні методи соціальної інженерії, які

застосовувалися до користувачів віртуального середовища: фішинг (54,83%), вішинг (35,48%), приманка (2%), контекстуалізація (3,23%) (табл. 2.6.)

*Таблиця 2.6.*

**Методи соціальної інженерії, які застосовувалися до користувачів Інтернету, які постраждали від онлайн шахрайства (за результатами бесіди)**

| метод соціальної інженерії | Користувачі Інтернету, які постраждали від онлайн шахрайства, (n=31) | |
|---|---|---|
| | n | % |
| Фішинг | 17 | 54,83 |
| Вішинг | 11 | 35,48 |
| Приманка | 2 | 6,45 |
| Контекстуалізація | 1 | 3,23 |

Зважаючи на кожен метод соціальної інженерії, можна виділити психологічні вразливості: необережність (схильні до натискання на посилання або відкривання вкладень у повідомленнях електронної пошти, особливо якщо вони виглядають авторитетно або створюють враження невідкладності); довірливість (використання підміни ідентичності, щоб виглядати як довірені джерела, і викликати віру у їхню автентичність та намір); легковірність (вірити, що веб-сайти, які виглядають аутентично, насправді є легітимними); бажання допомогти (допомагати, коли здається, що хтось потребує допомоги і це призводить до небезпечного розкриття особистої інформації); емоційна реакція (страх, цікавість або радість, що призводить до недбалості у виконанні обдуманих дій); бажання отримати щось безкоштовно або дешевше; відчуття впевненості в безпеці; (схильні діяти без обдумування, особливо якщо ситуація здається невинною або звичайною) [109, с. 211].

Користувачі Інтернету нашої вибірки відповіли на питання авторської анкети «Психоемоційний вимір взаємодії соціальної інженерії в Інтернеті» (Додаток Г). Проаналізуємо декілька питань, запропонованих в опитуванні.

На питання: «Чи знаєте Ви, що таке «соціальна інженерія» і які вона може мати загрози?» “так” відповіли у першій групі респондентів 23,33%, у другій - 30%. Не знають, що таке соціальна інженерія 36,67% першої групи та 23,33% другої. На питання: «Ні, але хотів дізнатися» відповіли 40% респондентів першої групи та 46,67% другої групи респондентів. Отже, робимо висновок, що дві третіх опитуваних не знають, що таке соціальна інженерія, що, у свою чергу, свідчить про вразливість цієї категорії до впливу соціально-інженерних атак.

До речі, бажання дізнатися про маніпуляції за допомогою методів соціальної інженерії говорить про актуальність теми та нагальну потребу. Так, це питання розглядалося у телепрограмі «Сніданок 1+1» на каналі «1+1» 13 квітня 2024 року. Мова йшла про нові види фішингу та стратегії захисту від атак шахраїв.

Користувачам Інтернету вибірки було запропоновано дати відповідь на питання: «Чи відомі Вам схеми шахрайства, які можуть включати відправку фішингових листів або надання фальшивих пропозицій?» Результати розподілилися таким чином: ствердну відповідь надали 10% респондентів першої групи та 43,33% другої групи. Постраждали від цієї схеми шахрайства 3,33% респондентів тільки другої групи. Все це засвідчує, що постраждалі від методів соціальної інженерії знають про фішингові атаки на 13,33% більше, а хотіли дізнатися ширше про це саме користувачі, які ймовірно можуть постраждати від атак онлайн-шахрайства 33,33%, що на 16,66% більше, ніж постраждалі користувачі. Можемо припустити, що обізнаність користувачів Інтернету про методи соціальної інженерії бажає кращого.

Аналіз результатів емпіричного дослідження відповідно до завдань роботи вимагає їх розгляду у встановленні зв’язків взаємодії показників. Тому нами був застосований кореляційний аналіз Пірсона. Нам було важливо встановити існування кореляційних зв’язків між досліджуваними психологічними вразливостями користувачів Інтернету та впливу методів соціальної інженерії. Для цього ми проаналізували статистично значущі коефіцієнти кореляції за шкалами опитувальників, які встановили значущі кореляційні зв’язки.

Показники визначення рівня довіри статистично значущо корелюють з кількістю випадків онлайн шахрайства у користувачів Інтернету, які постраждали від атак соціальної інженерії (ремп.=-0.762 за $p \leq 0,05$) Трохи вище значення, теж статистично значуще отримано за результатами показників шкали “Управління власними емоціями” та показниками впливу інформації в соціальних мережах на емоції користувачів (ремп. = 0.84884 за $p \leq 0,01$). На нашу думку це свідчить про те, що між особливостями психіки користувачів Інтернету, таких як довіра, вміння управляти власними емоціями та фактами застосування методів соціальної інженерії існує тісний зв’язок.

Тобто, можна припустити, що користувачі Інтернету з певними психічними характеристиками, наприклад, низьким рівнем довіри або обмеженим вмінням керувати власними емоціями, можуть бути більш схильними до атак методами соціальної інженерії у віртуальному середовищі. Такий зв’язок може впливати на їхню поведінку та реакції на різноманітні шахрайські схеми та маніпуляції у мережі.

Показники визначення рівня емоційної стійкості статистично значущо корелюють з показниками ймовірністі того, що користувачі відповіли б на питання, яке обіцяє виграш чи нагороду (ремп.=0.6742 за $p \leq 0,05$). Отже, застосувавши коефіцієнт кореляції Пірсона (r-Пірсона) можемо підтвердити вплив методів соціальної інженерії на одну із психологічних особливостей користувачів Інтернету: емоційну стійкість. Це може бути пов’язано з більш впевненістю у собі, бажанням досягти успіху чи просто більшою готовністю до ризику.

Проаналізувавши результати дослідження науковців Samar Muslah Albladi та George R. S. Weir, можна зробити висновок, який співпадає з нашими висновками емпіричного дослідження. «Результати цього дослідження показують, що більшість розглянутих характеристик користувача впливають на вразливість користувачів прямо чи опосередковано. Це дослідження також робить внесок у наявні знання про соціальну інженерію в соціальних мережах, зокрема розширюючи область досліджень прогнозування поведінки

користувачів щодо загроз безпеці, пропонуючи нову перспективу впливу, соціально-емоційну, яка раніше не була задовільно описана в літературі, як параметр, що впливає на вразливість користувача» [81, с. 14].

### 2.3. Рекомендації для користувачів щодо розпізнавання та запобігання соціально-інженерним атакам

Для боротьби з методами соціальної інженерії необхідний комплексний підхід, який включає в себе технічні заходи захисту, політики безпеки, освіту користувачів та моніторинг поведінки.

У результаті проаналізованої наукової літератури, матеріалів сайтів, проведення емпіричного дослідження з користувачами Інтернету розроблені рекомендації, які можуть допомогти захистити психіку від негативного впливу соціальної інженерії та зберегти психічну стійкість в цифровому середовищі.

Будьте пильними та критичними: навчіться розпізнавати типові схеми маніпуляції та обману, які використовуються соціальними інженерами. Це можуть бути, наприклад, електронні листи або повідомлення, що виглядають як відомі компанії чи організації, але насправді мають небезпечні цілі. Пам’ятайте, що справжні компанії часто не запитують конфіденційну інформацію через електронні листи [34].

Довіряйте своїм інстинктам: важливо навчитися довіряти своїм внутрішнім почуттям та інтуїції. Якщо щось здається підозрілим або неправильним, це може бути сигналом про те, що необхідно бути пильними та обережними.

Зберігайте особисту інформацію конфіденційною: уникайте ділитися особистою інформацією в мережі, особливо в публічних чи ненадійних джерелах. Це може включати адресу, номери телефонів, розташування або будь-яку іншу особисту інформацію, яка може бути використана соціальними інженерами для вашої шкоди.

Створюйте сильні паролі: використовуйте унікальні та складні паролі для кожного вашого облікового запису. Ідеальний пароль повинен містити комбінацію великих та малих літер, цифр та спеціальних символів і бути достатньо довгим, щоб бути безпечним.

Перевіряйте джерела повідомлень: перед наданням особистої інформації або виконанням будь-яких дій перевірте автентичність джерела, з якого ви отримали повідомлення. Переконайтеся, що веб-сайт, електронний лист чи повідомлення відомі та довірені.

Не панікуйте: якщо ви виявили підозрілу активність або стали жертвою атаки соціальної інженерії, намагайтеся залишитися спокійними і зібрати якнайбільше інформації про ситуацію. Паніка може призвести до нерозсудливих дій.

Наголошуємо: якщо ви відчуваєте стрес або тривогу через вплив соціальної інженерії, звертайтеся за підтримкою до своїх друзів, родини або

фахівців з психологічної підтримки. Іноді просте обговорення проблеми може допомогти зняти нервове напруження.

А ось почуття довіри може бути інструментом як для захисту, так і для вразливості в контексті впливу соціальної інженерії. Пропонуємо декілька порад, як ефективно використовувати почуття довіри для захисту від негативного впливу.

Довіряйте, але перевіряйте: довіра – це важлива складова взаємодії з іншими людьми, але це не означає, що ви повинні сліпо довіряти кожному. Пам'ятайте про необхідність перевіряти джерела інформації та перевіряти достовірність отриманої інформації перед тим, як вірити в неї.

Розвивайте критичне мислення: навчіться аналізувати інформацію критично та об'єктивно. Запитуйте себе, чи може бути це правдою, чи є якась прихована мотивація за даним повідомленням чи запитом.

Будьте обережними з особистою інформацією: необхідно бути обережними з тим, кому довіряєте свою особисту інформацію. Хоча взаємодія зі своїми друзями та родиною зазвичай викликає почуття довіри, важливо пам'ятати про те, що це також може стати об'єктом атак соціальної інженерії.

Будьте свідомими онлайн-загроз: розумійте потенційні ризики, пов'язані зі спілкуванням в інтернеті та використанням онлайн-сервісів. Будьте обережними з наданням особистої інформації та дотримуйтесь основних правил кібербезпеки.

Будьте відкритими до обговорення: відкритість та готовність обговорювати свої побоювання зі своїми близькими або колегами можуть допомогти виявити можливі загрози та вирішити їх разом.

Довіряйте своїй інтуїції: якщо ви відчуваєте, що щось не так або що щось не відповідає, вам, навіть якщо здається, що у всіх інших є довіра до цієї особи або джерела інформації, вірте своїй інтуїції.

Коли відчуваєте бажання допомогти, але звертаються до вас шахраї в онлайн-просторі, важливо діяти розумно та обережно. Пропонуємо поради, які можуть допомогти у такій ситуації. По -перше, підтверджуйте ідентифікацію: перш ніж надавати будь-яку допомогу, переконайтеся, що ви спілкуєтеся з

правильною особою. Звертайте увагу на неперевірені електронні листи, повідомлення від невідомих осіб або будь-яку непередбачену взаємодію.

По-друге, не надавайте особисту інформацію. Уникайте надання особистої інформації, такої як номери банківських карток, паролі або адреси, навіть якщо вас про це просять. Справжній фахівець або організація ніколи не буде запитувати таку конфіденційну інформацію через електронні листи чи повідомлення.

По-третє, перевіряйте інформацію. Перевірте інформацію, надану незнайомою особою, особливо якщо це стосується прохань про фінансову допомогу чи вкладення грошей. Пошукайте незалежні джерела підтвердження перед тим, як діяти.

По-четверте, повідомте відповідні служби. Якщо ви підозрюєте, що ви маєте справу з шахраєм, повідомте про це відповідні служби або організації, такі як місцева поліція, банк чи антифраудові агентства.

А також будьте обережними з посиланнями та вкладеннями! Уникайте натискати на сумнівні посилання або відкривати вкладення в електронних листах від невідомих або недовірених джерел. Це може призвести до вірусів, шпигунського програмного забезпечення або інших видів кіберзлочинності.

Найважливіше – запам’ятайте, що не зобов'язані виконувати прохання незнайомців у мережі, особливо якщо вони вимагають надання особистої інформації чи фінансових ресурсів. Перш ніж допомогти, завжди перевіряйте та дійте з обережністю.

Не слід також забувати і про сповіщення про такі небезпеки інших членів сімей. Адже часто літні люди, наприклад, можуть не знати про те, що розголошення CVV-коду банківської картки може призвести до викрадення грошей.

Поширюйте інформацію про онлайн-шахрайство та методи, які використовуються шахраями серед своїх друзів, родичів та співробітників. Чим більше людей буде обізнаних з цими методами, тим менше ймовірність, що вони стануть жертвами.

Використання критичного мислення є важливим у ситуаціях, коли стикаєтесь з потенційними шахраями в онлайн-просторі. Розберіться з основними методами шахрайства в Інтернеті, такими як фішинг, соціальна інженерія, шахрайство через телефон, і т. д. Чим краще розумієте загрози, тим ефективніше ви зможете їм запобігти.

Очевидним є той факт, що кіберзагрози стрімко зростають через поточні події та впливають на нас різними способами. Політика кібербезпеки важлива, оскільки кібератаки та викрадання потенційно дорого коштують, особливо в час війни. Посилення захисту від загроз, що постійно змінюються, стане легшим зі знанням нових технологій кібербезпеки, методології, тактики та організаційної структури.

## Висновки до другого розділу

У другому розділі проводилося емпіричне дослідження емоційної стійкості, емпатії, довіри, стилів ухвалення рішень, які на нашу думку, є вразливими під час атак соціальної інженерії в Інтернеті. Також цікавою була робота щодо виявлення методів соціальної інженерії від яких постраждали респонденти та вплив на особливості їхньої психіки.

Дослідження проводилося серед користувачів інтернет-спільноти (41 респондент) та тих користувачів Інтернету, які постраждали від атак методів соціальної інженерії (35 респондентів). Вибірку склали 76 громадян України, які проживають у Миколаївській області, Німеччині, Фінляндії та США. Психодіагностичні методики, тести за картинками та анкетування були спрямовані на вивчення дій, емоцій, поведінки користувачів.

Провівши емпіричне дослідження, використовуючи різні методи, можна зробити висновки, що шахраї все більше використовують різних методів соціальної інженерії для досягнення протиправних цілей. Йдеться про спеціальну методику маніпулювання людьми котра змушує останніх віддавати злочинцям необхідну інформацію. Безумовно таке можливо, адже ми люди і маємо свої слабкості та схильність приймати рішення спираючись на власні емоції. Зазначене явище є досить розвинутим в Україні. З упевненістю можна

сказати, що більшості хоча б одного разу надходив електронний лист чи СМС-повідомлення, де повідомлялось, що ти виграв автомобіль або твоя банківська платіжна карта заблокована і, лише зателефонувавши за вказаними номерами, можна отримати виграш чи розблокувати карту. Саме такими надзвичайно простимо діями шахраї намагаються отримати доступ до наших персональних даних (конфіденційної інформації) з метою, яка явно не спрямована на наше збагачення чи забезпечення нашої інформаційної безпеки. Соціальна інженерія спирається на психологічні особливості людини, такі як: я повинен зробити так, бо більшість так би і зробили (ми оцінюємо свою поведінку на фоні поведінки більшості); повага до авторитетних людей чи державних установ.

Тож соціальна інженерія – це те, проти чого не існує прийому, оскільки атакують людину. І відносно до стрибкоподібного росту технологій, мозок людини не еволюціонував настільки швидко та не опанував навичок виявлення і протидії соціальній інженерії, крім наявності критичного мислення та надмірної підозрілості.

Отже, отримані результати кореляційний аналіз підтвердили нашу гіпотезу про те, що існує зв’язок між особливостями психіки користувачів Інтернету та методами соціальної інженерії. Вивчалися такі вразливості як довіра, емпатія, стиль ухвалення рішення, емоційна стійкість. Інтернет-простір завдяки своїм особливостям та широкому користувацькому базису, може бути середовищем, де багато користувачів можуть стати жертвами шахрайства через різноманітні маніпуляції та атаки, тому доцільним є ознайомлення з рекомендаціями щодо розпізнавання та запобігання соціально-інженерним атакам.

# РОЗДІЛ 3.
# ТЕОРЕТИКО-ЕКСПЕРИМЕНТАЛЬНЕ ЗАСТОСУВАННЯ ТРЕНІНГОВОЇ РОБОТИ З КОРИСТУВАЧАМИ ІНТЕРНЕТУ ТРЕТЬОГО ВІКУ ДОРОСЛОСТІ

## 3.1. Методологічні засади, зміст і процедура програми тренінгу захисту від шахрайства та маніпуляцій в інтернеті для користувачів пенсійного віку

Взаємозв'язок між використанням соціальних мереж та психологічним функціонуванням не є простим і однозначним і залежить від багатьох факторів, таких як спосіб його використання, патерни комунікації, емоційний стан, супутні захворювання, самоусвідомлення, мотивація, цінності, атитюди та преференції. Сьогодні ми не можемо уникнути кіберпростору, в якому проходить значна частина нашого життя. Від нашого вміння ефективно взаємодіяти в ньому залежить здоров'я і благополуччя як окремого індивіда, так і суспільства в цілому [14, с. 119].

На думку дослідниці Н. Лавріненко пенсіонери як соціальна група рідко є предметом соціологічних, психологічних та економічних досліджень. На жаль, можливо несвідомо, суспільствознавці користуються стереотипними уявленнями про цю соціальну групу, як про неперспективну й нецікаву для майбутнього країни. Однак у сучасних спільнотах, коли після виходу на пенсію значна частина пенсіонерів живе і двадцять, а іноді і тридцять років, виникає завдання вивчення місця цієї соціальної групи в соціальній структурі кожного суспільства й відповідно адаптації цих людей до швидко мінливих соціально-економічних умов життя [38, с. 330]. Також актуальним є завдання розроблення певної соціальної політики щодо цієї категорії населення

Україна належить до країн з великою часткою населення у пенсійному віці. На початок жовтня 2024 року кількість населення, яка має соціальний статус пенсіонера становить 10,34 млн.чол. [79]. На тлі існуючої загальної тенденції зниження чисельності населення у нашій країні його старіння в найближчі десятиріччя прогресуватиме, збільшуватиметься частка людей похилого віку, що

потребує значних зусиль з боку суспільства із забезпечення гідного життя для цієї категорії населення. У наші дні старість і пов'язаний з нею вихід на пенсію є поняттям, що визначається законом. Мається на увазі вікова межа, коли більшість людей закінчують трудову діяльність і можуть розраховувати на різні види соціальної підтримки, зокрема на пенсію[38, с. 334].

Зміна акцентів на перспективу більш збалансованого стилю життя у похилому віці скерувала увагу вчених на способи підтримання продуктивного й активного довголіття, а також на позитивні наслідки такого стилю життя як для осіб похилого віку, так і для суспільства загалом. Таким чином, новий напрям у геронтології – позитивна геронтологія – ґрунтується на конвергенції трьох груп досліджень з проблем благополучного довголіття: успішне старіння, продуктивна діяльність і громадянська взаємодія, які акцентують на важливості залучення людей похилого віку до активності та до виконання суспільно важливих ролей [91, с. 32].

Разом з тим, результати досліджень у сфері геронтології доводять пряму залежність рівня когнітивної здатності людей похилого віку від систематичного розумового навантаження (вправляння) так само, як і фізичне функціонування підтримується регулярною фізичною активністю[71, с. 176].

П. Ласлетт підкреслює, що «третій вік – це час пошуку для старших людей шляхів взаємодії з іншими та збереження культурної спадщини, з якої вони користали» Необхідно наголосити, що невід'ємною умовою успішного старіння у третьому віці вчений визначив навчальну діяльність людини[100, с. 89].

Оскільки навчальна діяльність є одним з найбільш ефективних способів підтримання рівня когнітивної здатності людини, то залучення осіб похилого віку в освітній процес переосмислюється, і можливості навчання у похилому віці стають реальністю і навіть необхідністю. Вищий рівень освіти людей похилого віку позитивно пов'язаний з більш успішним старінням. Освітня діяльність осіб похилого віку – один з головних чинників їх адаптації до швидкозмінних умов суспільного життя [96, с. 215].

Адаптація – основна навичка виживання, тому зрозуміло, що освіта у похилому віці стає невід'ємною складовою успішного довголіття [70,с.28]. Концепції успішного старіння, позитивного старіння і громадянської взаємодії підтримують позитивний погляд на ресурсний потенціал осіб похилого віку. Кожна з цих концепцій визнає, що похилий вік може бути періодом взаємодії, співробітництва і благополуччя [83, с. 185].

Водночас, можна вважати, що їх підґрунтям є теорія активності, в основі якої доказ позитивного впливу активності на її відчуття задоволення від життя, а також на теорії неперервності, яка стверджує, що людина адаптується до процесу старіння через пристосування тривалості, типу і розподілу діяльності. Основні принципи активності залишаються відносно стійкими упродовж всього життєвого курсу людини [91, с. 34]. Концепція успішного старіння Д. Рова і Р. Кана (J. Rowe, R. Kahn) визначає роботу (в розумінні «заняття») як вагому складову успішного старіння і виокремлює участь у продуктивній діяльності як один з її елементів [70, с. 28].

Важливим є проведення специфічного тренінгу для літніх людей, де вирішуються такі загальні для них проблеми, як соціальна реадаптація до нової життєвої ситуації.

Громадянська взаємодія – діяльність, що здійснюється людьми похилого віку задля загального блага, – це «громадська» форма продуктивної діяльності, яка також є компонентом успішного старіння [71, с. 302]. Необхідно наголосити, що дослідження в усіх трьох сферах (успішне старіння, продуктивне старіння і громадянська взаємодія) доводять, що залучення осіб похилого віку у продуктивну діяльність часто має позитивний вплив [71, с. 339].

І. Коваленко підкреслює, що напрям наукових досліджень за напрямом теоретико-методологічних засад цифрової трансформації освіти дорослих постійно розвивається, і це пов'язано з цифровими трансформаціями сучасного суспільства та освітніми потребами зрілих людей і людей поважного віку, частка яких у віковій структурі суспільства має тенденцію до зростання [26, с.32].

Необхідним елементом цифрового життя є кібергігієна, оскільки вона допомагає забезпечувати захист даних та інформації в інтернеті. Розвиток технологій дозволяє легко отримувати доступ до різних сервісів та даних, але це також збільшує нашу вразливість перед кіберзлочинцями. Тому важливо дотримуватися правил та практик кібергігієни та кіберосвіти [80, с. 169].

Кібергігієна важлива тоді, коли ми тримаємо телефон у руках та ділимося особистою інформацією в соціальних мережах, відповідаємо на повідомлення від незнайомців чи не помічаємо незвичайної поведінки друзів онлайн. Справжній захист вимагає такого ж уважного ставлення до дій в мережі, як і офлайн. Хоча кіберзлочинець не може завдати фізичної шкоди, його хитрість може використати вашу необережність для отримання ваших даних або грошей. Таким чином, правила кібергігієни є своєрідними манерами та навичками самозахисту у цифровому середовищі [12, с. 26].

Саме розглядаючи тему вразливостей психіки користувачів онлайн середовища методами соціальної інженерії, через призму позитивної геронтології, враховуючи результати емпіричного дослідження, проаналізованого у другому розділі, виникла потреба у розробці та проведенні тренінгу з громадянами третього віку дорослості. А саме: для учасників клубу активного довголіття «Ти – не один», що проживають у селищі Доманівка.

Як показали результати опитування люди старшого віку часто більш довірливі, ніж молоді люди, і можуть бути більш схильними до маніпуляцій. Вони можуть менше довіряти сучасним технологіям і мати менше досвіду в розпізнаванні шахрайських схем.

З розвитком технологій зростає і кількість кіберзлочинів, спрямованих на пенсіонерів. Шахраї часто використовують емоційний шантаж, обіцянки легкого заробітку або погрози, щоб виманити у людей гроші або особисту інформацію.

Технологія може принести переваги дорослим, які виходять на пенсію, пропонуючи вирішення труднощів у переході до пенсії. І навпаки, інтернет-технології можуть призвести до додаткових проблем для літніх людей, наприклад, підвищеної вразливості до онлайн-віктимізації [106, с. 1].

Психологічний тренінг допоможе розвинути вміння розпізнавати маніпулятивні методи та захищатися від них.

О. Жмурко зазначає, що особливу увагу потрібно приділити дослідженню психологічних аспектів соціальної інженерії, розробці інтерактивних навчальних програм для підвищення обізнаності користувачів [21, с. 40].

Саме соціально-психологічний тренінг спрямований на розвиток критичного мислення, яке є важливим для захисту від соціальної інженерії. В таких тренінгах акцент робиться на навчанні пенсіонерів розпізнавати ознаки шахрайства, ставити під сумнів підозрілі повідомлення чи дзвінки та не піддаватися емоційним маніпуляціям. Це допомагає знизити ризик того, що людина зробить необдумані дії під тиском або емоційними впливами з боку шахраїв.

Зазначимо, що тренінг, як засіб адаптації людини до нової діяльності, перепрограмування поведінки та діяльності особи, у минулому сторіччі отримав широке визнання і впровадження у різні сфери людської діяльності. У сучасних умовах тренінг став одним з провідних засобів навчання, які спрямовані на формування і розвиток компетентностей [5, с. 11].

Метод соціально-психологічного тренінгу запропонував у 70-х роках XX століття М. Форверг, який працював у Лейпцигському та Йенському університетах. Засобами тренінгу виступали рольові ігри з елементами драматизації, що створювали умови для ефективного формування комунікативних навичок [33, с. 3].

Соціально-психологічний тренінг має дві фази – діагностичну та корекційну [78, с. 408]. Під час діагностичної фази тренінгу виконуються такі завдання: пізнання своїх особистісних якостей, комунікативних особливостей, рефлексія власного спілкування та поведінки; інформації про сприймання кожного учасника тренінгу як особистості, його вміння спілкуватися з людьми [60, с. 8].

Під час корекційної фази соціально-психологічного тренінгу окреслюються шляхи удосконалення психологічної компетентності, вироблення

у них певних якостей, таких як емоційна стійкість, здатність контролювати свої емоції та не піддаватися маніпуляціям [78, с. 409].

Саме через вправи практичного змісту тренінг вчить людей похилого віку конкретним крокам для захисту особистих даних та фінансової безпеки. Наприклад, як встановити двофакторну автентифікацію, як перевіряти надійність джерела повідомлень або як безпечно спілкуватися в соціальних мережах, як керувати своїми емоціями та розвивати критичне мислення.

Мета тренінгу “Твій цифровий щит” для людей третього віку дорослості:

1) ознайомити учасників з основними методами кібершахраїв та соціальної інженерії;

2) розвинути навички розпізнавання кіберзагроз;

3) навчити учасників використовувати психологічні засоби для підвищення своєї захищеності в онлайн-середовищі;

4) сприяти розвитку критичного мислення та самоконтролю.

Тренінг складається з 6 тренінгових занять. Кожне заняття має наступну структуру (вона повторюється кожної групової зустрічі):

1) привітання учасників, вправа-розминка;

2) ознайомлення з метою і загальним регламентом заняття;

3) обговорення очікувань та визначення правил роботи;

4) теоретико-практичний блок (інформування учасників);

5) виконання тематичних вправ із застосуванням різноманітних технік;

6) підбивання підсумків заняття;

7) групова та індивідуальна рефлексія.

Початок кожного тренінгового заняття спрямований на створення сприятливої психологічної атмосфери для подальшої роботи. Ця частина заняття зорієнтована на майбутнє і значною мірою визначає організованість та ефективність усього тренінгового процесу.

В основній частині заняття реалізується тематичне інформування за проблематикою заняття та вправи.

Завершальна частина – це можливість дати відповіді на запитання, які у ході основної частини були висвітлені недостатньо; визначити, наскільки результативно учасники заняття опрацювали запропонований матеріал; з'ясувати чи справдилися їхні очікування; сприяти усвідомленню змін на індивідуальному рівні; визначити перспективи застосування опрацьованого матеріалу у реальному житті [5, с.3 8].

В основу розробки змісту та структури циклу тренінгів покладено такі принципи тренінгової роботи [47, с. 8]:

1) принцип активності учасників (у процесі роботи дуже важливо залучити кожного у тренінговий процес, не дати можливості «заховатися» пасивним учасникам за активними особистостями);

2) принцип партнерського спілкування (ефективність і дієвість заняття значною мірою зумовлена визнанням цінності особистості кожного учасника тренінгу);

3) принцип дослідницької позиції (дуже важливо у процесі роботи з пенсіонерами самостійно знаходити відповіді на ключові питання, що піднімаються тренером);

4) принцип набутих компетенцій (тренінгові вправи підібрані з максимальною наближеністю до реального життя для уможливлення перенесення нового досвіду і його закріплення в практиці);

5) принцип екологічності (під час занять важливо створити безпечні та комфортні умови для роботи тренінгової групи, у яких зміни й особистісні трансформації здійснюються з урахуванням етичних засад психологічної практики та екологічності прийомів психологічного впливу) [47, с. 8-9].

Так як заняття проводилися з людьми похилого віку, враховувалися методологічні засади програми тренінгу, які базуються на принципах андрагогіки (науки про навчання дорослих), специфіки психологічних особливостей людей пенсійного віку, а також на сучасні підходи до навчання кібербезпеки [40, с. 26]. А саме:

1. принцип адаптивності, адже навчальні матеріали повинні бути доступними та зрозумілими для людей пенсійного віку з різним рівнем знань та досвіду користування інтернетом. Це вимагає використання простої та зрозумілої мови, уникання технічних термінів або пояснення їх значення;

2. принцип поступовості зосереджує на тому, що навчання має бути структурованим таким чином, щоб спершу покривати базові аспекти захисту від шахрайства в інтернеті, а потім переходити до більш складних тем. Це дозволить слухачам краще засвоїти матеріал і не перевантажуватись інформацією.

3. принцип підтримки та мотивації. Важливим аспектом навчання людей пенсійного віку є підтримка на всіх етапах тренінгу. Ведучі мають створити дружню та підтримуючу атмосферу, щоб учасники відчували себе комфортно і могли ставити питання без страху помилитися [35, с. 8].

На підготовчому етапі проведено аналіз рівня володіння учасниками базовими навичками користування інтернетом та цифровими пристроями. Це дозволяє адаптувати програму тренінгу під конкретні потреби та рівень знань слухачів.

Також проведено анкети: “Інтернет-поведінка користувачів” та “Психоемоційний вимір взаємодії соціальної інженерії в Інтернеті”. Перше анкетування спрямоване на дослідження цифрової поведінки та рівня кібербезпеки користувачів онлайн-середовища літнього віку. Це дало змогу виявити найбільш поширені загрози та вразливості, з якими стикаються пенсіонери в мережі Інтернет, зрозуміти психологічні аспекти сприйняття інформації та взаємодії з цифровим середовищем, ідентифікувати фактори, що впливають на довіру до інформації в Інтернеті та готовність стати жертвою шахрайства.

Друге анкетування дало змогу оцінити рівень обізнаності пенсіонерів щодо соціальної інженерії в інтернеті та їхню вразливість до таких атак. За результатами анкетування скоригована програма проведення занять. Ці ж анкетування були запропоновані учасникам і по закінченню роботи тренінгу

«Твій цифровий щит». Аналіз результатів як індикатор якості проведення тренінгових занять наведено у підрозділі 3.2.

Зміст програми тренінгу «Твій цифровий щит» зосереджений на актуальних загрозах, з якими можуть стикатися користувачі пенсійного віку в інтернеті. Основні теми, що охоплюються в тренінгу, включають:

1. Основи безпечного користування інтернетом:

- роз’яснення термінології: кібершахрайство, маніпуляції, кіберзагрози, соціальна інженерія;

- основні правила безпеки в інтернеті: використання надійних паролів, двофакторна автентифікація, оновлення програмного забезпечення;

- налаштування безпеки на пристроях: мобільні телефони, планшети, комп'ютери.

2. Виявлення шахрайських дій:

- основні види шахрайства в інтернеті: фішинг, вішинг, підроблені сайти, виманювання персональних даних та коштів;

- як розпізнати фальшиві електронні листи, повідомлення та посилання.

- практичні вправи на виявлення фішингових та вішингових спроб.

3. Соціальні мережі та приватність:

- основні загрози в соціальних мережах: злам акаунтів, поширення неправдивої інформації, маніпуляції;

- як захистити особисті дані в соціальних мережах: налаштування приватності, обмеження доступу до інформації;

- поради щодо безпечного спілкування в інтернеті: як розпізнати маніпуляції, шахрайські схеми у спілкуванні з незнайомцями.

4. Захист від фінансового шахрайства:

- як безпечно здійснювати покупки в інтернеті: вибір надійних магазинів, захист платіжної інформації;

- як уникнути інтернет-шахрайства: повідомлення про виграші, підозрілі пропозиції, кредитні пастки;

- практичні поради з захисту банківських рахунків та фінансової інформації.

5. Поведінка у разі шахрайства:

- що робити, якщо стали жертвою шахрайства: алгоритм дій, повідомлення відповідних служб;

- як правильно зберігати докази шахрайських дій;

- поради щодо відновлення втрачених даних або засобів.

Отже, основна частина включає серію занять, на яких поступово розглядаються ключові теми. Кожне заняття складається з теоретичної частини та практичних завдань, що дозволяє закріпити отримані знання. Кожен етап тренінгу містить:

1. Презентацію з основної теми (з використанням зрозумілих візуальних матеріалів).

2. Демонстрацію реальних прикладів шахрайських дій (наприклад, фальшиві електронні листи, підроблені сайти).

3. Практичні вправи для слухачів (розпізнавання шахрайських дій, налаштування захисту на пристроях тощо).

Після кожного заняття учасники отримують короткі тести для перевірки засвоєного матеріалу. Після завершення всієї програми тренінгу проводиться підсумкове оцінювання, щоб виявити рівень засвоєних знань та вмінь. Зворотний зв’язок від учасників тренінгу дозволяє вдосконалити програму для майбутніх груп.

Для підтримки результатів навчання учасникам надаються інформаційні матеріали у вигляді пам’ятки, які допоможуть закріпити знання і навички, а також надалі звертатись за консультаціями у випадку необхідності. Причому, основні її положення розроблялися самими учасниками під час практичного заняття тренінгової програми.

Саме навчання зможе допомогти користувачам онлайн-простору розпізнавати шаблони, які можна використовувати для виявлення атак

соціальної інженерії, навчання стратегіям боротьби з поточними атаками та покращення оцінки загроз і сприйняття ризику [6, с. 12].

Таким чином, розроблена програма тренінгу «Твій цифровий щит» для користувачів пенсійного віку, орієнтована на захист від шахрайства та маніпуляцій в інтернеті, є важливою складовою підвищення цифрової грамотності серед цієї групи населення. Методологія навчання враховує специфіку вікової категорії, забезпечує практичне закріплення знань та орієнтується на реальні загрози, з якими пенсіонери можуть стикатися в інтернеті. Тренінг допоможе користувачам пенсійного віку краще розуміти основи психологічного впливу методами соціальної інженерії, керувати своїми емоціями, аналізувати прояви маніпуляції та уникати шахрайства, зберігати свої персональні дані та фінанси у безпеці.

Німецькі науковці Peter Schaab, Kristian Beckers, Sebastian Pape у своїх дослідженнях підкреслюють, що саме робота з протидії методам соціальноїх інженерії повинна бути мультидисциплінарною. Соціальна інженерія зосереджена на експлуатації людської поведінки, і це недостатньо розглядається в IT-безпеці. Натомість більшість оборонних стратегій розробляють експерти з IT-безпеки, які мають досвід роботи з інформаційними системами, а не з людською поведінкою та психологічними вразливостями [109, с. 207].

### 3.2. Аналіз та інтерпретація результатів проведення тренінгової програми “Твій цифровий щит”

Цей розділ присвячений детальному аналізу та інтерпретації результатів, отриманих в ході проведення соціально-психологічної тренінгової програми «Твій цифровий щит». Мета цього дослідження полягає у визначенні ефективності програми у підвищенні рівня цифрової грамотності та кібербезпеки серед осіб пенсійного віку, а також у виявленні динаміки змін їхніх знань, умінь та ставлень до використання цифрових технологій через призму психологічних факторів мотивації та самооцінки, що впливають на сприйняття інформації та прийняття рішень у цифровому середовищі.

Як зазначалося, на початковому та завершальному етапах тренінгових занять проведено анкетування та тестування. Використані методи: кількісний аналіз – статистична обробка даних анкетування, проведеного до та після тренінгу. Це дозволило виявити кількісні зміни в рівні знань, умінь та ставлень учасників. Якісний аналіз – аналіз відповідей на відкриті питання анкет, що дозволило виявити якісні зміни в сприйнятті учасниками інформації про кібербезпеку та їхню готовність застосовувати отримані знання на практиці.

Соціально-психологічний тренінг «Твій цифровий щит» проходив у вересні – жовтні 2024 року на базі публічної бібліотеки Доманівської селищної ради Миколаївської області та проходив у рамках проєкту «Здобуття цифрових навичок у бібліотеках-Хабах цифрової освіти» за підтримки Програми розвитку ООН (UNDP) в Україні у межах «Проєкту підтримки Дія» [7]. Включав у себе 6 занять по 90 хвилин. Інформацію про проходження занять опубліковано на сторінці закладу соціальної мережі «Фейсбук» (https://www.facebook.com/domanlibfree?locale=uk_UA).

Участь у тренінгу взяли 18 членів клубу активного довголіття “Ти – не один” – мешканці селища Доманівка. Клуб створений за ініціативи ветеранської організації у 2017 році, девіз якого: «Вдихаємо щастя – видихаємо добро». Мета діяльності – формування соціальної активності літніх людей через організацію комунікації різних поколінь, що позитивно впливає на осіб третього віку дорослості, допомагає розвити здібності, підтримує спілкування, мислення, інтелект, впливає на підняття життєвого тонусу та дає можливість радіти життю і зрозуміти значущість їх ролі в суспільстві. 20 % учасників тренінгу брали участь у емпіричному дослідженні у лютому – квітні 2024 року, що стало основою розробки та проведення тренінгу такого типу.

Цікавим є той факт, що найстаршій учасниці тренінгу – 94 роки, наймолодшій – 60 років. Щодо статі учасників тренінгу: жінок – 14, що склало 77,8%, чоловіків – 4, що становить 2,2 % (жінки у такий період життя, як правило, активніші та з натхненням беруть участь у таких заходах).

Перше заняття передбачало знайомство, розробку правил роботи тренінгу, збір інформації про випадки шахрайства в онлайн-середовищі, з якими стикалися учасники тренінгу (https://bit.ly/3Atcs6L).

Виявилося, що 17 з 18 пенсіонерів особисто стикалися з проявами інтернет-шахрайства. Види методів соціальної інженерії розподілилися наступним чином: вішинг – 69%, фішинг – 23%, онлайн покупка – 8% (рис. 3.1). Під час розповіді учасники згадували про свої емоції та почуття під час дії методів соціальної інженерії, їх реакції та подальші дії.

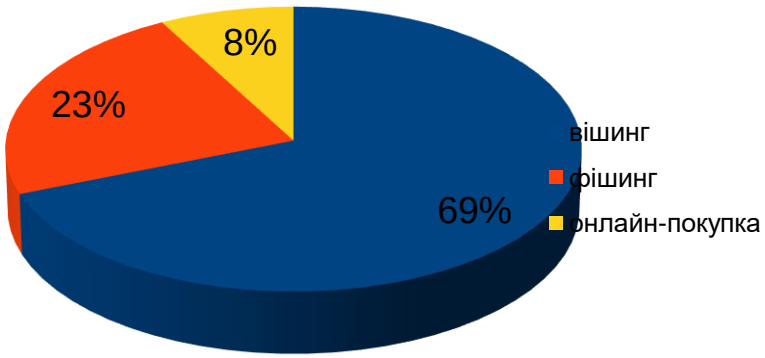



Рис. 3.1. Схеми шахрайства, з якими особисто зустрічалися учасники тренінгу

Щодо переліку соціальних мереж, де найбільше проводять час користувачі-пенсіонери, розподіл виявився передбачуваним (рис. 3.2.)

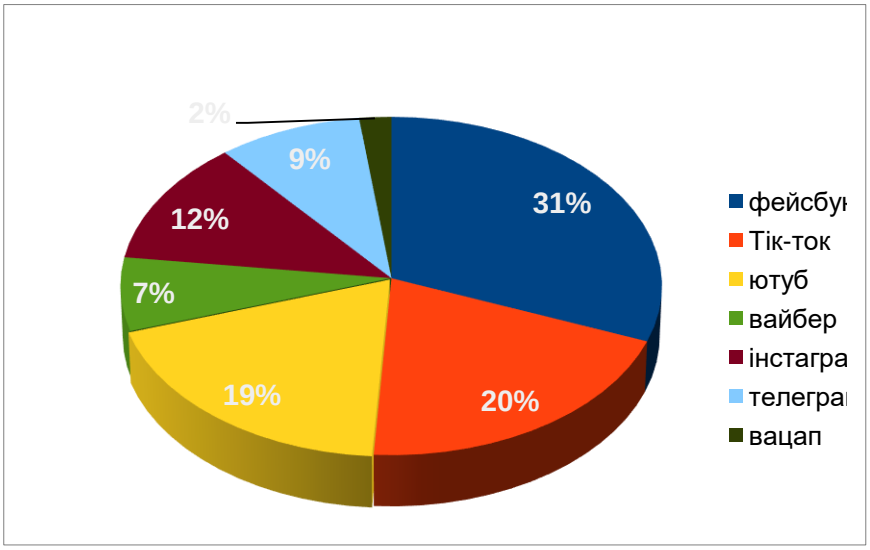



Рис. 3.2. Соціальні мережі, в яких учасники тренінгу проводять найбільше часу

Після теоретичної частини про особливості психіки користувачів інтернету, за допомогою яких шахраї маніпулюють під час “впровадження” своїх шахрайських дій, проаналізовані ситуації, що відбулися з учасниками тренінгу. Для цього використовувалися методи бесіди та інтерв’ю.

Група діяла активно, тому програму першого заняття виконано на 100%. Була проведена вправа для комфортного емоційного настрою всередині групи, та для саморозкриття. Наприкінці заняття обговорили початкові очікування та отримані враження.

Друга зустріч базувалася на отриманні нових знань. Продемонстровано лекцію з використанням відео роликів та презентації на тему: «Розгадай таємниці кіберзлочинців», яка мала на меті допомогти розвинути критичне мислення та навички розпізнавання шахрайських схем. Наступний крок – вправи та методи дослідження особистісних цінностей (проєктивна методика «Геометричні фігури» (Сьюзен Деллінгер) [22, с. 33], методика «Особистісна готовність до змін») [22, с. 29].

Вправа «Розпізнай шахрая» – рольова гра. Були розподілення ролі між учасниками: шахрай та пенсіонер, дані конкретні ситуації кожній парі та завдання розіграти їх. Мета – краще зрозуміти психологію шахрая та навчитися відмовляти на його пропозиції. На завершення – обмін та обговорення думок (https://bit.ly/4ftmGTj).

Третя зустріч була спрямована на навчання пенсіонерів конкретним крокам для захисту особистих даних та фінансової безпеки. Використовуючи відеоролики освітнього серіалу «Обережно! Шахраї (https://osvita.diia.gov.ua/courses/attention-cyber-fraudsters), розробленого Міністерством цифрової трансформації України, навчалися, як встановити двофакторну автентифікацію, як перевіряти надійність джерела повідомлень або як безпечно спілкуватися в соціальних мережах. На завершення проведена вправа «Скарбничка знань». Кожен учасник записував на папірець одну пораду з кібербезпеки, яку він запам’ятав. Потім всі поради зібралися в одну «скарбничку».

Четверте заняття мало на меті розвинути у пенсіонерів навички критичного мислення, щоб вони могли ефективніше оцінювати інформацію в Інтернеті та захищатися від кіберзагроз. Вправа «Правда чи брехня?» викликала багато дискусій. Активно аналізували, які аргументи наведені, як представлено факти, чи є емоційне забарвлення. Після цього обговорили, як можна відрізнити правдиву інформацію від маніпулятивної. Матеріали подавалися як текст та картинки. Продовженням цієї теми стала вправа «Фейкові новини» – перегляд відео роликів з обґрунтуванням, чому вони можуть вважати інформацію неправдивою, на що звернули увагу (наприклад, відсутність джерел, перевіреність фактів тощо), вчилися критично оцінювати медіаконтент.

П’яте заняття присвячене розвитку емоційної стійкості, покращення навичок саморегуляції та зниження рівня стресу у людей третього віку дорослості – користувачів онлайн-середовища.

Вправи «Глибоке дихання», «Дихання по квадрату» сприяла навчанню швидко заспокоювати себе в стресових ситуаціях [44, с. 189]. Обговорили, як змінилися відчуття учасників і як вони можуть використовувати цей метод у реальних ситуаціях.

Вправа «Дякую за…», яка проводилася з метою розвитку вміння фокусуватися на позитивному викликала бурю гарних емоцій та дала підґрунтя для проведення наступної вправи. Учасники отримали завдання подумати про щось приємне або хороше, що сталося з ними протягом останнього тижня. Кожен по черзі висловлював подяку за якусь подію чи людину, промовляючи «Я дякую за…». Пенсіонери переключилися з негативних думок на позитив. Як, підсумок, зазначено, що регулярна практика подяки сприяє зниженню рівня стресу та покращенню настрою.

А от вправа «Позитивна переоцінка ситуації» сприяла вмінню змінювати ставлення до стресових ситуацій. Кожному учаснику тренінгу пропонувалося пригадати недавню ситуацію, яка викликала роздратування або тривогу. Потім – подумати, які позитивні аспекти або уроки можна винести з цієї ситуації. Наприклад, замість думки «Я запізнився», можна подумати «Я встиг відпочити».

Далі відбулося обговорення, як така переоцінка допомагає знизити емоційний тиск і зменшити негативні емоції.

На завершення – вправа «Мудрий радник», за допомогою якої розвивали навички спокійніше реагувати на проблеми та приймати рішення. Завдання учасникам – уявити, що їхній друг зіткнувся з такою ж проблемою, як вони. Вони повинні порадити другу, як краще діяти або що робити. Такий підхід допомагає дистанціюватися від проблеми, знайти раціональне рішення та знизити емоційне напруження.

На шостому завершальному занятті проведена повторна діагностика та рефлексія. А саме: обговорили новий досвід та здобуті знання, які навички стали для них найбільш цінними.

Невеличке тестування проведено з метою підкреслити особисті досягнення учасників, щоб вони побачили, що стали впевненішими та обізнанішими у цифровому середовищі, які були труднощі під час тренінгу, чи будуть ділитися інформацією з друзями та рідними.

Вправа «Люстерко» запропонована для заключної рефлексії, щоб створити теплу та дружню атмосферу, де кожен учасник відчув свою важливість, отримані знання та впевненість. Це допомогло пенсіонерам запам’ятати тренінг як важливий етап на шляху до безпечного користування цифровими технологіями (https://bit.ly/4hqEHUl).

В цілому отримані результати можна оцінити позитивно: учасники оптимізували теоретичні знання та практичні навички, які отримали під час занять, проаналізували власні психологічні особливості. Порівняння результатів до та після тренінгу показало значне зростання середнього балу знань учасників щодо основних понять кібербезпеки, типів онлайн-шахрайств, правил безпечної роботи в інтернеті тощо. Так, до тренінгу лише 10% учасників могли правильно визначити основні види інтернет-шахрайства (фішинг, вішинг, фейковий сайт-магазин тощо). Після проходження програми цей показник зріс до 75%.

Люди літнього віку продемонстрували значне покращення практичних навичок, таких як створення складних паролів, розпізнавання підозрілих

посилань. Спостерігається зростання рівня довіри до власних можливостей безпечного використання інтернету. Зменшилася тривожність щодо можливих негативних наслідків використання цифрових технологій.

Щодо зміни в сприйнятті: пенсіонери відзначають, що після тренінгу вони стали більш обережними при користуванні інтернетом, уважніше читають інформацію, що надходить, і менше довіряють незнайомим джерелам. 90% учасників тренінгу зазначили, що отримали корисні знання, які планують застосовувати в повсякденному житті та поділитися ними з друзями.

Аналізуючи завершальне тестування у питаннях бар'єрів та труднощів, 32% учасників відзначили, що деякі технічні аспекти кібербезпеки є складними для розуміння, 7% – не мають та не користуються гаджетами як ноутбук, комп'ютер. 58% учасників висловила потребу в додаткових тренінгах для закріплення отриманих знань.

Отримані результати свідчать про високу ефективність тренінгової програми «Твій цифровий щит». Програма дозволила значно підвищити рівень цифрової грамотності та кібербезпеки серед осіб пенсійного віку. Учасники не лише отримали теоретичні знання, але й розвинули практичні навички, необхідні для безпечної роботи в інтернеті.

Однак, слід зазначити, що для досягнення стійких результатів необхідне проведення повторних тренінгів та створення спільноти взаємодопомоги для обміну досвідом та вирішення проблем.

Одним з ключових факторів успіху стало поєднання теоретичної інформації з активними практичними вправами, що дозволило учасникам відчути реальний контекст загроз і навчитися діяти в небезпечних ситуаціях. Крім того, важливу роль відіграла підтримка та дружня атмосфера під час тренінгу, яка зменшувала страх і тривогу щодо використання інтернету.

Аналіз та інтерпретація результатів тренінгу мають важливе значення для оцінки його ефективності, виявлення сильних і слабких сторін, а також вдосконалення програми для майбутніх учасників – людей третього віку дорослості.

Для аналізу результатів проведено кількісне та якісне дослідження, яке включало наступні методи: анкетування учасників до та після тренінгу з метою оцінки рівня знань і впевненості у власних силах щодо використання інтернету; тестування для перевірки практичних навичок розпізнавання шахрайських схем та загроз в онлайн-середовищі; інтерв'ю з учасниками після завершення тренінгу для збору якісних даних про їхній досвід та враження від участі у програмі; спостереження під час виконання практичних завдань для аналізу активності, залученості та рівня освоєння матеріалу.

Проведена з учасниками тренінгу проєктивна методика «Геометричні фігури» (за Сьюзеном Деллінгером) [22, с. 33-35] дала можливість визначити психологічні риси, які роблять пенсіонерів вразливими до методів соціальної інженерії. Розглянемо, як кожен тип вибору у цій методиці може відображати потенційні вразливості та способи маніпуляції.

1. Прямокутник (36%): Пенсіонери, які вибрали прямокутник, перебувають у пошуковому стані і можуть відчувати невпевненість. Такі люди більш схильні до маніпуляцій, заснованих на пропозиціях «нових можливостей» або «покращення життя», оскільки вони відкриті до змін. Соціальні інженери можуть використовувати їхню вразливість, граючи на потребі знайти стабільність і впевненість, що часто зустрічається серед пенсіонерів, які відчувають самотність або нестабільність.

2. Коло (24%): Люди, які ідентифікують себе з колом, мають сильну потребу у гармонійних стосунках і часто уникають конфліктів. Вони можуть бути схильні до маніпуляцій, що базуються на емоційному зв’язку, наприклад, шахрайства «друг чи родич в біді» або «прохання про допомогу». Оскільки вони прагнуть підтримувати добрі стосунки, їм важче відмовити незнайомцям або уникнути ситуацій, що викликають емоційний тиск.

3. Зигзаґ (19%): Учасники з креативним мисленням, які обрали зигзаг, можуть виявляти інтерес до нестандартних ідей, але також можуть піддаватися впливу обіцянок «унікальних» чи «ексклюзивних» можливостей. Соціальні інженери можуть скористатися цікавістю таких людей, заманюючи їх у сумнівні

схеми чи фінансові піраміди, маскуючи їх як новаторські ідеї або інноваційні проєкти.

4. Квадрат (18%): Люди, які обрали квадрат, прагнуть до стабільності та структурованості, що робить їх більш чутливими до маніпуляцій, які виглядають надійно і офіційно. Шахраї можуть впливати на них через фальшиві листи «від офіційних установ», прохання сплатити «податки» або «комунальні послуги», адже такі люди зазвичай більше довіряють структурованим і чітким запитам.

5. Трикутник (3%): Люди з лідерськими якостями і амбітністю менш поширені серед учасників, що може означати низьку схильність до вразливості в контексті соціальної інженерії. Проте, якщо такі люди й стають жертвами, то частіше через схеми, які пропонують швидкий шлях до досягнення цілей або підвищення статусу (наприклад, інвестиційні схеми).

Отже, більшість пенсіонерів у цій групі (прямокутник і коло) мають підвищену вразливість до маніпуляцій, що апелюють до емоцій або пропонують стабільність і підтримку (рис. 3.3.)

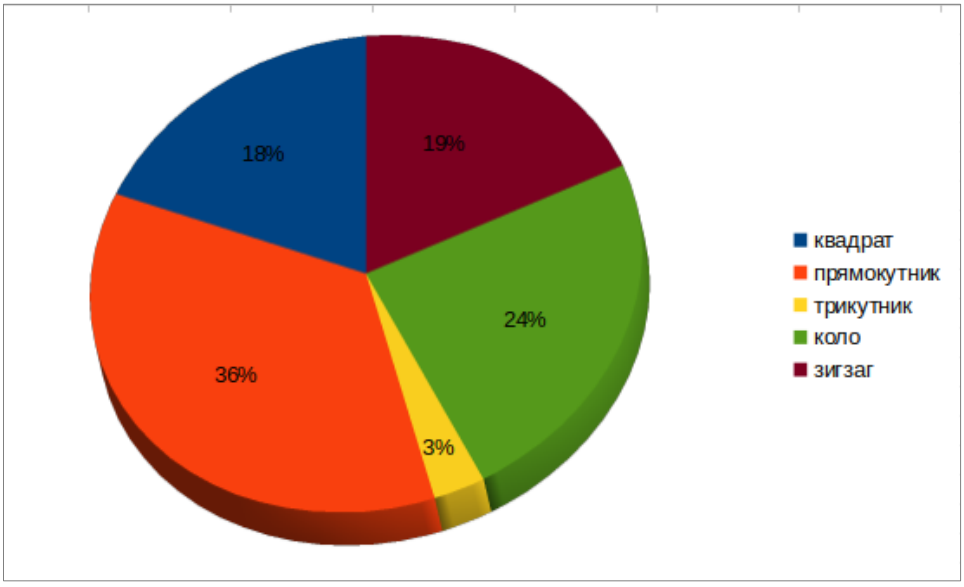



Рис. 3.3. Результати проєктивної методики «Геометричні фігури»

Тренінги для таких груп можуть включати вправи на розпізнавання маніпуляцій, побудову навичок критичного мислення і аналізу ситуацій, а також розвиток впевненості, щоб допомогти уникати імпульсивних рішень під впливом емоційного тиску.

Так, вдалося визначити динаміку змін щодо розпізнавання шахрайських дій. До тренінгу 45% учасників змогли правильно виявити фальшиві електронні листи та сайти, тоді як після тренінгу цей показник зріс до 87%.

Шкала «Рівень цифрової впевненості» показала суттєве підвищення власної впевненості у використанні інтернету. Якщо до тренінгу лише 19% пенсіонерів почувалися впевнено при виконанні базових операцій в інтернеті, то після навчання цей показник збільшився до 58%. Безпека персональних даних. До тренінгу лише 28% учасників знали про необхідність використання двофакторної аутентифікації для захисту облікових записів. Після тренінгу 69% учасників змогли самостійно налаштувати подібні механізми безпеки на своїх пристроях.

Таким чином, кількісні результати чітко демонструють суттєве підвищення рівня обізнаності та практичних навичок учасників у сфері цифрової безпеки, що наглядно простежується на діаграмі (рис. 3.4.)

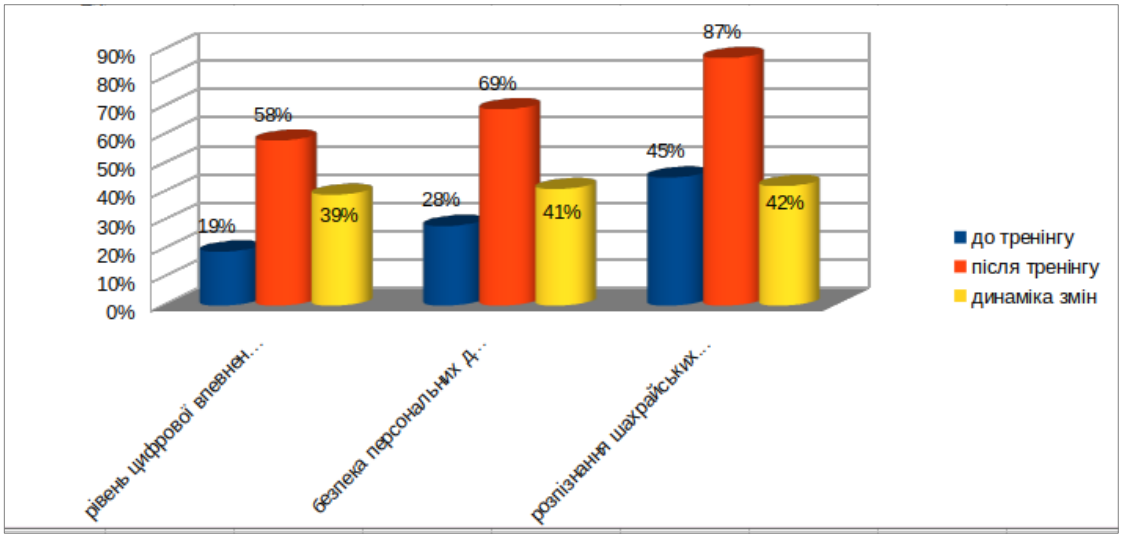



Рис. 3.4. Навички з кібербезпеки

Завершальним етапом експериментального дослідження став контрольний етап, на якому ми ставили завдання: проведення повторної діагностики й оцінку та інтерпретації результатів. На контрольному етапі роботи проводили повторну діагностику тими ж методами, що й на констатувальному.

За результатами тесту «Стиль ухвалення рішень» можна побачити, як змінився стиль ухвалення рішень пенсіонерів після тренінгу (рис. 3.5) Стиль «Швидке і впевнене ухвалення рішень» переважав у 53% учасників, але після тренінгу показник знизився до 45%, тобто на 8%. Це свідчить, що після тренінгу у пенсіонерів дещо підвищилася обачність та критичне мислення.

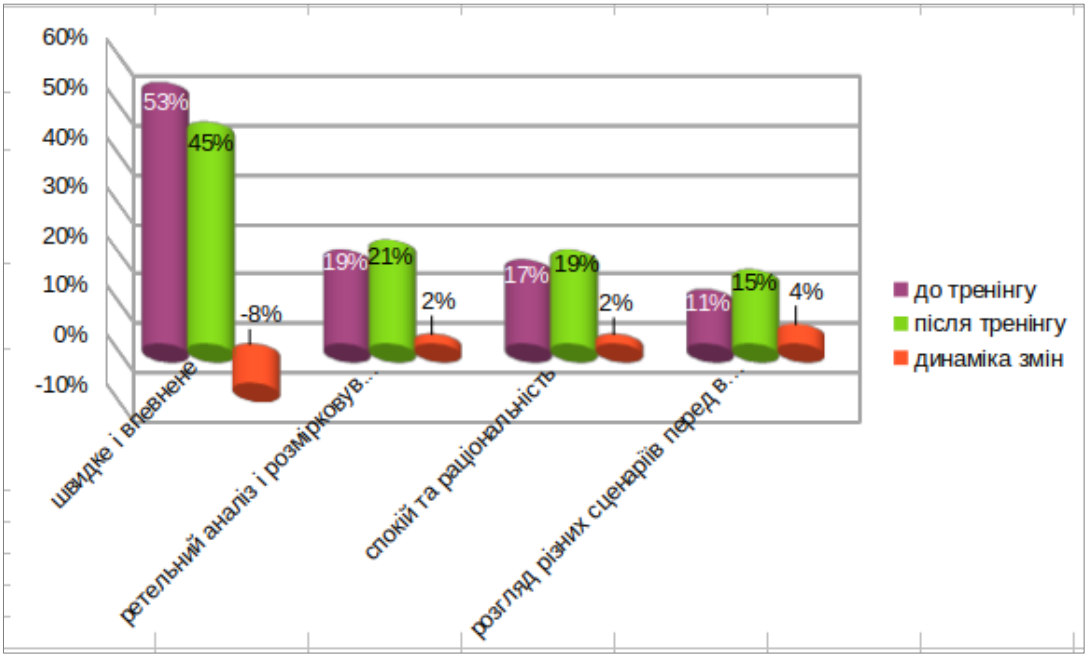



Рис. 3.5. Динаміка змін стилів ухвалення рішення

19% учасників обирали стиль ухвалення рішень «Ретельний аналіз і розмірковування», а після тренінгу – 21%, тобто відбулося зростання на 2%. Це свідчить про збільшення готовності учасників уважніше аналізувати ситуацію перед тим, як зробити вибір, що, у свою чергу, позитивно впливатиме на захист від методів соціальної інженерії в онлайн-просторі.

«Спокій і раціональність» – цей стиль до тренінгу був характерний для 17% учасників, а після – для 19%, що також показує зростання на 2%. Учасники стали трохи більш раціональними та спокійними під час прийняття рішень.

До тренінгу лише 11% учасників розглядали кілька можливих сценаріїв (стиль № 4), а після – 15%, що означає зростання на 4%. Це найвищий позитивний приріст серед усіх категорій, що свідчить про те, що учасники

почали враховувати більше варіантів перед прийняттям остаточного рішення та зробити правильний вибір у захисті від методів соціальної інженерії.

У роботі з людьми літнього віку досліджувалася здібності особистості розуміти відносини, що репрезентується в емоціях, і керувати своєю емоційною сферою на основі прийняття рішень (методика Н. Холла). Таким чином, в експериментальному дослідженні ми отримали наступні показники, наведені в табл. 3.1 та відображені на рис. 3.6 та 3.7.

Таблиця 3.1.

**Динаміка розвитку ключових компонентів емоційного інтелекту в процесі тренінгу для людей похилого віку**

| Шкали | | Користувачі Інтернету – люди третього віку дорослості, які проходили діагностику до тренінгу (n=18) | | Користувачі Інтернету – люди третього віку дорослості, які проходили діагностику після тренінгу (n=18) | |
|---|---|---|---|---|---|
| | | n | У % | n | у % |
| емоційна обізнаність | Низький | 9 | 50 | 4 | 22,2 |
| | Середній | 4 | 22,2 | 6 | 33,3 |
| | Високий | 5 | 27,8 | 8 | 44,4 |
| Управління власними емоціями | Низький | 11 | 61,1 | 8 | 44,4 |
| | Середній | 4 | 22,2 | 6 | 33,33 |
| | Високий | 3 | 16,7 | 4 | 22,2 |
| Самомотивація | Низький | 7 | 38,9 | 6 | 33,3 |
| | Середній | 7 | 38,9 | 7 | 38,9 |
| | Високий | 4 | 22,2 | 5 | 27,8 |

| | | | | | |
|---|---|---|---|---|---|
| Емпатія | Низький | 2 | 11,1 | 1 | 5,6 |
| | Середній | 6 | 33,3 | 6 | 33,3 |
| | Високий | 10 | 55,6 | 11 | 61,1 |
| Розпізнавання емоцій інших людей | Низький | 9 | 50,0 | 8 | 44,4 |
| | Середній | 7 | 38,9 | 7 | 38,9 |
| | Високий | 2 | 11,1 | 3 | 16,7 |

Результати таблиці свідчать про зміни у рівні емоційної обізнаності та навичок управління емоціями серед пенсіонерів після проходження тренінгу, спрямованого на зниження їхньої вразливості до методів соціальної інженерії. Нижче наведено детальний аналіз кожного показника до та після тренінгу.

Щодо шкали «Емоційна обізнаність»: До тренінгу 50% пенсіонерів мали низький рівень емоційної обізнаності, 22,2% – середній, а 27,8% – високий. Після тренінгу кількість учасників із низьким рівнем зменшилася до 22,2%, а частка з високим рівнем зросла до 44,4%. Це свідчить про позитивну динаміку – тренінг допоміг учасникам краще усвідомлювати свої емоції, що може знизити їхню вразливість до емоційних маніпуляцій.

Показник «Управління власними емоціями» вказує, що до тренінгу більшість (61,1%) мала низький рівень навичок управління емоціями, 22,2% – середній і лише 16,7% – високий. Після тренінгу число людей з низьким рівнем зменшилося до 44,4%, а кількість з високим рівнем дещо зросла до 22,2%. Покращення в цій категорії свідчить про те, що учасники почали краще контролювати свої емоції, що важливо для протидії маніпуляціям.

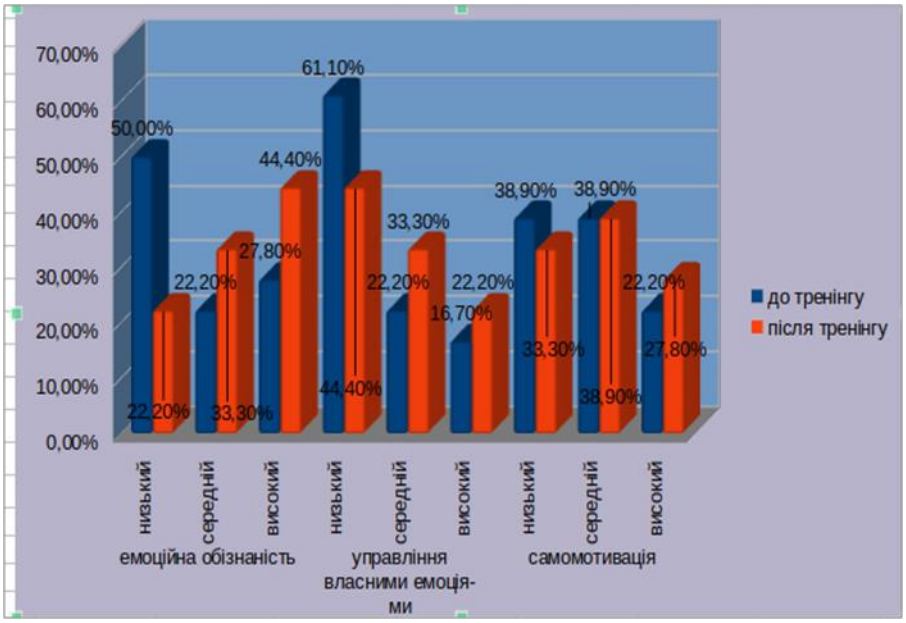



Рис. 3.6. Результати тесту Н. Холла. Частина І.

До початку тренінгу 38,9% учасників мали низький рівень самомотивації, стільки ж (38,9%) – середній, і 22,2% – високий. Шкала «Самомотивація» після тренінгу показала, що відсоток літніх людей з низьким рівнем знизився до 33,3%, а кількість з високим рівнем зросла до 27,8%. Незначне покращення у цій категорії може свідчити, що тренінг допоміг деяким учасникам відчути більшу внутрішню мотивацію, що є корисним для захисту від маніпуляцій, які базуються на використанні страхів чи інтересів людини.

Наступний показник «Емпатія» має такі результати: до тренінгу лише 11,1% учасників мали низький рівень емпатії, 33,3% – середній, а 55,6% – високий. А після тренінгу рівень емпатії у групі залишився стабільним, з незначним збільшенням кількості учасників із високим рівнем (61,1%). Це означає, що учасники зберегли високу здатність розуміти та відчувати емоції інших, що корисно для соціальної взаємодії, але також може зробити їх вразливішими до маніпуляцій, які апелюють до співчуття.

Результати показників шкали «Розпізнавання емоцій інших людей» до тренінгу становлять: половина учасників (50%) мала низький рівень розпізнавання емоцій інших людей, 38,9% – середній, і лише 11,1% – високий. Кількість учасників після тренінгу з низьким рівнем знизилася до 44,4%, а з

високим — зросла до 16,7%. Це показує, що учасники стали трохи краще розпізнавати емоції інших, що може сприяти кращій соціальній взаємодії, хоча цей навик також потребує обережності, щоб уникнути маніпуляцій.

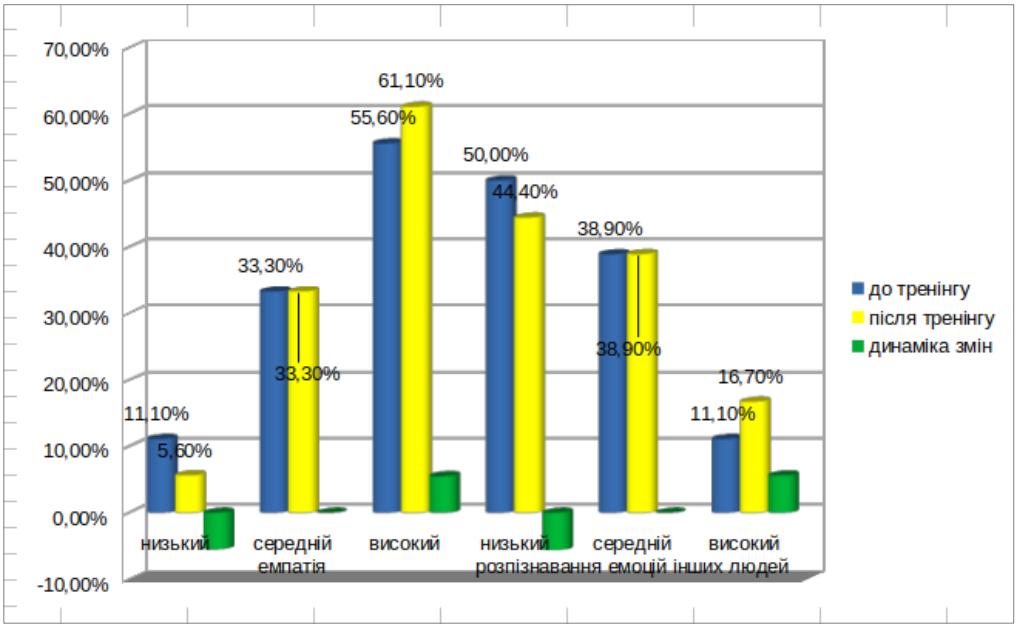



Рис. 3.7. Результати тесту Н.Холла. Частина 2.

Тренінг позитивно вплинув на більшість учасників, підвищивши їхню емоційну обізнаність і здатність управляти власними емоціями, що може допомогти знизити їхню вразливість до методів соціальної інженерії. Покращення у цих категоріях означає, що пенсіонери стали більш обачними, обізнаними про власні реакції та менш схильними до емоційних маніпуляцій, що є важливим кроком до захисту від шахрайства.

Загалом тренінг сприяв тому, що пенсіонери стали менш імпульсивними та більш обдуманими у своїх рішеннях, що є важливим для захисту від соціальної інженерії та маніпуляцій.

На додаток до кількісних показників, інтерв’ю та спостереження дозволили отримати важливу інформацію щодо суб'єктивного досвіду учасників тренінгу. Більшість респондентів відзначили, що програма допомогла їм відчути себе більш захищеними у цифровому середовищі. Вони розуміють як шахраї, використовуючи вразливості психіки людини, можуть маніпулювати та вчиняти шахрайські дії проти користувачів онлайн-середовища. Деякі учасники

зізналися, що до тренінгу вони несвідомо здійснювали покупки в інтернеті або користуватися банківськими сервісами онлайн, тоді як після навчання почали усвідомлено і з обережністю користуватися цими можливостями.

Учасники позитивно оцінили практичні завдання, зазначаючи, що вони допомогли набути реальних навичок критичного мислення і відпрацювати поведінкові стратегії у випадку зустрічі з шахрайством.

Аналіз отриманих результатів вказує на високу ефективність тренінгу «Твій цифровий щит». Кількісні та якісні показники свідчать про суттєве покращення знань та навичок учасників у сфері цифрової безпеки. При цьому позитивні зміни відбулися як у когнітивній (засвоєння знань), так і в емоційно-поведінковій (впевненість у діях), розуміння сферах.

Результати аналізу соціально-психологічної тренінгової програми «Твій цифровий щит» демонструють її ефективність для підвищення рівня цифрової безпеки серед пенсіонерів. Програма не лише сприяє покращенню технічних знань, але й позитивно впливає на емоційний стан учасників, знижуючи тривогу та підвищуючи впевненість у власних силах.

Подальше вдосконалення тренінгу може включати поглиблення практичних завдань та повторення складніших тем, що дозволить ще більше підвищити рівень захищеності пенсіонерів у цифровому середовищі.

Саме такі заходи і входять до поняття «цифрова трансформація освіти». Це трансформація механізмів формування людини як особистості, її талантів, інтелектуальних, творчих і фізичнихздібностей, та цінностей за допомогою використання цифрових технологій у формальному і неформальному освітньому процесі [19, с. 141].

## Висновки до третього розділу

Соціально-психологічна тренінгова програма "Твій цифровий щит" була спрямована на підвищення рівня цифрової грамотності пенсіонерів та їхньої здатності захищатися від шахрайства й маніпуляцій в інтернеті. Основними завданнями тренінгу були навчання безпечному користуванню інтернетом,

розвиток навичок розпізнавання шахрайських дій, а також підвищення впевненості учасників у цифровому середовищі.

Проведене дослідження підтвердило актуальність та ефективність соціально-психологічного тренінгу для підвищення кібербезпеки серед старшого покоління. Отримані результати можуть бути використані для подальшого вдосконалення програми та розробки нових інструментів для підвищення цифрової грамотності серед різних верств населення.

За результатами встановлено, що люди похилого віку часто стають мішенню для шахраїв, які використовують методи соціальної інженерії. Це пов'язано з низкою психологічних та соціальних факторів. Літні люди часто більше довіряють людям, які представляються як авторитети (лікарі, юристи, представники державних органів), навіть якщо вони контактують з ними лише онлайн. Пенсіонери можуть приймати рішення, спираючись на інтуїцію, а не на раціональні аргументи, що робить їх більш схильними до емоційних маніпуляцій. Почуття соціальної відповідальності може спонукати літніх людей відгукнутися на прохання про допомогу, навіть якщо вони здаються підозрілими.

Страх втрати близьких, майна або здоров'я може зробити людей похилого віку більш вразливими до залякування та шантажу. Бажання уникнути самотності може спонукати їх до спілкування з незнайомцями в Інтернеті, навіть якщо це потенційно небезпечно.

Зловмисники можуть використовувати ностальгічні почуття, апелюючи до спогадів про минуле. Сентиментальність може зробити людей похилого віку більш схильними до маніпуляцій, пов’язаних з емоційними спогадами.

Шахраї можуть пропонувати легкі способи заробітку грошей, використовуючи бажання людей похилого віку бути фінансово незалежними. Бажання відчувати себе значущими може спонукати їх брати участь у підозрілих схемах.

Кожен з цих факторів може посилювати один одного, створюючи додаткові ризики для людей похилого віку.

Отже, необхідно опановувати навички та застосовувати методи захисту від соціальної інженерії, забезпечувати належний рівень свідомості та уважності серед користувачів інформаційних технологій третього віку дорослості.

# ВИСНОВКИ

Проведене дослідження дозволяє зробити наступні висновки:

1. На основі здійсненого теоретичного аналізу наукових джерел щодо визначення поняття «соціальна інженерія», «методи соціальної інженерії» встановлено, що соціальна інженерія – це метод маніпуляції людьми з метою отримання конфіденційної інформації, доступу до систем або ресурсів без застосування технічних засобів злому. Цей підхід використовує психологічні прийоми, які спрямовані на довіру, страх, емпатію або інші емоції, які змушують користувача діяти у бажаному для інтернет-шахрая напрямку. З'ясовано, що для визначення рівня вразливостей до методів соціальної інженерії користувачів Інтернету третього віку дорослості необхідно враховувати емоційну стійкість, емпатію, довіру, стиль ухвалення рішення.

2. Емпірично доведено, що негативний вплив методів соціальної інженерії є поширеним явищем у сучасному онлайн середовищі (40,8% учасників дослідження постраждали від атак соціальної інженерії). Результати проведеного дослідження вказують, що соціальна інженерія стає серйозною загрозою для користувачів онлайн середовища, особливо для людей третього віку дорослості. При цьому домінуючим визначачено методи соціальної інженерії, від яких постраждали користувачі Інтернету третього віку дорослості: вішинг, фішинг, онлайн-покупка. Результати проведених анкетувань підтвердили факт, що для користувачів пенсійного віку виникає значний ризик стати жертвою шахрайських дій та маніпуляцій через недостатні знання про сучасні загрози в мережі.

3. Встановлено, що за допомогою превентивних заходів, а саме – соціально-психологічного тренінгу можна позитивно впливати на зниження ризику негативного впливу методів соціальної інженерії. Статистично підтверджені дані засвідчують той факт, що запропонована програма тренінгу «Твій цифровий щит» є ефективною у підвищенні кібербезпеки серед людей старшого віку. Може інтегруватися у навчальні програми, тренінги та

консультаційні сесії з метою підвищення цифрової безпеки користувачів пенсійного віку; застосовуватися соціальними працівниками, психологами та організаціями, які взаємодіють із літніми людьми.

На основі проведеного дослідження для користувачів Інтернету третього віку дорослості сформульовані рекомендації, які сприяють вдосконаленню навичок розпізнавання маніпуляційних технік в онлайн- середовищі, знижують ризики кіберзагроз та потрапляння в шахрайські схеми.

Подальші дослідження вбачаємо у вивченні комплексного підходу до вивчення впливу методів соціальної інженерії у рамках розвитку нової підгалузі психології – кіберпсихології. Протягом історії можна знайти різні форми соціальної інженерії, але, враховуючи збільшення використання технологій у сучасному світі в кожному аспекті життя, загроза продовжує зростати та перетворюватися на складний процес, який важко зупинити. Фактично, соціальну інженерію можна вважати однією з головних загроз інформаційній безпеці сьогодні.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Акерлоф Д., Шиллер Р. Фішинг. Хто і як маніпулює вашим вибором. К.: Наш формат. 2017. 278 с.

2. Алгрен М. 50 + статистики та тенденцій кібербезпеки (оновлення за 2024 р.) URL: https://www.websiterating.com/uk/research/cybersecurity-statistics-facts/. (дата звернення: 09.04.2024)

3. Амплєєва О. М., Миропольцева Н. І. Математична статистика та математичні методи у психології: Методичні рекомендації для практичних занять, самостійної роботи та контролю знань. Миколаїв: ЧНУ ім. П. Могили, 2019. 60 с.

4. Анісімов А.А. Цифрова автентифікація: досягнення та перспективи. Стенограма доповіді на засіданні Президії НАН України 31 травня 2023 року. *Вісник Національної академії наук України*. 2023. № 8. С. 65-68. URL: https://doi.org/10.15407/visn2023.08.065 (дата звернення: 09.04.2024)

5. Афанасьєва Н.Є., Перелигіна Л.А. Теоретико–методологічні основи соціально-психологічного тренінгу. Навч. посібн. 2016. – 252 с. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/4053/1/%D0%9C%D0%A1%D0%9F%D0%A2%20%D0%BD%D0%B0%D0%B2%D1%87%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9%20%D0%BF%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA.pdf (дата звернення 23.10.2024)

6. Беседа Д., Сорочинський О. Найпоширеніші види кіберзагроз серед українських громадян. *Актуальні проблеми управління інформаційною безпекою держави*: зб. матер. всеукр. наук.-практ. конференції. Київ: Нац. акад. СБУ, 2023. С.12-13. URL: https://sci.ldubgd.edu.ua/bitstream/123456789/12539/1/p_57_92088934.pdf (дата звернення: 12.11.2024)

7. Бібліотеки – Хаби цифрової освіти. *Українська бібліотечна асоціація.* URL: https://ula.org.ua/resursy/biblioteky-khaby-tsyfrovoi-osvity (дата звернення: 12.11.2024)

8. Бойко Н. Інтернет у демократизаційному процесі: роздуми про діалектику та складові впливу технічних інновацій у полеміці з Такісом Фотопулосом та іншими. *Соціальні виміри суспільства*. 2019. Випуск 11 (22). С. 413-423.

9. Брижко В.М. Безпека інформаційної приватності: види та схеми шахрайства у сфері електронно-інформаційної взаємодії. *Інформаційя і право*. 2022. № 3(42). С. 65-79. URL: https://doi.org/10.37750/2616-6798.2022.3(42).270237 (дата звернення: 22.11.2024)

10. Войтко О. В., Кацалап В. О., Рахімов В. В. Аналіз особливостей маніпуляції, як інструменту психологічного впливу на свідомість. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2019. № 2 (35). С. 121–126. URL:https://journals.indexcopernicus.com/api/file/viewByFileId/1028047.pdf (дата звернення: 09.04.2024)

11. Ганченко М.І. Людський психологічний та біометричний фактор у розвитку та використанні методів соціальної інженерії у мирний та воєнний час. *Сучасний захист інформації*. 2022. №1(49). С. 16-26. URL: https://journals.dut.edu.ua/index.php/dataprotect/article/view/2611/2510 (дата звернення: 07.04.2024)

12. Головко Д.Ю. Безпека в цифровому просторі: електронний навчальний курс. Біла Церква: БІНПО ДЗВО «УМО» НАПН України, 2024. 54 с. URL: https://lib.iitta.gov.ua/id/eprint/739432/1/%D0%95%D0%9D%D0%9A%20%D0%91%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0%20%D0%B2%20%D0%A6%D0%9F.pdf (дата звернення: 17.11.2024)

13. Гончарова І.П. Кібербезпека в цифровому освітньому середовищі закладів професійної освіти: електронний навчальний курс. Біла Церква, БІНПО ДЗВО «УМО» НАПН УКРАЇНИ, 2022. 80 с. URL: https://binpo.com.ua/wp-content/uploads/2022/12/%D0%9AI%D0%91%D0%95%D0%A0%D0%91%D0%95%D0%97%D0%9F%D0%95%D0%9A%D0%90.pdf (дата звернення 21.10.2024)

14. Гоян І.М., Данилова Т.В. Вплив соціальних мереж на психологічне функціонування особистості: до постановки проблеми. *Гуманітарні студії:*

*педагогіка, психологія, філософія.* 2021. Том 12. № 4. С.118-124 URL: http://hdl.handle.net/123456789/11767 (дата звернення 28.10.2024.)

15. Гроші за «лайки» – кіберполіція застерігає від онлайн-шахраїв. *Кіберполіція України. Офіційний сайт.* URL: https://cyberpolice.gov.ua/article/groshi-za-lajky---kiberpolicziya-zasterigaye-vid-onlajn-shaxrayiv-3412/ (дата звернення 29.10.2024)

16. Гуцалюк М.В. Новітні тенденції кіберзлочинності. *Інформація і право.* 2021. № 1(36). С. 79-89. URL: https://doi.org/10.37750/2616-6798.2021.1(36).238186 (дата звернення 28.11.2024.)

17. Дзюба О. У 2023 році середня сума шахрайської операції з «веденням клієнта» – 8500 грн. Ось інші важливі цифри щодо онлайн-зловмисників. URL: https://dev.ua/news/v-2023-rotsi-serednia-suma-shakhraiskoi-operatsii-z-vedenniam-kliienta-8500-hrn-os-inshi-vazhlyvi-tsyfry-shchodo-onlain-zlovmysnykiv (дата звернення: 06.04.2024)

18. Довгань О.Д., Тарасюк А.В. Кібербезпека «Суспільства знань» як невід'ємна складова поступального розвитку України у постВоєнний період». *Інформація і право*. 2022. №4 (43). С. 109-117. URL: https://doi.org/10.37750/2616-6798.2022.4(43).270072 (дата звернення: 06.04.2024)

19. Дубняк М.В. Цифрова трансформація освіти та цифрових компетентностей: правові аспекти. *Інформація і право*. 2022. №3 (42). С.141-155. URL: https://doi.org/10.37750/2616-6798.2022.3(42).270253 (дата звернення: 09.11.2024)

20. Еріксон Т. В оточенні ідіотів або як зрозуміти тих, кого неможливо зрозуміти. Харків: Фоліо, 2019. 251с.

21. Жмурко О. Соціальна інженерія як загроза кібербезпеці: методи запобігання та захист. *Педагогіка безпеки.* 2024. Том 9. №1. С. 37-42. URL: https://doi.org/10.31649/2524-1079-2024-9-1-037-042. (дата звернення 30.10.2024)

22. Збірник методик діагностики лідерських якостей сержантського та офіцерського складу: Методичний посібник. К.: НДЦ ГП ЗСУ, 2023. 37 с.

23. Калашнікова С.А. Підготовка і проведення тренінгів на основі компетентісно-орієнтованого підходу. Навчально-методичні матеріали до Модуля 2. Київ, 2008. 56 с.

24. Кібер поліція назвала три найпопулярніші в Україні шахрайські схеми. *Кібер поліція. Офіційний сайт*. URL: yberpolice.gov.ua/news/kiberpolicziya-nazvala-try-najpopulyarnishi-v-ukrayini-shaxrajski-sxemy-8249/ (дата звернення 22.09.2024)

25. Климчук В. О. Математичні методи у психології: навч. посіб. К.: Освіта України, 2019. 288 с.

26. Коваленко І.Е. Теоретико-методологічні засади цифрової трансформації освіти дорослих. *Аналітичний вісник у сфері освіти й науки: довідковий бюлетень*. 2023. Вип. 13. С. 31-45. URL: https://lib.iitta.gov.ua/id/eprint/736044/1/Kovalrnko_IE_ASEduSci-RB-17-2023.pdf (дата звернення 29.11.2024)

27. Ковальчук А.Ю., Гавловський В.Д. Інформаційно-психологічні впливи як засіб маніпуляції свідомістю, що застосовується організованими злочинними угрупуваннями. *Інформація і право*. 2022. № 2(41). С. 94-98. URL: https://doi.org/10.37750/2616-6798.2022.2(41).270370 (дата звернення 29.11.2024)

28. Козар А. В. Соціальна інженерія як спосіб шахрайства. *Протидія кіберзлочинності та торгівлі людьми*: збірник матеріалів міжнародної наук.-практ. конф. (м. Харків, 18 травня 2021 р.) / МВС України, Харків. нац. ун-т внутр. справ; ГС «Глобальний центр взаємодії в кіберпросторі». Харків: ХНУВС. 2021. С. 24-25. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/d7ae08aa-ad7e-4c34-a8aa-94b6866a799f/content (дата звернення 17.10.2024)

29. Кокун О.М., Пішко І.О., Лозінська Н.С., Олійник В.О. Психодіагностика лідерських якостей військовослужбовців. метод. посіб. К.:ТОВ «7БЦ», 2023. 171с.

30. Колісник Т., Ющенко Я. Актуальні проблеми кібербезпеки: небезпека соціальної інженерії в кіберпросторі. *Протидія кіберзлочинності та торгівлі*

*людьми*: збірник матеріалів міжнародної наук.-практ. конф. (м. Харків, 18 травня 2021 р.) / МВС України, Харків. нац. ун-т внутр. справ ; ГС «Глобальний центр взаємодії в кіберпросторі». Харків : ХНУВС. 2021. С. 63-65. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/d7ae08aa-ad7e-4c34-a8aa-94b6866a799f/content (дата звернення 13.09.2024)

31. Корченко О., Горніцька Д., Гололобов А. Розширена класифікація методів соціального інжинірингу. *Безпека інформації*. 2014. Т. 20. № 2. С. 197-205. URL: http://nbuv.gov.ua/UJRN/bezin_2014_20_2_16. (дата звернення 13.09.2024)

32. Костенко В.О., Кринична І.П., Журбинський Д.А. Актуальність посилення кібербезпеки України в умовах дії воєнного стану в контексті Європейської інтеграції. *Публічне управління та адміністрування в Україні.* 2023. Вип. 34. С. 74-77. URL: https://doi.org/10.32782/pma2663-5240-2023.34.14 (дата звернення 10.04.2024)

33. Котвіцька А.А., Пляка Л.В. Соціально-психологічний тренінг як засіб розвитку комунікативних здібностей майбутніх провізорів. *Наукові записки Харківського університету Повітряних Сил. Соціальна філософія, психологія*. 2008. Вип. 2(31). С. 165-169. URL: http://dspace.nuph.edu.ua/handle/123456789/8847 (дата звернення 10.10.2024)

34. Крайнікова Т. Чому люди віддають свої гроші шахраям? Механіки соціальної інженерії та як від них уберегтися. *Finance.ua*. URL: https://finance.ua/ua/goodtoknow/socialna-inzheneria (дата звернення 23.11.2024)

35. Крилова-Грек Ю. Використання дистанційних технологій для формування інформаційноїх грамотності у дорослої аудиторії. *Technologies of intellekt development*. 2021. Том 5. № 2(30). С.1-13. URL: https://www.psytir.org.ua/index.php/technology_intellect_develop/article/view/560 (дата звернення 13.11.2024)

36. Кримінальний Кодекс України. (Відомості Верховної Ради України (ВВР), 2001, № 25-26, ст.131) Офіційний сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text. (дата звернення 18.11.2024)

37. Кушнерьов О. Детермінанти поширення та локалізації кіберзагроз в умовах цифровізації національної економіки: дис. ... докт. філос. Наук. Суми, 2023. 205 с. URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/93819/1/Kushneryov%20O.S._PhD_thesis.pdf;jsessionid=2CBFB2F6335154151D683E9CCCF03953 (дата звернення 21.10.2024)

38. Лавріненко Н. Пенсіонери в мережах соціальних нерівностей. *Соціальні виміри суспільства*. 2019. Випуск 11 (22). С.332-354. URL: https://i-soc.com.ua/assets/files/socvimirsysp/svs-2019.pdf (дата звернення 28.10.2024)

39. Лемак М. В., Петрище В. Ю. Психологу для роботи: діагностичні методики: методичне видання. Ужгород, 2012. 616 с.

40. Мельниченко О.В., Андрагогічні принципи освіти дорослих та забезпеченнгя якості неперервної педагогічної освіти. *Педагогічна освіта: теорія і практика. Психологія. Педагогіка.* 2020. № 33(1). С. 24-30. DOI: 10.28925/2311-2409.2020.33.3. URL: file:///home/natalia/%D0%97%D0%B0%D0%B2%D0%B0%D0%BD%D1%82%D0%B0%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F/obylan,+%D0%9F%D0%B5%D0%B4%D0%BE%D1%81%D0%B2%D1%96%D1%82%D0%B0_33_%D0%9C%D0%B5%D0%BB%D1%8C%D0%BD%D0%B8%D1%87%D0%B5%D0%BD%D0%BA%D0%BE+24-30.pdf (дата звернення 23.10.2024)

41. Методичні рекомендації для тренерів щодо розроблення та проведення тренінгів /за ред. Т. Фулей. К.: ФОП Демчинський О. В., 2017. 92 с.

42. Мехед Д., Ткач Ю., Базилевич В.Дослідження технологій впливу та методів протидії фішингу. *Захист інформації*. 2019. № 4. С.246-251. URL: https://www.researchgate.net/publication/370837323_Doslidzenna_tehnologij_vplivu_ta_metodiv_protidii_fisingu (дата звернення 31.10.2024)

43. Мехед Д. Інформаційна безпека в соціальних мережах. Методи поширення інформації в соціальних мережах. *Прав., нормат. та метрол. забезп. системи захисту інформації в Україні*. 2015. Вип. 2. С. 14-18. URL: https://ela.kpi.ua/handle/123456789/18028 (дата звернення 31.10.2024)

44. Ми пережили: техніки відновлення для сімей, військових, цивільних та дітей / наук. ред. Циганенко Г. Психологічна кризова служба ГО “Українська асоціація фахівців з подолання наслідків психотравмуючих подій”, 2023. 200 с.

45. Мінсоцполітики застерігає: шахраї під виглядом іноземних партнерів пропонують отримати неіснуючі види допомоги. *Урядовий портал*. URL:https://www.kmu.gov.ua/news/minsotspolityky-zasterihaie-shakhrai-pid-vyhliadom-inozemnykh-partneriv-proponuiut-otrymaty-neisnuiuchi-vydy-dopomohy (дата звернення 20.04.2024)

46. Найпоширеніші види кіберзлочинів у 2024 році. *Galeranews*. URL: https://galera.news/najposhyrenishi-vydy-kiberzlochyniv-u-2024-rotsi-3637/ (дата звернення 21.10.2024)

47. Панасенко Е., Сурчилова С. Соціально-психологічний тренінг в системі підготовки майбутніх практичних психологів закладів освіти: принципи та стратегії побудови програм. *Молодь і ринок*. 2018. № 6 (161). С. 6-11. URL: https://doi.org/10.24919/2308-4634.2018.136840 (дата звернення 28.10.2024)

48. Пітиляк Д.В., Білоус І.І., Бондаренко І.Д. Людський фактор як вразливість інформаційної безпеки при застосування соціальної інженерії. *Актуальні проблеми управління інформаційною безпекою держави*: зб. матер. всеукр. наук.-практ. конференції. Київ : Нац. акад. СБУ, 2023. С. 302-305.

49. Половенко, Л., Мерінова, С. Виявлення ознак соціальної інженерії та технологія протидії соціальним хакерам на підприємстві. *Підприємництво та інновації*. 2019. № 10. С. 183-187. URL: https://doi.org/10.37320/2415-3583/10.28. (дата звернення 28.10.2024)

50. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України". Указ Президента України від 26 серпня 2021 року. № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення 26.11.2024)

51. Протасова Н. Г. Навчально-методичні матеріали до модуля «Особливості навчання дорослих» програми підвищення кваліфікації науково-

педагогічних працівників НАДУ при Президентові України. Київ: Дидактичний центр НАДУ, 2006. 215 с.

52. Про утворення територіального органу Національної поліції. Постанова Кабінету Міністрів України від 13 жовтня 2015 року №831. URL: https://zakon.rada.gov.ua/laws/show/831-2015-%D0%BF#Text (дата звернення 25.11.2024)

53. Ржевський Г.М. Актуальні проблеми психології особистості: формування основ безпечної роботи студентів в інтернет-середовищі. *Сучасна вища освіта: проблеми та перспективи*: тези доповідей VI Всеукр. наук.-практ. конф. (Дніпро, 22 березня 2018 р.). Дніпро: Університет імені Альфреда Нобеля, 2018. С. 147-150. URL: https://old.duan.edu.ua/images/staff/departments/pedagogy_and_psychology/Conferences/conf_Pedagogy_2018.pdf (дата звернення: 29.11.2024)

54. Російське вторгнення в Україну (2022). URL: https://uk.wikipedia.org/wiki/%D0%A0%D0%BE%D1%81%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B5_%D0%B2%D1%82%D0%BE%D1%80%D0%B3%D0%BD%D0%B5%D0%BD%D0%BD%D1%8F_%D0%B2_%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%83_(%D0%B7_2022) (дата звернення: 29.05.2024)

55. Руденко М.І., Власова С.М. Особливості захисту від соціальної інженерії як складової кібератак. *Актуальні проблеми управління інформаційною безпекою держави*: зб. матер. всеукр. наук.-практ.конференції. Київ : Нац. акад. СБУ, 2023. С. 316-319.

56. Савчук Т. Соціальна інженерія: як шахраї використовують людську психологію в інтернеті. Радіо Свобода. URL: https://www.radiosvoboda.org/a/socialna-inzhenerija-shaxrajstvo/29460139.html. (дата звернення: 09.04.2024)

57. Селіванова А., Левитський Ю. Дослідження методів соціальної інженерії. Частина І. Вплив на здоров'я людини. *Automation of Technological and*

*Business Processes*, 2022. № 14(2). С. 56-62. URL: https://doi.org/10.15673/atbp.v14i2.2334 (дата звернення: 09.04.2024)

58. Скибун О.Ж. Фішинг та фішери в сучасному світі. *Грааль науки*. 2022. № 23. С. 259-264. URL: https://archive.journal-grail.science/index.php/2710-3056/article/view/780 (дата звернення: 09.04.2024)

59. Скочинська К. Куди звертатися при інтернет-шахрайстві. *Протокол UA.* URL: https://protocol.ua/ua/kudi_zvertatisya_pri_internet_shahraystvi/ (дата звернення 10.04.2024)

60. Соловей О. Соціально-психологічний тренінг як метод розвитку комунікативної компетенції державних службовців. eVNUIR. 2016. 16 березня. С. 1-12. URL: http://evnuir.vnu.edu.ua/handle/123456789/724 (дата звернення 23.10.2024)

61. Соціальна інженерія – що це таке, атаки з використанням соціальної інженерії. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/sotsialnayainzheneriya/ (дата звернення: 08.04.2024)

62. Соціально-психологічний тренінг як метод практичної психології. Розділ 1. С. 1-34. URL: https://psychology.karazin.ua/dist2020/materialy/Ianovska/konspekt.pdf (дата звернення 20.04.2024)

63. Теслик Н., Гончаренко А., Громико Д. Психологічні особливості сприйняття кібершахрайства студентською молоддю. *Вісник Національного університету оборони України*, 2021. № 60(2). С. 143–149. URL: https://doi.org/10.33099/2617-6858-2021-60-2-143-149 (дата звернення 10.11.2024)

64. Терентьєва Н., Фалько Н. Взаємозалежність особливостей психіки користувачів Інтернет-середовища та методів соціальної інженерії. *Габітус*. 2024. № 66.

65. Терентьєва Н.О., Фалько Н.І. Психологічні аспекти вразливостей користувачів Інтернету до методів соціальної інженерії: емпіричне дослідження. *Могилянські читання – 2024: досвід та тенденції розвитку суспільства в Україні: глобальний, національний та регіональний аспекти. Психологічні*

*аспекти розвитку особистості в сучасних реаліях*: XXVII Всеукр. наук.-практ. конф. (6–10 листоп. 2024 р., Миколаїв). Миколаїв: Вид-во ЧНУ ім. Петра Могили, 2024. С.239-243. URL: https://chmnu.edu.ua/naukovo-praktichnij-seminar-z-mizhnarodnoyu-uchastyu-naukovo-informatsijnij-suprovid-profesijnoyi-pidgotovki-fahivtsiv-v-umovah-neviznachenosti-25-04-2024/ (дата звернення 21.11.2024)

66. Фалько Н. Соціальна інженерія: зброя масового психологічного впливу в цифрову епоху. *Науково-інформаційний супровід професійної підготовки фахівців в умовах невизначеності*: тези науково-практичного семінару з міжнародною участю (25 квітня 2024 року, м. Миколаїв), Миколаїв , 2024. С. 171-176. URL: https://chmnu.edu.ua/naukovo-praktichnij-seminar-z-mizhnarodnoyu-uchastyu-naukovo-informatsijnij-suprovid-profesijnoyi-pidgotovki-fahivtsiv-v-umovah-neviznachenosti-25-04-2024/ (дата звернення 21.11.2024)

67. Федоренко О.І. Інформаційний тероризм як спосіб психологічного впливу на людину. *Особистість, суспільство, війна*: тези доп. учасників міжнар. психолог. форуму (м. Харків, 26 квіт. 2024 р.). Харків: ХНУВС, 2024. С. 327-331. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/a202cdd2-15a9-4cc3-b995-fabee09fe1ee/content (дата звернення: 28.11.2024)

68. Цубін О. Методика проведення аудиту компанії на схильність до атак методами соціальної інженерії. Випускна робота. Суми. 2021. URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/84438/1/Tsubin_bac_rob.pdf;jsessionid=DFE24EF011F4523D01E2902E961719D5. (дата звернення 21.11.2024)

69. ЦурканО., Герасимов Р., Крук О. Методи протидії використанню соціальної інженероії. *Information Technology and Security*. 2019. Том. 7. № 2 (13). С.161-170. URL: https://ela.kpi.ua/server/api/core/bitstreams/9feea6ee-1a2b-4a4b-9364-f471cf50ed5a/content (дата звернення 22.10.2024)

70. Чаграк Н. І., Липа І. Ю. Зародження позитивної геронтології: від соціального відсторонення людей похилого віку до соціальної участі. *Актуальні дослідження в соціальній сфері*: матеріали десятої міжнародної наук.-практ.

конф. (Одеса, 17 листопада 2017 р.). Одеса, 2017. С. 27-29. URL: http://dspace.opu.ua/jspui/bitstream/123456789/7443/1/Sbornik%2010.pdf (дата звернення: 28.10.2024)

71. Чаграк Н. Теорія і практика освіти людей похилого віку у США. (1962 – 2015 рр.). дис. дослідж.... докт. пед. наук: 13.00.01. Київ. 2019. 505 с. URL: https://npu.edu.ua/images/file/vidil_aspirant/dicer/D_26.053.01/dis_Chahrak.pdf (дата звернення 20.11.2024)

72. Чаплінська Ю. С., Кабанова П. С. Ризики кіберсоціалізації: Сьогодення і недалеке майбутнє. *Інформаційні процеси і соціально-психологічні технології. Наукові студії із соціальної та політичної психології*. 2021. Вип. 47 (50). С.160-179. URL: https://lib.iitta.gov.ua/id/eprint/728119/1/220-%D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96-462-1-10-20210730.pdf (дата звернення:28.10.2024)

73. Чистяков С.А. Емоційна стійкість як критерій психічного здоров'я особистості. *Психічне здоров'я особистості у кризовому суспільстві*: збірник матеріалів VII Всеукр. наук.-практ. конф. (Львів, 28 жовтня 2022 р.). Львів : Львівський державний університет внутрішніх справ, 2022. С. 380-383. URL: https://files.znu.edu.ua/files/Bibliobooks/Inshi69/0050386.pdf#page=356 (дата звернення: 28.11.2024)

74. Шевченко А. Звіт про тенденції загроз фішингу. URL: https://top-ai.com.ua/news/zvit-pro-tendencziyi-zagroz-fishyngu/. (дата звернення: 08.04.2024)

75. Що таке соціальна інженерія? URL: https://nadiyno.org/shho-take-soczialna-inzheneriya/ (дата звернення: 29.03.2024)

76. Що таке соціальна інженерія? Напади, методи та запобігання. Cyber Witcher. URL: https://hackyourmom.com/kibervijna/shho-take-soczialna-inzheneriya-napady-metody-ta-zapobigannya/ (дата звернення: 05.04.2024)

77. Яковенко В. С., Казеян Н. К. Соціальна інженерія в Інтернет-просторі. *Інформаційні технології та моделювання економічних процесів*. 2016. Вип. III-IV (63-64). С. 119-126.

78. Ященко. Е. Комунікативний тренінг як інноваційна форма розвитку комунікативної культури студентів в контексті освітньої діяльності. *Вища освіта України у контексті інтеграції до європейського освітнього простору*. 2019. №83(I). С. 404-413. URL:https://osvita.eeipsy.org/index.php/eeip/article/view/109 (дата звернення 23.10.2024)

79. 43% українців отримують пенсії менші за 100 доларів. *Опендатабод.* URL: https://opendatabot.ua/analytics/pensions-2024-10 (дата звернення 20.10.2024)

80. Adejuwon F. E., Ojeagbase I. O. Role of Cybersecurity Education in Promoting Ethical and Responsible Use of Technology for Sustainable Development. *Lead City University Postgraduate Multidisciplinary Conference Proceedings*. 2023. Том l. № 3. С. 193-186.

81. Albladi S.M., Weir G.R.S. Predicting individuals' vulnerability to social engineering in social networks. *Cybersecur*. 2020. №3, 7. С. 1-19. URL: https://doi.org/10.1186/s42400-020-00047-5 (дата звернення 13.11.2024)

82. Ashfaq S., Chandre P., Pathan S., Mande U., Nimbalkar M., Mahalle P. Defending Against Vishing Attacks: A Comprehensive Review for Prevention and Mitigation Techniques. *Cyber Security and Digital Forensics*. Консп. лекцій. 2024. Том. 896. С. 411-422. URL: https://doi.org/10.1007/978-981-99-9811-1_33 (дата звернення 15.04.2024)

83. Atchley R. C. A community theory ofnormalaging. *The Gerontologist*. 1989. Том 29. Випуск 2. С. 183–190. URL: https://doi.org/10.1093/geront/29.2.183 (дата звернення 23.11.2024)

84. Atkins B. Huang W. A Study of Social Engineering in Online Frauds Open. *Journal of Social Sciences*. 2013. Том.1, № 3. С. 23-32. URL: https://www.scirp.org/html/36435.html (дата звернення: 04.11.2024)

85. Cialdini Robert B. The Science of Persuasion. *Scientific American Magazine*. 2001. № 2. С. 76-81 URL: https://digitalwellbeing.org/documents/CialdiniSciAmerican_01.pdf (дата звернення 19.10.2024)

86. Chetioui K. Bah B. Ouali A. Bahnasse A. Overview of Social Engineering Attacks on Social Networks. *Procedia Computer Science*. 2022. № 198. С. 656-661. URL: https://www.sciencedirect.com/science/article/pii/S1877050921025412 (дата звернення: 14.11.2024)

87. Cho J.-H., Cam H., Oltramari A. Effect of personality traits on trust and risk to phishing vulnerability: Modeling and analysis. In: 2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (*CogSIMA*). 2016. С. 7–13. DOI: 10.1109/COGSIMA.2016.7497779. URL: https://ieeexplore.ieee.org/abstract/document/7497779 (дата звернення 29.09.2024)

88. Cyber Witcher. Соціальна Інженерія: Методи та захист в цифровому світі. *HackYourMom* URL: https://hackyourmom.com/kibervijna/shho-take-soczialna-inzheneriya-chastyna-1/ (дата звернення: 03.04.2024)

89. Cyber Witcher. Що таке лжеантивірус? *HackYourMom.* URL: https://hackyourmom.com/kibervijna/shho-take-lzheantyvirus/ (дата звернення 22.10.2024)

90. Cyber Witcher. Як розпізнати прийоми соціальної інженерії? *HackYourMom.* URL: https://hackyourmom.com/kibervijna/soczialna-inzheneriya/ (дата звернення: 04.04.2024)

91. Diamond M. C. An optimistic view of the agingbrain. *Gerontologist*. 1993. №17 (1). С. 31–33.

92. Goel S., Williams K., and Dincelli E. "Got Phished? Internet Security and Human Vulnerability". *Journal of the Association for Information Systems*. 2017. V.18(1). P. 22-44. DOI:10.17705/1jais.00447 URL: https://aisel.aisnet.org/jais/vol18/iss1/2 (дата звернення: 04.04.2024)

93. Halevi T., Memon N., Lewis J., Kumaraguru P., Arora S., Dagar N., Aloul F. Cultural and psychological factors in cyber-security. Матеріали 18 міжнар. конф. «Information Integration and Web-based Applications and Services». 2016. С. 318–324. URL: https://doi.org/10.1145/3011141.301116 (дата звернення 25.07.2024)

94. Harl G. People Hacking-The Psychology of Social Engineering. *Talk at Access All Areas.* 1997. № III. С. 1-3.

95. Hatfield J. Social engineering in cybersecurity: The evolution of a concept. *Computers and Security*. 2018. № 73. С. 102-113. URL: https://doi.org/10.1016/j.cose.2017.10.008 (дата звернення: 04.04.2024)

96. House J. S., Lepkowski J., Kinney A., Mero R., Kessler R., Herzog R. Social satisfaction of a geingand health. *Journal of Health and Social Behavior*. 1994. № 35. С. 213–234. URL: https://doi.org/10.2307/2137277 (дата звернення 23.11.2024)

97. Jakobsson. M. The human factor in phishing. *In In Privacy and Security of Consumer Information.* 2007. № 7(1). С. 1–19. URL: https://markus-jakobsson.com/papers/jakobsson-psci07.pdf (дата звернення 29.09.2024)

98. Knisley R., Lin H. A Review of Literature and Experimental Evidence on Fraud Motivation: Differentiating Incentive and Pressure ORCID logo Author and Article Information. *Forensic Accounting Research*. 2022. Том 7. Випуск 1. С. 184–209 URL: https://doi.org/10.2308/JFAR-2020-024 (дата звернення 29.11.2024)

99. Kurylo V., Karaman O., Bader S., Pochinkova M., Stepanenko V. Critical thinking as an information security factor in the modern world. *Social and Legal Studios*. 2023. Т.6. № 3. С. 67-74. DOI: 10.32518/sals3.2023.67 URL: https://doi.org/10.32518/sals3.2023.67 (дата звернення 29.11.2024)

100. Laslett P. A fresh map of life: the emergence of the third age. London: Macmillan, 1996. 311 с. URL: https://books.google.com.ua/books?hl=uk&lr=&id=TxqhSpbjVGgC&oi=fnd&pg=PR7&dq=Laslett+P.+A+fresh+map+of+life:+the+emergence+of+the+third+age,+2nd+edn.+London:+Macmillan,+1996.+311+p&ots=Qi-8AAhd5W&sig=qGIJ0wPILKbwsoZn6c6hf7Cvnjk&redir_esc=y#v=onepage&q&f=false (дата звернення 23.11.2024)

101. Lohani Shivam. Social Engineering: Hacking into Humans. *International Journal of Advanced Studies of Scientific Research*. 2019. Том. 4. № 1. С. 385-393. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3329391 (дата звернення 20.04.2024)

102. Mitnick Kevin та Simon William L. Ghost in the Wires: My Adventures as the World's Most Wanted Hacker Little, Brown and Company, 2011. 412 p.

103. Mitnick Kevin та Simon William L. The Art of Deception: Controlling the Human Element of Security. Wiley, 2003. 368 p.

104. Montañez R, Golob E., Xu S. Human Cognition Through the Lens of Social Engineering Cyberattacks. *Frontiers*. 2020. Том. 11. С. 1-18. URL: https://doi.org/10.3389/fpsyg.2020.01755 (дата звернення 21.11.2024)

105. Montanez R., Atyabi A., Xu S. Social engineering attacks and defenses in the physical world vs. cyberspace: a contrast study. *ResearchGate*. 2022. № 10. С. 1-26. DOI:10.48550/arXiv.2203.04813. URL: https://www.researchgate.net/publication/359130132_Social_Engineering_Attacks_and_Defenses_in_the_Physical_World_vs_Cyberspace_A_Contrast_Study (дата звернення 10.04.2024)

106. Morrison A. B., Coventry L., Briggs P. Technological Change in the Retirement Transition and the Implications for Cybersecurity Vulnerability in Older Adults. *Frontiers in Psychology*. 2020. Том 11. С. 1-13. URL: https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2020.00623/full (дата звернення 01.12.2024)

107. Okaiwele E. The Psychology of Social Engineering Attacks. URL: https://developerehis.medium.com/the-psychology-of-social-engineering-attacks-ac0e551a5612 (дата звернення: 28.03.2024)

108. Purkait, S., Kumar De, S., Suar, D. An empirical investigation of the factors that influence internet user's ability to correctly identify a phishing website. Inform. *Manage. Comput. Secur*. 2014. Випуск 22. С. 194–234. doi: 10.1108/IMCS-05-2013-0032. URL: https://www.emerald.com/insight/content/doi/10.1108/imcs-05-2013-0032/full/html (дата звернення 10.08.2024)

109. Schaab P., Beckers K., Pape S. Social engineering defence mechanisms and counteracting training strategies. *Information and computer security*. 2017. Том 25. № 2. С. 206–222. URL: https://doi.org/10.1108/ICS-04-2017-0022 (дата звернення 13.09.2024)

110. Siddiqi MA, Pak W, Siddiqi MA. A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. *Applied Sciences*.

2022. № 12(12). С.1-19. URL: https://doi.org/10.3390/app12126042 (дата звернення 21.11.2024)

111. Smit V. A study and analysis of human behaviour influence on cybersecurity. A human behaviourist approach to mitigate social engineering attacks. *Thesis presented in fulfilment of the requirements for the degree of Master of Arts (Socio-Informatics) in the Faculty of Arts and Social Sciences at Stellenbosch University.* 2023. 169 с. URL: https://scholar.sun.ac.za/server/api/core/bitstreams/511c1680-7257-4882-a4d7-e9b0b9345185/content (дата звернення 29.10.2024)

112. Vishwanath A., Harrison B., Ng Y. J. Suspicion, Cognition, and Automaticity Model of Phishing Susceptibility. *Communication Research.* 2018. № 45(8). С. 146-166. URL: https://doi.org/10.1177/0093650215627483 (дата звернення 23.11.2024)

113. Wang Z., Sun L., Zhu H. Defining Social Engineering in Cybersecurity. *IEEE Access.* 2020.Том. 8. С. 85094-85115. doi: 10.1109/ACCESS.2020.2992807 URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9087851 (дата звернення 23.11.2024)

114. Washo Amy Hetro. An interdisciplinary view of social engineering: A call to action for research. *Computers in Human Behavior Reports.* 2021. Том 4. С. 1-8. URL: https://doi.org/10.1016/j.chbr.2021.100126 (дата звернення 18.10.2024)

## ДОДАТКИ

ДОДАТОК А

Методика призначена для виявлення здібності особистості розуміти відносини, що репрезентується в емоціях, і керувати своєю емоційною сферою на основі прийняття рішень. Вона складається з 30 тверджень і містить п'ять шкал:

- шкала 1 - "Емоційна обізнаність";
- шкала 2 - "Управління своїми емоціями" (емоційна відхідливість, емоційна нерігідность);
- шкала 3 - "Самомотивація" (довільне керування своїми емоціями);

- шкала 4 - "Емпатія";
- шкала 5 - "Розпізнавання емоцій інших людей" (вміння впливати на емоційний стан інших).

**Інструкція**

Нижче наведені висловлювання, які так чи інакше відображають різні сторони життя. Праворуч від кожного твердження напишіть цифру, виходячи з вашої ступеня згоди з ним: повністю не згоден (-3 бали); в основному не згоден (-2 бали); почасти не згоден (-1 бал); частково згоден (+1 бал); в основному згоден (+2 бали); повністю згоден (+3 бали).

**Тестовий матеріал**

1. Для мене як негативні, так і позитивні емоції служать джерелом знання про те, як чинити в житті.
2. Негативні емоції допомагають мені зрозуміти, що я повинен змінити у своєму житті.
3. Я спокійний, коли відчуваю тиск з боку.
4. Я здатний спостерігати зміну своїх почуттів.
5. Коли необхідно, я можу бути спокійним і зосередженим, щоб діяти відповідно до запитів життя.
6. Коли необхідно, я можу викликати у себе широкий спектр позитивних емоцій, таких як веселощі, радість, внутрішній підйом і гумор.
7. Я стежу за тим, як я себе почуваю.
8. Після того як щось засмутило мене, я можу легко впоратися зі своїми почуттями.
9. Я здатний вислуховувати проблеми інших людей.
10. Я не зациклююсь на негативних емоціях.
11. Я чутливий до емоційних потреб інших.
12. Я можу діяти на інших людей заспокійливо.
13. Я можу змусити себе знову і знову встати перед обличчям перешкоди.
14. Я намагаюся підходити до життєвих проблем творчо.
15. Я адекватно реагую на настрої, спонукання і бажання інших людей.

16. Я можу легко входити в стан спокою, готовності і зосередженості.

17. Коли дозволяє час, я звертаюся до своїх негативним почуттям і розбираюся, в чому проблема.

18. Я здатний швидко заспокоїтися після несподіваного засмучення.

19. Знання моїх справжніх почуттів важливо для підтримки "хорошої форми".

20. Я добре розумію емоції інших людей, навіть якщо вони не виражені відкрито.

21. Я можу добре розпізнавати емоції за виразом обличчя.

22. Я можу легко відкинути негативні почуття, коли необхідно діяти.

23. Я добре вловлюю знаки у спілкуванні, які вказують на те, в чому інші потребують.

24. Люди вважають мене добрим знавцем переживань інших.

25. Люди, які усвідомлюють свої справжні почуття, краще управляють своїм життям.

26. Я здатний поліпшити настрій інших людей.

27. Зі мною можна порадитися з питань відносин між людьми.

28. Я добре налаштовуюся на емоції інших людей.

29. Я допомагаю іншим використовувати їх спонукання для досягнення особистих цілей.

30. Я можу легко відключитися від переживання неприємностей.

**КЛЮЧ**

**Шкала 1** - пункти 1, 2, 4, 17, 19, 25. **Шкала 2** - пункти 3, 7, 8, 10, 18, 30. **Шкала 3** - пункти 5, 6, 13, 14, 16, 22. **Шкала 4** - пункти 9, 11, 20, 21, 23, 28. **Шкала 5** -пункт 12, 15,24, 26, 27,29

**Обробка та інтерпретація РЕЗУЛЬТАТІВ**

Рівні парціального емоційного інтелекту у відповідності зі знаком результатів: **14 і більше** - високий; **8-13** - середній; **7 і менш** - низький.

Інтегративний рівень емоційного інтелекту з урахуванням домінуючого знака визначається за такими кількісними показниками: **70 і більше** - високий; **40-69** - середній; **39 і менше** - низький.

ДОДАТОК Б

**Тест “Рівень емоційної стійкості”**

(автор: Тарасов Є.О., кандидат психологічних наук,

психотерапевт вищої категорії)

Потрібно відповісти на 10 тверджень, підрахувати бали і прочитати результати.

1. Мені часто сняться нічні кошмари

Так-2 бали. Ні-1 бал.

2. Мене дратує велика кількість людей

Так-3 бали. Ні-0 балів.

3. Мене часто мучить почуття провини

Так-3 бали. Ні-0 балів.

4. Я не забороняю собі висловлювати свої переживання, почуття

Так-0 балів. Ні-1 бал.

5. Я легко ображаюся на жарти в свою адресу

Так-3 бали. Ні-1 бал.

6. В мене часто змінюється настрій

Так-2 бали. Ні-1 бал.

7. Я потребую людей, здатних мене зрозуміти, підтримати, втішити

Так-2 бали. Ні-1 бал.

8. Я легко почуваюся в колі нових для мене людей

Так-0 балів. Ні-2 бали.

9. Я приймаю все те, що відбувається близько до серця

Так-3 бали. Ні-0 балів.

10. Мене легко розізлити

Так-2 бали. Ні-1 бал.

Результати тесту:

• 7 балів означає, що у вас високий рівень емоційної стійкості, який базується на стабільній психіці. Вам, швидше за все, не страшні ніякі емоційні стреси. Підтримуйте свою нервову систему в такому ж чудовому стані.

• Від 8 до 9 балів: ви досить врівноважені. Ви адекватно реагуєте на більшість стресових ситуацій. У вас середній рівень емоційної стійкості, тобто та норма, яка властива більшості людей.

• Від 15 до 20 балів: вас характеризує підвищений рівень емоційності. Вам слід опанувати прийоми і навички психічної саморегуляції (способи емоційного розвантаження), а можливо (хоча б іноді), приймати і заспокійливі збори трав.

ДОДАТОК В

**Тест за картинками “Довіра”**

Собаки – не лише найкращі друзі людини, а й дзеркало наших внутрішніх якостей та станів. Ваш вибір собаки у цьому тесті може розповісти багато про ваш рівень довіри та відкритість до світу.

Розібратися у собі вам допоможе тест за картинкою. Оберіть собаку, яка привертає вас найбільше, і дізнайтеся, що це говорить про вас.


Розшифровка результатів

Золотий ретрівер: Ваш вибір говорить про високий рівень довіри та позитивне ставлення до світу. Ви легко налагоджуєте зв’язки з з людьми і завжди готові протягнути руку допомоги. Ви цінуєте відвертість і лояльність у відносинах.

Німецька вівчарка: Вибір цієї собаки вказує на Вашу обережність та вимогливість у відносинах. Ви вірні друзі, але вам потрібен час, щоб відкритися новим людям. Ваша довіра заробляється чесністю та взаємною повагою.

Чихуахуа: Цей вибір показує, що ви дивитеся на світ з обережним оптимізмом. Ви відкриті до нових досвідів, але завжди оцінюєте потенційні ризики. Ви цінуєте глибокі, змістовні зв’язки та не поспішаєте довіряти незнайомцям.

Хаскі: Обираючи цю собаку, ви показуєте свою любов до життя та бажання досліджувати невідоме.Ви маєте високий рівень довіри до оточуючих та вірите у добрі наміри людей. Ваш оптимізм та ентузіазм часто надихають інших.

Джерело:

https://fun.24tv.ua/diznaytesya-sviy-riven-doviri-psihologichniy-test-za-kartinkoyu_n2523771

ДОДАТОК Г

**Тест за картинками “Стиль ухвалення рішень”**

Життя – це сукупність виборів та подій. Шляхи, які ми обираємо, і рішення, які ухвалюємо, визначають напрямок нашого курсу. Але яким же є ваш стиль ухвалення рішень?

Оберіть одну з чотирьох картинок нижче.


Розшифровка результатів

Картинка 1: Ваш вибір є відображенням вашої здатності до швидкого і впевненого ухвалення рішень. Це свідчить про те, що ви людина дії, яка не вагається перед новими викликами і можливостями. Ваша внутрішня сила і рішучість дозволяють вам впевнено крокувати крізь зміни, приймаючи їх як можливість для особистісного росту та розвитку. Ваша сміливість в ухваленні рішень може надихати оточуючих, оскільки ви виступаєте як приклад стійкості і адаптивності у постійно мінливому світі.

Картинка 2: Якщо ваш вибір припав на цю картину, це вказує на вашу схильність до ретельного аналізу та розмірковування перед ухваленням рішення.

Ви володієте здатністю до глибокого аналізу, завжди враховуючи потенційні наслідки ваших дій. Ви цінуєте обачність та витрачаєте час на розгляд усіх аспектів проблеми, шукаючи найбільш збалансоване та ефективне рішення.

Картинка 3: Обрання цієї картини вказує на вашу здатність зберігати спокій і раціональність у стресових або критичних ситуаціях. Ви не панікуєте і можете швидко адаптуватися до змінюваних обставин, знаходячи оптимальні рішення навіть під тиском. Ваша витримка та вміння зосереджуватися на фактах дозволяють вам ефективно розв'язувати складні задачі.

Картинка 4: Ваш вибір цієї картини свідчить про вашу вдумливість та стратегічний підхід до життя. Ви володієте високим рівнем планування і любите розглядати різні сценарії перед тим, як вчиняти. Ви вважаєте за краще діяти, виходячи з обдуманих рішень, які базуються на широкому огляді ситуації, що робить ваш підхід особливо ефективним у досягненні тривалого успіху.

Джерело:

https://fun.24tv.ua/viznachte-sviy-stil-priynyattya-rishen-za-dopomogoyu-psihologichnogo_n251901

ДОДАТОК Д

**Анкета “Психоемоційний вимір взаємодії соціальної інженерії в Інтернеті”**

1. Ви отримуєте електронні листи або повідомлення з невідомих джерел?

*Варіанти відповідей:*

- Так, дуже часто
- Так, але рідко
- Якщо лист від невідомого адресата, не відкриваю його
- Ні
- Не звертав уваги!

2. Чи відомі Вам схеми шахрайства, які можуть включати відправку фішингових листів або надання фальшивих пропозицій?

*Варіанти відповідей:*

- Так
- Ні
- Так, але я знаю, як діяти у такій ситуації
- Ні, але хотів про це більше дізнатися
- Так, я постраждав від цього

3. Чи знаєте Ви, що таке "соціальна інженерія" і які вона може мати загрози?

*Варіанти відповідей:*

- Так
- ні
- ні, але хотів про це дізнатися
- я з цим працюю
- не знала (в), що це називається соціальною інженерією

4. Чи знаєте Ви, як розпізнати підроблені повідомлення або веб-сайти?

*Варіанти відповідей:*

- так

- так, я знаю про це на своєму досвіді
- ні
- ні, але хотів (ла) про це більше дізнатися
- їх зустрічається все більше

5. Яка ймовірність того, що Ви відповіли б на повідомлення, яке обіцяє виграш чи нагороду, але вимагає надання особистої інформації?

*Варіанти відповідей:*

- обов'язково відповім
- не відповім
- подивлюся, що за винагорода
- що за безглузде питання! Авжеж, ні!
- з невідомих джерел - 0%, з надійних, перевірених, офіційних - 50%

Дякую за участь в опитуванні! Будьте пильними, хай жодні маніпулятивні техніки шахраїв не вплинуть на Вас та Ваш психоемоційний стан!

Джерело: https://docs.google.com/forms/d/1XeY29tREklZOJ9Dyby9HUUdRrT0HZwEY9Nkmy35yGBg/edit

ДОДАТОК Е

**Анкета “Інтернет-поведінка користувачів”**

Анкета для проведення дослідження впливу особливостей психіки користувачів методами соціальної інженерії в мережі Інтернет

1. Вкажіть Ваше ім’я та прізвище
2. Ваш вік
   - 18-25
   - 26-45
   - 46-60
   - 61-75
   - 76 і більше
3. Ваша зайнятість
   - працюю
   - тимчасово не працюю
   - навчаюся
   - пенсіонер
   - інше
4. У яких соціальних мережах Ви зареєстровані?
   - 


   - 

   - 

   - 


5. У якій соціальній мережі Ви найбільше проводите часу? Оберіть одну із переліку:

- 


- 

- 

- 



6. Скільки часу в день Ви тратите на перегляд новин, стрічок, акаунтів соціальних мереж, веб-сайтів?

- до 1 години на день
- 1- 3 години на день
- 4 - 6 годин на день
- більше 6 годин на день
- інше

7. Якою мірою довіряєте інформації, яку Ви отримуєте через соціальні мережі?

- довіряю повністю
- довіряю не завжди
- довіряю, але перевіряю
- не довіряю
- інше

8. Як Ви оцінюєте рівень безпеки онлайн-транзакцій та платежів?

- високий
- середній
- низький

- це реалії сучасного життя

9. Наскільки Ви відчуваєте, що маєте контроль над своїми особистими даними в Інтернеті?

- Слабкий(менше 25%)
- Задовільний (25-50%)
- Добрий (50-75%)
- Добрий (50-75%)

10. Чи впливає інформація з мережі Інтернет на Ваші особисті думки та дії?

- впливає 100%
- впливає частково
- впливає в залежності від інформації
- в залежності від мого емоційного стану
- ніяк не впливає
- інше

11. Чи стикалися Ви з випадками шахрайства в мережі Інтернет?

- ні, ніколи
- ні
- так
- так, це було з моїми знайомими і близькими
- я про це чув(ла)
- інше

12. Ви розумієте, що можна стати жертвою шахрайства, якщо ділитеся особистою інформацією з невідомими людьми в Інтернеті?

- так
- ні
- не замислювався над цим
- це біда сучасності

13. Чи маєте Ви план дій для випадків, коли вам здається, що хтось намагається вас обманути в Інтернеті?

- звісно
- не замислювався над цим
- зі мною такого не станеться!
- маю план дій
- треба про це більше дізнатися
- інше

Дякую за участь у анкеті!

Джерело:

https://docs.google.com/forms/d/1UxAbYxNRSnqGUy-cKBcWeguC5Gfg0sMZlWZ_VWddHXc/edit

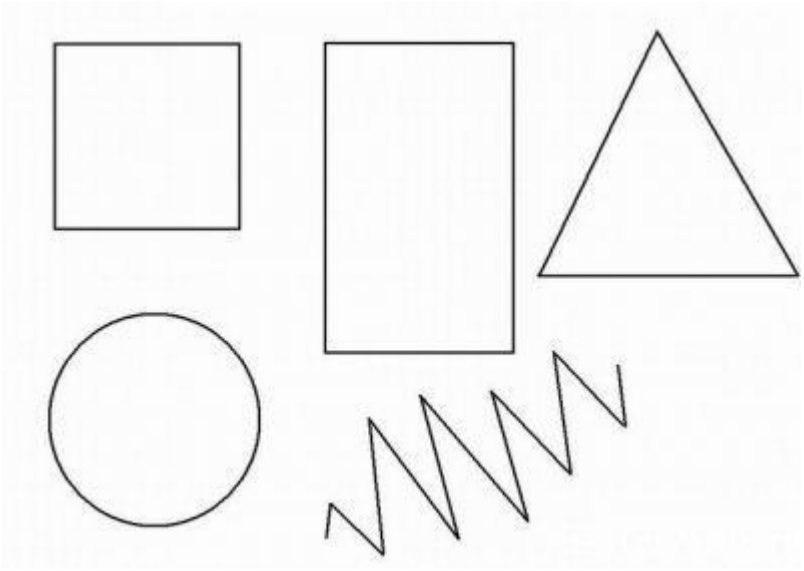
ДОДАТОК Є

**Проєктивна методика “Геометричні фігури”**

**(за Стюзеном Деллінгером)**

Коротка інструкція: Оберіть одну з 5 фігур, просто ту, що привернула Вашу увагу.

**Повна інструкція:** *Подивіться на п’ять фігур: квадрат, трикутник, прямокутник, круг, зигзаг. Оберіть з них ту, яка першою привабила Вас. Запишіть її назву під № 1. Тепер проранжуйте чотири фігури, що залишилися, в порядку переваги і запишіть їх назви під відповідними номерами*.



Перша обрана фігура – це власне ви, вона описує ваші домінуючі риси характеру і тип поведінки. Решта, в порядку убування – ті риси, які присутні, але в меншій мірі, або доповнюють домінуючу мелодію вашої поведінки.

**Квадрат**

Що за фігура? Рівненька, красива, акуратненька… Ось і людина, яка її обирає, людина типу «квадрат» — працелюбна, методична, акуратна, відповідальна, старанна, уважна… Десь навіть педантична, занадто любить порядок.

Невтомний трудівник. Володіє працьовитістю, ретельністю, завзятістю, що дозволяють завжди домагатися завершення роботи. Терпіння і методичність роблять з квадрата висококласного фахівця. Квадрат як би колекціонує інформацію, причому вона в нього розкладена суворо по поличках, тому він

здатний швидко витягати потрібну і заслужено має славу ерудитом у своїй галузі. Відноситься до лівопівкульним мислителям, для яких характерні логічне мислення і математичний аналіз. Квадрат швидше обчислює результат, ніж здогадується про нього.

Ідеал квадрата – розплановане, розмірене життя, де все передбачувано. Він не любить несподіванок і сюрпризів. У діловій сфері такі люди часто стають хорошими адміністраторами, виконавцями, але рідко досягають успіху як менеджери через постійну потреби в додатковій інформації для прийняття рішень – це позбавляє їх оперативності. Крім того, раціональність і холодність заважають квадратам швидко встановлювати контакти з іншими людьми.

Зазвичай квадрати обирають і відповідні професії: бухгалтер, аналітик, заступник директора з господарських питань, керівник у забюрократизованій організації тощо. На робочому місці в нього завжди порядок, кожна річ знаходиться там, де треба, у кожного папірчика є свій файлик або своя папка…

При всій інтелектуальній силі і прагненні квадрата до порядку, регламенту, дотримання чітких правил і приписів природно страждає емоційна сторона їх життя. Квадрати не люблять пустих і безцільних розмов, не дуже приділяють увагу проблемам і переживанням інших людей, через що останні можуть вважати їх бездушними. Квадрати дуже стримані у вираженні почуттів, вони рідко жестикулюють, їх мова може бути монотонною, навіть в’ялою, одноманітною.

Розглянемо трохи детальніше «сильні» і «слабкі» сторони квадратів. При цьому матимемо на увазі під «сильними» якостями ті прояви, які допомагають квадратам у повсякденному житті і діяльності, а під «слабкими» — ті, які заважають. На наш погляд, в однієї і тієї ж якості особистості можуть бути як позитивні, так і негативні прояви, залежно від того, наскільки ця якість адекватна ситуації, в якій перебуває суб’єкт.

Отже, сильні якості квадратів: старанність, дисциплінованість, раціональність, чесність, відповідальність, акуратність, пунктуальність, працьовитість, наполегливість, вірність слову. Слабкі сторони: негнучкість,

педантизм, сухість, нерішучість, упертість, боязнь ризику, замкненість, скупість, схильність до бюрократизму, спротив новому, нетовариськість, неемоційність.

Як спілкуватися з квадратом? Поважати всі регламенти, процедури і правила, які використовує квадрат. Хвалити ті досконалі, ідеальні результати, які він отримав, той стерильний порядок, що йому вдалося створити. Завжди уважно і до кінця слухайте квадрата, якщо хочете і далі спілкуватися з ним і не нажити собі ворога.

**Трикутник**

Ця форма символізує лідерство. Головна здатність – концентруватися на наміченій меті, глибоко і швидко аналізувати ситуацію. Тому, хто обирає цю фігуру як найбільш переважну, важливо бути першим, вести людей за собою, захоплювати їх, управляти ними, мати владу над іншими.

Вони орієнтовані на те, щоб зайняти якомога вище соціальне положення. Трикутникам дуже подобається, коли хтось слухає їх з відкритим ротом, захоплюється ними та їх успіхами, надає позитивні оцінки їх поведінці. Отже, у трикутника дві основні цінності — влада і досягнення.

Трикутник – дуже впевнена у собі людина, яка хоче бути правою у всьому. З великими труднощами визнає свої помилки, легко навчається, інформацію вбирає як губка. Сенс життя – зробити кар’єру. Негативна якість – надмірний егоцентризм. Він чудово вміє представити вищестоящому керівництву значимість власної роботи, за версту відчуваючи вигідну справу, і в боротьбі за нього може “зіштовхнути лобами” своїх супротивників.

Зрозуміло, що трикутники на професійному терені найчастіше стають керівниками, політиками, бізнесменами… У цих людей широкі, розмашисті жести, упевнена хода, гучна мова.

Сильними сторонами їх особистості є цілеспрямованість, раціональність, орієнтованість на результат, сміливість, рішучість, ініціативність, енергійність, харизматичність. Слабкі сторони: егоїзм, владність, самовпевненість, нечутливість до нюансів, безжальність…

Якщо ви спілкуєтеся з трикутником, будьте готові до його нетерплячості, вам потрібно викласти інформацію максимально швидко, при цьому мотивувати трикутника його власною вигодою. Спочатку йому потрібно пояснити, навіщо йому взагалі варто про щось знати. Ну і не забувайте компліменти стосовно останніх проектів і кар'єрних просувань трикутника.

**Прямокутник**

Це як би перехідна форма від однієї фігури до іншої. Прямокутником сприймають себе люди, не задоволені своїм життям і тому зайняті пошуками кращого положення. Основний психічний стан прямокутника – усвідомленого відчуття замішання, заплутаності в проблемах, невизначеності. Найбільш значущі риси – непослідовність, непередбачуваність вчинків, низька самооцінка. Позитивні якості – допитливість, цікавість, живий інтерес до всього що відбувається, сміливість. Намагається робити те, що ніколи раніше не робив, задає питання, на які колись у нього не вистачало духу.

У практиці управління С. Деллінгер рекомендує відправляти співробітника-прямокутника у відпустку. Враховуючи сильні сторони прямокутників, які ви побачите нижче, нам здається, що їх також можна записувати на курси підвищення кваліфікації, тренінги, конференції і лекції, щоб вони отримували нову інформацію, яка сприяла б позитивним змінам.

Навіть такий, нехай кризовий і перехідний, стан має свої позитивні сторони: відкритість новому досвіду, висока здатність до навчання, допитливість, готовність вислухати і приміряти на себе думку іншої людини. Слабкі сторони? Так, і їх достатньо багато: невпевненість, тривожність, недовірливість, емоційна нестійкість.

Спілкуючись з прямокутником, важливо підтримувати його, не кричати і не критикувати. Постарайтеся також зрозуміти, до якої фігури прямокутник ближче за своїм станом, підтримайте його спробу все-таки схилитися в ту чи іншу сторону.

**Коло**

Це символ гармонії. Коло — людина-комунікатор, справжня душа компанії, дипломат. Той, хто вибрав цю фігуру, зацікавлений у хороших міжособистісних відносинах. Вища цінність для кола – люди і їх благополуччя. Це найбільш доброзичлива з п’яти фігур. Коло служить свого роду клеєм, який скріпляє колектив, сім’ю, стабілізує групу, має високу здатність співчуття, співпереживання. Коло відчуває чужу радість і чужий біль як свій власний. Це правопівкульний тип мислення, що не логічний, а образний, більш емоційно забарвлений. Переробка інформації у таких людей не послідовна, а мозаїчна.

Головна риса стилю їхнього мислення – орієнтація на суб’єктивні чинники проблеми.

Отже, основна цінність круга — спілкування з іншими людьми. Відповідно їм підходять професії, пов’язані з комунікацією, — педагоги, священики, менеджери з персоналу, секретарі, психологи.

Сильні сторони круга: комунікабельність, доброта, м’якість, неконфліктність, терпимість, делікатність, дипломатичність, доброзичливість. Слабкі сторони: пасивність, нерішучість, схильність погоджуватися, навіюваність, залежність від думки оточення, непунктуальність, неорганізованість. Круги емоційні, відкриті, товариські, схильні до компромісів. Як спілкуватися з кругом? О! Він сам вас знайде.

Проте його потрібно повертати до суті питання, нагадувати про цілі, критерії, строки. Про всі ці незначні в порівнянні з людським життям і почуттями речі він схильний забувати, чим може серйозно зашкодити організації.

**Зигзаг**

Є в цьому світі незвичайні люди, вони бачать цей світ по-своєму, їх думка часто не збігається з думкою інших, вони придумують нові слова, пишуть картини, люблять дивний одяг і непрості книги… Так, усе це про зигзаги.

Це символ творчості. Йому властива образність. Правопівкульне мислення зигзага не фіксуються на деталях, тому воно, спрощуючи в чомусь картину світу, дозволяє будувати цілісні, гармонійні концепції і образи, бачити красу. Зигзаг не

може довго працювати на одному місці – це ж дуже нудно, але ж навколо так багато цікавого!

Основне призначення зигзага – генерація нових ідей і методів, а не їх реальне втілення. Він спрямований у майбутнє і більше цікавиться можливістю, ніж дійсністю.

У зигзагів особливе мислення. Там, де квадрат або трикутник рухається з пункту А в пункт Б і лише потім у пункт В, тобто їх логіка лінійна і послідовна, там зигзаг скаче з Я в А і взагалі легко допускає невраховану конфігурацію, одночасну присутність АЯВБА. Вони схильні схоплювати рішення відразу як цілісність, а не рухатися до нього поступово, розглядати навіть найбільш маловірогідний варіант як істинний, просто тому, що він цікавий, осягати рішення інтуїтивно, а не шляхом довгих і послідовних міркувань.

З особливої цінності власних ідей для зигзагів виходить те, що вони часто живуть у якомусь власному, дивовижному і прекрасному, але не дуже реалістичному світі.

Які професії підходять зигзагу? Ну, звичайно ж, усі творчі: артист, креативний директор, дизайнер, художник, страховий агент…

До сильних сторін зигзага можна віднести: креативність, дотепність, оригінальність, напористість, спонтанність, захопливість. До слабких: непередбачуваність, нестриманість, індивідуалізм, непостійність, некерованість.

Як спілкуватися із зигзагом? Терпіння, тільки терпіння! Висловлюйте зигзагу захоплення його ідеями, адже він їх цінує найбільше. Будьте готові повторювати і нагадувати по сто разів, оскільки зигзаг усе одно все робитиме по-своєму. Не дивуйтеся змінам настрою, планів, думок, для зигзага це нормально. Іноді корисно піти шляхом шкідливої поради. Скажіть, як ви не хочете, щоб зигзаг діяв, і скоріше за все він так і вчинить. Хоча, так, з останньою порадою варто бути обережним, усе-таки дуже ці зигзаги непередбачувані.

Що ж, ось ми і розглянули основні якості кожного з типів особистості в психогеометричному підході і навіть трохи торкнулися того, як з ними спілкуватися.