МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

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

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “МЕТОДИКА ВПРОВАДЖЕННЯ НАВЧАЛЬНИХ КАМПАНІЙ ДЛЯ ПІДВИЩЕННЯ ОБІЗНАНОСТІ СПІВРОБІТНИКІВ ПРО СОЦІОІНЖЕНЕРНІ ЗАГРОЗИ”

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

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

_____ Аліна РЕДЬКІНА
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконала: здобувачка вищої освіти гр. УБД-41

Аліна РЕДЬКІНА
Ім’я, ПРІЗВИЩЕ

Керівник: Михайло ЗАПОРОЖЧЕНКО
Доктор філософії з кібербезпеки Ім’я, ПРІЗВИЩЕ

Рецензент: _____
_____ Ім’я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

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

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Редькіній Аліні Вікторівні
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Методика впровадження навчальних кампаній для підвищення обізнаності співробітників про соціоінженерні загрози”,
керівник кваліфікаційної роботи ЗАПОРОЖЧЕНКО Михайло, доктор філософії з кібербезпеки
(ПРІЗВИЩЕ, Ім’я, науковий ступінь, вчене звання)

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

2. Строк подання кваліфікаційної роботи “12” травня 2025р.

3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека підприємства, методи та засоби управління персоналом з інформаційної безпеки, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
4.1. Визначити сутність соціальної інженерії, класифікувати основні види технік та чинників, що впливають на сприйнятливість працівників.
4.2. Проаналізувати існуючі підходи до організації навчання персоналу щодо протидії соціоінженерним загрозам.
4.3. Розробити методику впровадження навчальної кампанії з протидії соціоінженеррним загрозам.
4.4. Реалізувати навчальну кампанію в умовах організації, оцінити зміни у рівні обізнаності персоналу.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “5“ березня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2025	
2.	Збір та аналіз літератури.	29.03.2025	
3.	Аналіз теоретичних основ протидії соціоінженерним загрозам у сфері інформаційної безпеки	08.04.2025	
4.	Дослідження методологічних підходів до розроблення навчальних кампаній із підвищення рівня обізнаності персоналу	15.04.2025	
5.	Практична реалізація та оцінювання результатів навчальної кампанії з протидії соціоінженерним загрозам	22.04.2025	
6.	Формулювання висновків за результатами проведеного дослідження.	29.04.2025	
7.	Оформлення роботи.	06.05.2025	
8.	Оформлення презентації.	09.05.2025	
9.	Отримання рецензії на роботу.	12.06.2025	
10.	Захист в ДЕК.	__.06.2025	

Здобувачка вищої освіти _____ Аліна РЕДЬКІНА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Михайло ЗАПОРОЖЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

Направляється здобувачка Редькіна А.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Методика впровадження навчальних кампаній для підвищення обізнаності співробітників про соціоінженерні загрози"

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувачка РЕДЬКІНА Аліна у кваліфікаційній роботі дослідила соціоінженерні загрози в корпоративному середовищі, класифікувала їх, проаналізувала чинники вразливості персоналу та розробила методику побудови навчальної кампанії з підвищення обізнаності. У практичній частині успішно реалізовано навчальну програму в реальному корпоративному середовищі з оцінкою її ефективності.

Робота демонструє високий рівень теоретичної підготовки та практичних навичок здобувачки. РЕДЬКІНА Аліна проявила самостійність, відповідальність та вміння застосовувати здобуті знання. Результати дослідження апробовані на конференції.

Все це дозволяє оцінити кваліфікаційну роботу здобувачки РЕДЬКІНОЇ Аліни на оцінку "відмінно" та присвоїти їй кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Михайло ЗАПОРОЖЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувачка Редькіна А.В. допускається до захисту даної роботи в Екзаменаційній комісії.

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

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувачки вищої освіти РЕДЬКІНОЇ Аліни
на тему “Методика впровадження навчальних кампаній для підвищення обізнаності співробітників про соціоінженерні загрози”

Актуальність. В умовах активної цифровізації суспільства соціоінженерні атаки залишаються одними з найнебезпечніших інструментів зловмисників, оскільки спрямовані не лише на технічні, а й на психологічні вразливості людини. Незважаючи на розвиток технічних засобів захисту, людський фактор продовжує відігравати визначальну роль у забезпеченні інформаційної безпеки. Відтак, розробка ефективних навчальних програм, орієнтованих на підвищення обізнаності персоналу щодо соціоінженерних загроз, є вкрай важливим і науково обґрунтованим завданням. Дослідження, присвячене практичному впровадженню навчальної кампанії та оцінюванню її ефективності, має вагоме прикладне значення для підвищення кіберстійкості організацій.

З огляду на це, вивчення методик впровадження освітніх кампаній для підвищення обізнаності працівників про соціоінженерні загрози є актуальним і своєчасним науковим завданням.

Позитивні сторони.

1. У роботі здійснено глибокий аналіз природи соціоінженерних атак, їх класифікації та особливостей впливу на інформаційну безпеку організацій.
2. Представлено обґрунтований методологічний підхід до побудови навчальної кампанії з протидії соціоінженерним загрозам, включаючи вибір освітніх методів та визначення критеріїв ефективності.
3. Проведено експериментальне впровадження навчальної програми, що дозволило оцінити початковий рівень обізнаності працівників, зафіксувати зміни після навчання та сформулювати рекомендації щодо вдосконалення процесу.

Недоліки.

Доцільним було б доповнити роботу оглядом і порівняльним аналізом спеціалізованих програмних рішень, що використовуються для автоматизації процесів навчання та тестування персоналу (зокрема систем управління навчанням або платформ для моделювання фішингових атак).

Зазначене зауваження має уточнюючий характер і не впливає на загальну позитивну оцінку кваліфікаційної роботи.

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

Рецензент:
_____ _____ _____
підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню технологій формування обізнаності й навчання персоналу з інформаційної безпеки. Робота складається зі вступу, трьох розділів, що містять 28 рисунків, висновків і списку використаних джерел із 47 найменувань. Загальний обсяг роботи становить 99 аркушів, з яких 6 аркушів займає список використаних джерел.

Метою роботи є підвищення рівня обізнаності співробітників організації щодо соціоінженерних загроз шляхом розроблення та впровадження ефективної навчальної кампанії з урахуванням чинників, що впливають на сприйнятливість працівників до маніпуляцій, а також сучасних підходів до організації навчання персоналу.

Об'єктом дослідження є процес організації навчання персоналу з питань протидії соціоінженерним загрозам.

Предмет дослідження – методика розробки і впровадження навчальних кампаній, спрямованих на підвищення обізнаності персоналу про соціоінженерні загрози.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, класифікації, емпіричного методу, системного підходу до оцінювання рівня обізнаності співробітників.

Галузь застосування. Запропоновані підходи можуть бути використані під час розробки та впровадження навчальних кампаній у рамках системи управління інформаційною безпекою організацій. Особливо корисними ці рішення є для підвищення обізнаності співробітників щодо соціоінженерних загроз, формування навичок безпечної цифрової поведінки та зниження ризику людського чинника у сфері кіберзахисту.

Ключові слова: СОЦІАЛЬНА ІНЖЕНЕРІЯ, ІНФОРМАЦІЙНА БЕЗПЕКА, НАВЧАННЯ ПЕРСОНАЛУ, ОБІЗНАНІСТЬ ЩОДО КІБЕРЗАГРОЗ, ПРОТИДІЯ СОЦІОІНЖЕНЕРНИМ АТАКАМ, НАВЧАЛЬНА КАМПАНІЯ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

ABSTRACT

The qualification thesis is devoted to the study of technologies for raising awareness and training personnel in information security. The thesis consists of an introduction, three chapters including 28 figures, conclusions, and a list of references comprising 47 sources. The total volume of the work is 99 pages, of which 6 pages are occupied by the list of abbreviations and references.

The purpose of the study is to increase the level of employees' awareness regarding social engineering threats by developing and implementing an effective training campaign, taking into account the factors influencing their susceptibility to manipulation and modern approaches to organizing staff training.
The object of the study is the process of organizing personnel training on countering social engineering threats.

The object the study is the principles of awareness and training for personnel.

The subject of the study is the methodology of developing and implementing training campaigns aimed at increasing employees' awareness of social engineering threats.

Research methods. In order to solve the above-mentioned scientific task, the methods of analysis and synthesis, comparison, classification, expert assessment, and a systematic approach to information security management were used.

Field of application. The proposed approaches can be used in the development and implementation of training campaigns within the framework of the organization's information security management system. They are especially useful for increasing employees' awareness of social engineering threats, developing safe digital behavior skills, and reducing the human factor risks in cybersecurity.

Keywords: SOCIAL ENGINEERING, INFORMATION SECURITY, STAFF TRAINING, CYBER THREAT AWARENESS, COUNTERING SOCIAL ENGINEERING ATTACKS, INFORMATION SECURITY TRAINING CAMPAIGN.

ЗМІСТ

ВСТУП

Актуальність теми. У світі, де держави, компанії та навіть окремі користувачі є об’єктом кібератак, забезпечення інформаційної безпеки є важливим, як ніколи. До того ж, IT-сфера постійно розвивається, а разом з цим зростають інформаційні ризики і загрози. Важливо формувати культуру безпеки серед персоналу підприємства, забезпечуючи працівникам необхідні знання й навички для виявлення загроз інформаційній безпеці. Інноваційні підходи до навчання персоналу з інформаційної безпеки можуть допомогти підтримувати персонал у курсі останніх трендів та методів захисту і, як наслідок підвищити рівень інформаційної безпеки підприємства.

Мета роботи **–** підвищення рівня обізнаності співробітників організації щодо соціоінженерних загроз шляхом розроблення та впровадження ефективної навчальної кампанії з урахуванням чинників, що впливають на сприйнятливість працівників до маніпуляцій, а також сучасних підходів до організації навчання персоналу.

Об’єкт дослідження **–** процес організації навчання персоналу з питань протидії соціоінженерним загрозам.

Предмет дослідження – методика розробки і впровадження навчальних кампаній, спрямованих на підвищення обізнаності персоналу про соціоінженерні загрози.

Для досягнення цієї мети в роботі необхідно виконати наступні завдання:

1. Визначити сутність соціальної інженерії, класифікувати основні види технік та чинників, що впливають на сприйнятливість працівників.

2. Проаналізувати існуючі підходи до організації навчання персоналу щодо протидії соціоінженерним загрозам.

3. Розробити методику впровадження навчальної кампанії з протидії соціоінженеррним загрозам.

4. Реалізувати навчальну кампанію в умовах організації, оцінити зміни у рівні обізнаності персоналу.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, класифікації, емпіричні методи (спостереження, експеримент), системного підходу до оцінювання рівня обізнаності співробітників.

Практичне значення одержаних результатів. Застосування напрацювань дасть змогу здійснити обґрунтований вибір методів і інструментів формування обізнаності й навчання персоналу як важливого елемента управління інформаційною безпекою відповідно до цілей бізнесу, можливостей та ресурсів підприємства.

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

Розділ 1 ТЕОРЕТИЧНІ ОСНОВИ ПРОТИДІЇ СОЦІОІНЖЕНЕРНИМ ЗАГРОЗАМ У СФЕРІ ІНОРМАЦІЙНОЇ БЕЗПЕКИ

У межах першого розділу представлено формалізацію поняття соціальної інженерії та здійснено класифікацію методів, що використовуються зловмисниками для маніпулятивного впливу на користувачів. Окрему увагу приділено аналізу існуючих підходів до протидії соціоінженерним загрозам, оцінці впливу таких загроз на підхід організації до управління інформаційною безпекою, а також дослідженню чинників, що визначають рівень сприйнятливості персоналу до маніпулятивного впливу. Аналіз зазначених аспектів дозволяє забезпечити цілісне розуміння теоретичних основ і закласти підґрунтя для подальшого формування ефективної стратегії підвищення обізнаності персоналу.

1.1 Формалізація поняття соціальної інженерії та класифікація методів її реалізації

У сучасному інформаційному суспільстві, що характеризується високим рівнем цифровізації процесів, інформація набула статусу стратегічного активу, вразливість якого є об’єктом цілеспрямованого впливу з боку зловмисників. Кіберзагрози, що постають перед організаціями, дедалі частіше пов’язані не лише з технічними вразливостями, а й із так званим “людським чинником” – сукупністю психологічних, поведінкових та організаційних характеристик, що зумовлюють вразливість користувача до зовнішніх впливів.

Однією з найпоширеніших і водночас найбільш складних для виявлення форм таких загроз є соціальна інженерія – сукупність методів, що базуються на використанні соціально-психологічних механізмів впливу на осіб з метою отримання несанкціонованого доступу до інформаційних активів або реалізації інших цілей, які суперечать інтересам організації. Замість технічного втручання, соціальна інженерія експлуатує довіру, обмежену обізнаність, емоційну

вразливість або відсутність критичного мислення у цільової особи. У цьому контексті користувач інформаційної системи розглядається як потенційний об’єкт атаки, через який зловмисник може ефективно обійти формалізовані технічні заходи захисту.

На відміну від традиційних кібератак, що передбачають використання зловмисного програмного забезпечення або експлуатацію технічних вразливостей, соціальна інженерія базується на спотворенні соціальної взаємодії, де головним інструментом виступає комунікативний тиск або введення в оману. Саме тому навіть у середовищах із високим рівнем технічного захисту соціоінженерні атаки залишаються ефективним методом обходу систем безпеки.

Водночас соціоінженерні техніки дедалі частіше використовуються не лише щодо фізичних осіб або суб’єктів господарювання приватного сектору, а й проти працівників державних установ, органів виконавчої влади, силових структур та критичної інфраструктури. Така трансформація об’єктів атак свідчить про цілеспрямоване використання соціоінженерних атак як складової частини інформаційно-психологічних операцій, спрямованих на компрометацію осіб, що мають доступ до службової інформації обмеженого або конфіденційного характеру.

Наслідки реалізації подібних атак можуть мати системний характер, оскільки порушення конфіденційності службової інформації, у контексті функціонування державних інституцій, безпосередньо впливає на стабільність управлінських процесів, ефективність міжвідомчої взаємодії та загальну стійкість інституціонального середовища.

Поширення загроз соціоінженерного характеру становить суттєву загрозу для елементів національної безпеки, оскільки подібні атаки здатні порушувати політичну стабільність, впливати на економічну ситуацію, дестабілізувати суспільні настрої та знижувати рівень обороноздатності. В умовах гібридного середовища безпеки, що передбачає одночасне використання технічних, інформаційних та психологічних векторів впливу, необхідність формування

цілісної системи протидії соціоінженерним атакам набуває особливої ваги та стратегічного значення [1].

Згідно з аналітичними звітами Державної служби спеціального зв'язку та захисту інформації України, впродовж останніх років спостерігається стабільне зростання кількості кіберінцидентів, у яких ключову роль відіграють техніки соціальної інженерії. Так, лише у 2023 році на території України було зафіксовано понад 3000 випадків фішингових атак, що на 25% перевищує відповідний показник за 2022 рік [2]. Паралельно з цим зростає активність вішингових атак, зокрема спрямованих на незаконне отримання банківських реквізитів, облікових даних та персональної інформації громадян.

Аналіз сучасних соціоінженерних технік свідчить про зростаючу різноманітність методів, що застосовуються зловмисниками для отримання несанкціонованого доступу до конфіденційної інформації. Основною спільною ознакою таких методів є використання психологічного впливу, що має на меті зміну поведінки користувача без застосування технічного втручання в інформаційну систему. Найбільш поширені на сьогодні форми реалізації соціальної інженерії представлені на рисунку 1.1.

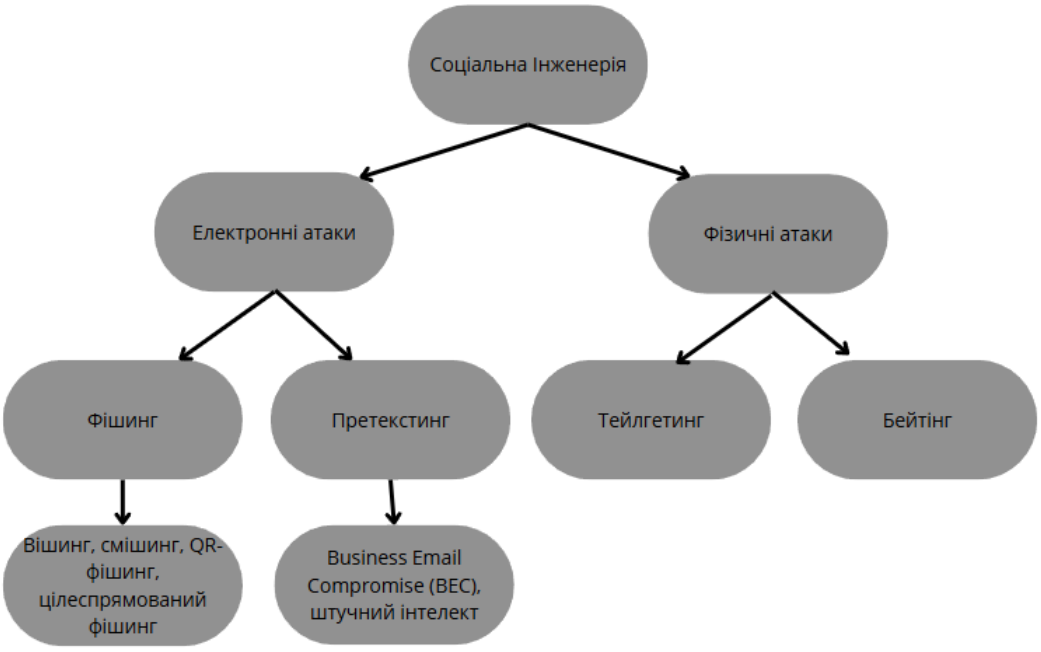

Рис. 1.1. Класифікація форм реалізації соціальної інженерії

Нижче наведено короткий опис зазначених технік:

- фішинг – практика масової розсилки електронних листів, що імітують повідомлення від легітимних установ (банків, державних органів, постачальників послуг тощо). Повідомлення зазвичай містить гіперпосилання на фальшивий веб-ресурс, що візуально копіює інтерфейс справжнього сайту. Основна мета – отримання автентифікаційних даних користувача (логінів, паролів, реквізитів платіжних карток тощо), які можуть бути використані для шахрайства;
- вішинг – метод, що полягає у телефонному зверненні зловмисника, який видає себе за представника банку, служби безпеки або правоохоронного органу. Застосовуючи техніки соціального тиску, зокрема створення ілюзії термінової загрози (наприклад, повідомлення про блокування рахунку чи спробу несанкціонованої транзакції), зловмисник стимулює особу до передачі конфіденційних даних або вчинення інших небажаних дій;
- смішинг – різновид фішингу, що реалізується через текстові повідомлення. Користувачу надсилається SMS із посиланням на шкідливий ресурс або із проханням зв’язатися за певним номером. Часто повідомлення імітують офіційну комунікацію від банку, поштової служби, мобільних операторів чи іншої авторитетної організації. Мета полягає у викраденні даних або зараженні пристрою шкідливим програмним забезпеченням [1];
- QR-фішинг – метод, який використовує підроблені QR-коди. Користувач сканує QR-код (наприклад, у кафе, транспорті або на рекламному банері), який перенаправляє його на фішинговий сайт або інсталює шкідливе ПЗ. Особливо небезпечно те, що візуально користувач не може перевірити, на який ресурс він потрапляє після сканування [3];
- цілеспрямований фішинг – метод, орієнтований на конкретну особу або організацію. Його відмінною рисою є персоналізований підхід: зловмисники вивчають діяльність цільової особи, її службову роль, стиль комунікації, щоб створити правдоподібне повідомлення. Така атака має набагато вищий рівень успішності порівняно з масовим фішингом [4];

- претекстинг – метод, що базується на попередньо створеній легенді, у межах якої зловмисник видає себе за довірену або авторитетну особу з метою отримання конфіденційної інформації. Найчастіше атака здійснюється через телефонний дзвінок або повідомлення в месенджерах (Telegram, WhatsApp тощо). Завдяки збору інформації з відкритих джерел (OSINT), зловмисники створюють максимально достовірні сценарії взаємодії, що викликають довіру жертви [5];
- Business Email Compromise (BEC) – один із найнебезпечніших типів соціоінженерних атак, у якому використовується підробка електронної пошти вищого керівництва. Зловмисники просять працівників здійснити терміновий платіж або надати фінансову інформацію. Часто для цього застосовується компрометація корпоративного облікового запису або реєстрація домену, схожого на легітимний. Нападники зазвичай довго стежать за внутрішньою перепискою організації, щоб не викликати підозр [6, 7];
- персоналізований фішинг із використанням штучного інтелекту – сучасна форма атак, коли за допомогою штучного інтелекту генеруються фішингові листи, чат-повідомлення або навіть дзвінки, що імітують стиль спілкування реальних осіб. ШІ дозволяє швидко проаналізувати дані з відкритих джерел (профілі у соцмережах, сайти компаній, блоги) й автоматично створити персоналізовані сценарії атак. В окремих випадках використовується генерація фейкових облич або голосів [8, 9];
- тейлгетинг – фізичний метод атаки, коли зловмисник проникає у захищене приміщення, проходячи за співробітником, який має дозвіл на доступ. Атака базується на людській ввічливості або небажанні створювати конфлікт. Часто шахрай вдає, що несе великі речі або розмовляє по телефону, щоб уникнути підозр;
- бейтінг – ще один метод соціальної інженерії, коли зловмисники залишають USB-накопичувачі, телефони або інші цифрові пристрої у публічних місцях. Потенційна жертва, намагаючись допомогти або з цікавості, підключає

пристрій до корпоративної системи, що призводить до інфікування вірусами або до встановлення бекдорів [4].

Більшість зазначених методів реалізації соціоінженерних атак ґрунтуються на цілеспрямованому психологічному впливі, що спричиняє зміну поведінки цільової особи без фізичного примусу. У процесі атаки активно використовуються когнітивні й емоційні тригери, які значною мірою впливають на здатність користувача критично осмислювати отриману інформацію. Найпоширенішими з них є:

- авторитетність джерела – імітація комунікації з боку офіційної установи, уповноваженої особи або загальновідомого сервісу;
- терміновість – створення враження обмеженого часу для реагування з метою пришвидшення прийняття рішень;
- виклик страху – використання потенційних загроз (блокування рахунків, штрафи, дисциплінарні заходи) як засобу тиску;
- мотивація винагородою – обіцянка матеріальних або нематеріальних вигод, що спонукає до дій без належної перевірки достовірності джерела.

Застосування вказаних прийомів спрямоване на те, щоб викликати імпульсивну реакцію з боку користувача – тобто прийняття рішень у стані когнітивного перевантаження або емоційної напруги, без застосування механізмів раціональної оцінки ризику. Такий підхід суттєво підвищує ефективність атак і виявляє вразливість навіть серед користувачів із базовою технічною підготовкою.

Типова структура атаки з використанням соціоінженерних технік включає кілька послідовних етапів, які представлені на рисунку 1.2.

1. Ідентифікація цільового об’єкта впливу (конкретної особи або групи осіб, вибір яких часто обумовлюється доступом до критичних ресурсів або роллю в організаційній структурі) та формування очікуваного результату атаки (отримання облікових даних, компрометація службової інформації, ініціювання фінансових транзакцій, встановлення шкідливого програмного забезпечення тощо).

Рис. 1.2. Схема-алгоритм атаки з використанням соціоінженерних технік

2. Збір інформації про об’єкт впливу шляхом аналізу відкритих джерел (OSINT) в т.ч. соціальних мереж, корпоративних сайтів, електронних публікацій, метаданих документів, фото- й відеоматеріалів з метою отримання персональних, професійних або контекстуальних даних, що можуть бути використані для персоналізації сценарію атаки. На цьому етапі зловмисник також вивчає типові шаблони комунікацій, стиль поведінки, коло контактів та внутрішні регламенти.

3. Формування та реалізація сценарію впливу на основі зібраної інформації, що передбачає створення ситуаційної моделі, тобто штучно сконструйованого середовища або інформаційної події, яка викликає довіру або спонукає до дій відповідно до очікуваної поведінки. Такий вплив може здійснюватися через електронну пошту, телефонні дзвінки, SMS-повідомлення, соціальні мережі або особисту комунікацію. Ключовими характеристиками цього етапу є використання соціальних тригерів (довіра, авторитет, терміновість,

страх, мотивація вигодою) та повна відсутність необхідності технічного втручання в інформаційну систему [10].

4. Аналіз результатів, під час якого перевіряється, чи були досягнуті цілі атаки: чи отримано доступ до конфіденційної інформації, чи виконала жертва необхідні дії. Також зловмисник оцінює рівень підозри з боку користувача або IT-безпеки.

5. Приховування слідів – на цьому етапі здійснюються дії для мінімізації вірогідності виявлення атаки: видалення слідів комунікації, знищення шкідливого ПЗ, використання анонімізуючих технологій. Це ускладнює подальше розслідування та затримку порушника.

У складніших випадках атака може включати додаткові етапи, які підвищують її результативність, зокрема:

- тестування реакції об’єкта впливу на первинні стимули (наприклад, контроль відкриття листа або клік на посилання) з метою адаптації подальших дій;
- повторні цикли впливу, які передбачають ескалацію загроз або підвищення психологічного тиску;
- розширення охоплення через мережеву взаємодію, коли атака поширюється на колег, підлеглих або керівників цільової особи з урахуванням її комунікаційного контексту.

У разі цільових атак (spear phishing, whaling), вищезазначені етапи реалізуються з високим рівнем деталізації, що значно ускладнює виявлення спроб компрометації з боку механізмів захисту організації.

Отже, соціальна інженерія є цілеспрямованим інструментом несанкціонованого доступу до інформаційних ресурсів, що базується на маніпулятивному впливі на користувача та експлуатації його поведінкових особливостей. Різноманіття технік, зростання частоти атак і поширення таких загроз на державний сектор свідчать про високий рівень їх ефективності. У зв’язку з цим виникає потреба у аналізі підходів, які використовуються організаціями для виявлення, запобігання та мінімізації наслідків соціоінженерних атак.

1.2 Аналіз підходів та практик організацій щодо запобігання соціоінженерним атакам

В умовах стрімкого зростання кількості кіберзагроз і підвищеної активності зловмисників, які застосовують техніки соціальної інженерії, забезпечення належного рівня інформаційної безпеки набуває пріоритетного значення для організацій незалежно від їхнього галузевого спрямування та масштабу діяльності. Оскільки соціоінженерні атаки спрямовані не на технічні вразливості, а на експлуатацію людського фактору, ефективне протистояння таким загрозам потребує реалізації комплексної системи заходів захисту – організаційних, технічних і, насамперед, навчальних (рис. 1.3).

Рис. 1.3. Комплексна система заходів захисту протидій соціальній інженерії

Організаційні підходи включають нормативне та процедурне забезпечення інформаційної безпеки. Зокрема, йдеться про розробку внутрішніх політик і регламентів, що встановлюють правила взаємодії з невідомими особами, порядок обробки підозрілих повідомлень, а також включення аспектів соціальної інженерії до процедур управління інцидентами [11]. До організаційних заходів також належить застосування принципу мінімальних привілеїв, проведення регулярних аудитів (у тому числі з використанням методів соціальної інженерії або перевірок фізичної безпеки), атестація співробітників, а також залучення HR-підрозділів для виявлення психологічних станів, що можуть свідчити про

вразливість до маніпулятивного впливу [12]. Основною перевагою таких підходів є забезпечення системного контролю за поведінкою персоналу. Недоліком є необхідність постійної актуалізації політик і високий рівень управлінської відповідальності. Застосування організаційних заходів дозволяє зменшити ризики необізнаності працівників і несанкціонованого доступу через психологічний вплив.

Навчальні підходи орієнтовані на підвищення рівня обізнаності персоналу щодо соціоінженерних загроз. До них належать проведення навчальних кампаній, тренінгів з інформаційної безпеки з демонстрацією типових сценаріїв атак, моделювання фішингових інцидентів, а також використання візуальних засобів інформування (інфографіка, плакати, нагадування у робочому середовищі) [13]. Ефективним елементом є також ігрове моделювання ролей “нападника” і “захисника”, що дозволяє сформувати поведінкові шаблони в умовах соціального тиску. Перевагою таких підходів є формування навичок розпізнавання атак, розвиток культури кібергігієни та залучення працівників до процесу безпеки. Обмеженням виступає необхідність регулярного оновлення програм і залежність результативності від мотивації персоналу [14]. Ці підходи спрямовані на зниження ризику успішного психологічного впливу через необізнаність або низьку стійкість до маніпуляцій.

Технічні підходи передбачають впровадження засобів інформаційної безпеки, які ускладнюють реалізацію соціоінженерних атак або дозволяють оперативно їх виявляти. До таких заходів належать використання багатофакторної автентифікації, яка знижує ризик компрометації облікових даних, фільтрація електронної пошти з автоматичним виявленням ознак фішингу, перевіркою вкладень, посилань та доменів, логування та моніторинг дій користувачів з метою виявлення аномальної поведінки, а також сегментація мережі для обмеження поширення загроз. Переваги технічних засобів полягають у високій швидкості реагування та автоматизації процесів виявлення. Серед недоліків – потреба в ресурсах на впровадження, обслуговування та постійне оновлення систем. Вони дозволяють мінімізувати ризик успішного вторгнення

шляхом технічного захисту каналів, які можуть бути використані зловмисниками.

У цьому контексті особливу актуальність має систематизований аналіз існуючих підходів та практик протидії соціальній інженерії, що впроваджуються як у державному, так і в корпоративному секторах. Дослідження таких практик дозволяє ідентифікувати ефективні моделі захисту, оцінити релевантність обраних інструментів і розробити обґрунтовані рекомендації для посилення організаційної стійкості до соціоінженерних загроз.

З урахуванням сутності соціоінженерного впливу як цілеспрямованої діяльності, заснованої на маніпулятивному використанні когнітивних упереджень, емоційних реакцій та поведінкових особливостей людини, у сучасній практиці протидії сформовано низку концептуальних підходів. Вони базуються на принципах зниження впливу людської помилки, підвищення обізнаності персоналу, впровадження процедур верифікації дій користувачів і формування культури інформаційної безпеки як елементу внутрішньої політики організації.

У комплексі ці підходи сприяють глибшому розумінню особливостей використання методів соціальної інженерії та створенню ефективних стратегій запобігання таким впливам. Це, у свою чергу, дозволяє вдосконалювати існуючі механізми протидії, враховуючи як їхні переваги, так і обмеження.

1.3 Оцінка впливу соціоінженерних атак на підхід інформаційної безпеки організацій

Сучасна практика управління інформаційною безпекою засвідчує зростання загроз, що походять від соціоінженерних атак, які дедалі частіше використовуються як основний або допоміжний інструмент кіберзлочинців. Відмінною рисою таких атак є їхня орієнтація не на технічні вразливості систем, а на психологічні особливості, емоційні реакції та поведінкові шаблони користувачів – переважно співробітників організацій. Це зумовлює високий

рівень ефективності соціальної інженерії в обхід формалізованих механізмів автентифікації, контролю доступу або виявлення вторгнень, оскільки сам користувач, діючи несвідомо або під тиском, надає зловмиснику необхідні повноваження.

Такий вектор атак має системний вплив на концепцію управління інформаційною безпекою в організації, помітно зменшуючи значущість переважно техніко-орієнтованого підходу. У цьому контексті загроза соціоінженерного впливу вимагає переосмислення ключових пріоритетів у межах системи менеджменту інформаційної безпеки, включаючи оновлення процедур ризик-менеджменту, підвищення ролі внутрішніх політик поведінки, а також розвиток інструментів безперервного навчання персоналу.

Відповідно до положень національного законодавства (зокрема, Закону України “Про інформацію” [16], “Про захист інформації в інформаційно-телекомунікаційних системах” [17]) та міжнародних стандартів, зокрема ISO/IEC 27001 [18] та ISO/IEC 27002 [19], організація зобов’язана забезпечити цілісну систему захисту таких об’єктів інформаційної безпеки:

- людських ресурсів – працівників, які мають доступ до конфіденційної, комерційної або службової інформації, з урахуванням рівня їх обізнаності, посадових повноважень та відповідальності;
- фізичних активів – приміщень, обладнання, носіїв інформації, транспортних засобів, доступ до яких може створити передумови для витоку даних або реалізації шахрайських дій;
- фінансових ресурсів – систем оплати, бухгалтерської документації, інструментів внутрішнього фінансового контролю;
- інформаційних систем і баз даних – програмно-апаратних комплексів, систем збереження та обробки даних, а також каналів обміну інформацією;
- засобів технічного та програмного захисту – механізмів контролю доступу, шифрування, виявлення атак, моніторингу аномальної активності тощо.

Соціоінженерні атаки здатні впливати на всі зазначені об’єкти як безпосередньо, так і опосередковано. Наприклад, компрометація працівника,

який має доступ до фінансової системи, може призвести до незаконного переказу коштів або зміни параметрів бухгалтерського обліку; вплив на особу, відповідальну за технічну підтримку, може спричинити відкриття критичних вразливостей або деактивацію механізмів захисту; та безліч інших подібних ризиків.

При цьому, відповідно до визначення, наведеного у стандарті ISO/IEC 27000:2018, інформаційний ризик розглядається як ймовірність реалізації загрози через використання вразливостей активів, що призводить до негативного впливу на досягнення цілей організації. Тобто такий ризик не обмежується виключно технічними аспектами, а включає також людський фактор, який охоплює як ненавмисні дії працівників, так і цілеспрямовану маніпуляцію ними у межах соціоінженерних атак [15].

Зважаючи на універсальність соціоінженерних атак, які можуть реалізовуватися як дистанційно (через електронну пошту, месенджери, телефонний зв’язок, соціальні мережі), так і під час особистого контакту з об’єктом впливу (що трапляється рідше через вищу ресурсомісткість та ризик ідентифікації, але не знижує рівня потенційної небезпеки), користувач опиняється під постійною загрозою впливу через численні канали комунікації, що у поєднанні зі складністю прогнозування його поведінки в умовах інформаційного тиску робить людський фактор однією з найменш контрольованих і найуразливіших ланок корпоративної безпеки.

Тому ефективне реагування на соціоінженерні атаки потребує врахування ризиків, пов’язаних з поведінковими аспектами персоналу, при плануванні захисту матеріальних та нематеріальних активів організації.

У рамках міжнародної практики класифікації інцидентів, зокрема у документах ENISA Reference Incident Classification Taxonomy, Europol EC3 та рекомендаціях CERT/CSIRT, соціоінженерним загрозам надається окрема категорія, що відображає їхню зростаючу вагу у загальному ландшафті кіберризиків. Особливої уваги заслуговує фішинг, який часто виконує роль початкового вектора складних цільових атак, зокрема APT (Advanced Persistent

Threat) [20], які поєднують соціоінженерні та технічні методи впливу, реалізуються у довгостроковій перспективі, мають високий ступінь таргетованості та підготовки. Такі атаки передбачають поетапне вивчення об’єкта, у тому числі ідентифікацію ключових співробітників, аналіз внутрішніх бізнес-процесів, технологічного стеку та особливостей корпоративної культури. Соціоінженерний компонент часто є критичним для отримання початкового доступу – наприклад, через надсилання електронного листа зі шкідливим вкладенням, підготовленого з урахуванням контексту діяльності конкретного співробітника [21].

В цьому контексті серйозну загрозу становить використання відкритих джерел інформації (OSINT), зокрема соціальних мереж та загальнодоступних публікацій, які дозволяють зловмиснику сформувати психологічний портрет цільової особи або колективу. Особливий інтерес становлять користувачі, які активно публікують особисті дані, проявляють емоційну відкритість, наївність або схильність до довіри. Саме ці характеристики широко експлуатуються при формуванні маніпулятивних сценаріїв соціоінженерного впливу.

Це вимагає від організацій впровадження політик інформаційної гігієни, навчання персоналу правилам безпечної поведінки у публічному цифровому середовищі та здійснення системного OSINT-моніторингу чутливої інформації про організацію та своїх співробітників.

Як вже було зазначено, соціальна інженерія як інструмент компрометації інформаційної безпеки ґрунтується на низці передумов, серед яких ключову роль відіграють когнітивні та психологічні особливості поведінки людини, недостатній рівень обізнаності персоналу щодо методів інформаційного захисту, а також відсутність підготовки до розпізнавання ознак маніпулятивного впливу.

Традиційні засоби забезпечення інформаційної безпеки, такі як антивірусне програмне забезпечення, міжмережеві екрани, системи виявлення та запобігання вторгненням (IDS/IPS), розроблені для протидії технічним загрозам і не враховують уразливості, пов’язані з людською поведінкою. Як наслідок, ефективна протидія соціоінженерним атакам потребує суттєвого розширення

концепції захисту – від вузькотехнічного підходу до багатовимірної моделі, що охоплює також організаційні та поведінкові аспекти.

У цьому контексті організації повинні впроваджувати додаткові заходи, спрямовані на підвищення стійкості до соціоінженерного впливу, серед яких:

- систематичне навчання персоналу та розвиток навичок інформаційної гігієни;
- моделювання та відпрацювання типових сценаріїв соціоінженерних атак;
- впровадження систем поведінкового моніторингу з метою виявлення нетипових дій користувачів;
- адаптація політик інформаційної безпеки з урахуванням динаміки соціоінженерних загроз, актуальних сценаріїв і реальних ризиків, пов’язаних із людським чинником.

Таким чином, захист від соціоінженерних загроз є можливим лише за умови застосування комплексного підходу, що інтегрує технічні, організаційні та поведінкові заходи безпеки. У сучасних умовах організації мають орієнтуватися не лише на удосконалення технічної інфраструктури, але й на формування культури інформаційної безпеки серед співробітників. Ігнорування людського чинника як вектора ризику нівелює ефективність навіть найсучасніших технічних рішень, перетворюючи інформаційну систему на об’єкт, уразливий до соціоінженерного впливу [22].

1.4 Дослідження чинників, що зумовлюють сприйнятливість працівників до маніпулятивного впливу

Успішність соціоінженерних атак значною мірою залежить від характеристик цільової аудиторії, які обумовлюють її сприйнятливість до маніпуляцій. Ці характеристики можна класифікувати на чотири основні групи: психологічні, соціально-професійні, організаційні та пов’язані з цифровою поведінкою (рис 1.4).

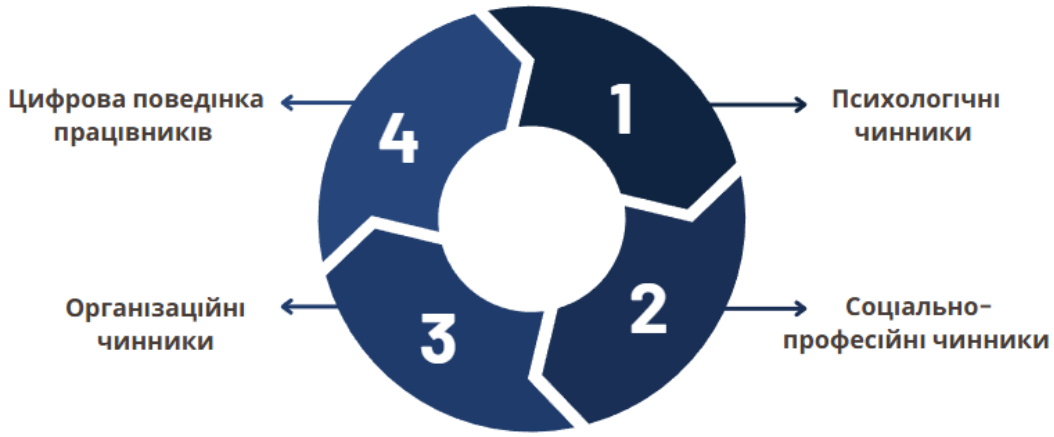

Рис. 1.4. Класифікація чинників, що зумовлюють сприйнятливість працівників до маніпулятивного впливу

Психологічні чинники є однією з найважливіших складових, що визначають індивідуальну вразливість працівника до соціоінженерних атак. До таких факторів відносяться когнітивні упередження, емоційна нестабільність, підвищена тривожність, потреба у схваленні, низький рівень критичного мислення та саморефлексії, а також надмірна готовність допомагати [24].

Когнітивні упередження, зокрема ефект авторитету, упередження підтвердження або ефект терміновості, часто знижують здатність людини раціонально аналізувати ситуацію та сприяють прийняттю імпульсивних рішень. Наприклад, атаки типу претексинг часто апелюють до авторитетних фігур або термінових ситуацій, стимулюючи людину виконати інструкції без перевірки їх достовірності [23].

Емоційна нестабільність і підвищена тривожність можуть призводити до неадекватного сприйняття загроз, унаслідок чого користувач або ігнорує небезпеку, або, навпаки, діє занадто швидко і необдумано. Люди з високою потребою у соціальному схваленні або зниженим рівнем саморефлексії схильні швидше відповідати на запити, що апелюють до їхньої емпатії чи обов'язку, навіть якщо запит виглядає підозрілим [25].

Користувачі з низьким рівнем цифрової обізнаності та критичного мислення виявляють значно вищий рівень довіри до електронних повідомлень, навіть у випадках очевидних ознак фішингу [27]. Саме тому підвищення усвідомленості

щодо особистісних психологічних ризиків є критичним завданням програм підготовки з кібербезпеки.

Таким чином, психологічні характеристики особистості безпосередньо впливають на вірогідність успішності соціоінженерної атаки. Тому ефективна протидія таким атакам має враховувати не лише технічну, але й психоемоційну підготовку співробітників, зокрема через тренінги, що розвивають критичне мислення, саморефлексію і стійкість до маніпуляцій.

Соціально-професійні чинники включають особливості віку, досвіду, професійної ролі та цифрових навичок працівника, які суттєво впливають на його вразливість до соціоінженерних впливів. Найбільш ризикованими вважаються групи співробітників із низьким рівнем досвіду в інформаційній безпеці, слабкими цифровими компетенціями, високим рівнем комунікаційної взаємодії або підвищеним емоційним навантаженням [24].

Так, дослідження показують, що працівники похилого або, навпаки, дуже молодого віку можуть бути менш обізнаними в актуальних методах соціоінженерії. Молодші співробітники, особливо ті, хто не проходив належної підготовки з інформаційної безпеки, схильні недооцінювати ризики, що асоціюються з онлайн-спілкуванням або робочими комунікаціями. Старші працівники можуть демонструвати довіру до традиційних форм звернень і не мати достатньої обізнаності про новітні загрози [25].

Особливо вразливою є категорія посад із високою комунікаційною інтенсивністю: HR-менеджери, офіс-менеджери, секретарі, служби технічної підтримки. Вони щоденно взаємодіють з великою кількістю людей і не завжди мають змогу ретельно перевіряти достовірність вхідних запитів, що робить їх легкою ціллю для атак на кшталт spear phishing чи voice phishing [26].

Додатковим чинником ризику є стан професійного вигорання чи високий рівень стресу. У таких умовах працівники можуть діяти за інерцією, не аналізуючи інформацію або пропускаючи ознаки маніпуляцій. Соціоінженери активно використовують цей аспект, створюючи ситуації терміновості або конфлікту, які вимагають негайної реакції [23].

Отже, професійне середовище й особливості трудових обов’язків можуть значно підвищувати сприйнятливість до соціоінженерних атак. Організаціям слід враховувати ці фактори при плануванні навчання з інформаційної безпеки, особливо для груп ризику [24].

Організаційне середовище відіграє критичну роль у формуванні кібергігієни працівників і їх здатності протистояти соціоінженерним атакам. Навіть при високій обізнаності окремих співробітників, слабкі або формальні внутрішні політики безпеки можуть створювати вразливе середовище [23].

Одним із ключових ризиків є відсутність системного навчання з інформаційної безпеки або його поверхнева реалізація. Якщо працівники не розуміють, як розпізнати фішинг, шахрайські дзвінки або підозрілі посилання, вони значно частіше стають жертвами атак [24].

Ще одним проблемним аспектом є непрозорість або відсутність чітких політик реагування на підозрілі дії. У ситуаціях, коли працівник не знає, куди і як повідомити про підозру, інцидент може залишитися непоміченим або не отримає належної уваги. Це особливо небезпечно при атаках, що використовують техніки “ланцюгового компрометування” через кілька співробітників [25].

Також важливу роль відіграє організаційна культура. У структурах, де не заохочується ініціатива чи критичне ставлення до нетипових дій керівництва, працівники можуть сліпо виконувати вказівки зловмисника, що видає себе за менеджера. Недостатній рівень довіри або страх покарання за помилки заважають співробітникам повідомляти про інциденти, що лише посилює проблему [28].

Варто також відзначити, що велике значення має підтримка ініціатив з боку вищого керівництва. Якщо менеджмент демонструє байдуже ставлення до питань інформаційної безпеки, це послаблює загальний пріоритет безпеки в очах працівників і знижує ефективність навчальних кампаній [24].

Загалом, організаційні чинники визначають фундамент, на якому будується поведінка співробітників. Чітко сформульовані політики, доступні канали

повідомлення про інциденти, культура довіри та підтримки – це базові складові ефективного захисту від соціоінженерних атак.

Цифрова поведінка працівників і обсяг персональних даних, які вони залишають у відкритому доступі, прямо впливають на рівень їх сприйнятливості до соціоінженерних атак. Соціальні інженери активно використовують відкриті джерела (OSINT) для збору інформації про потенційних жертв: профілі в соцмережах, коментарі, фото, участь у подіях тощо. Це дозволяє зловмисникам створювати персоналізовані сценарії атак – від цільового фішингу до емоційно забарвлених повідомлень [23].

Поширені цифрові звички, як-от використання однакових паролів для кількох облікових записів, відсутність двофакторної автентифікації або нехтування оновленнями програмного забезпечення, значно спрощують проникнення зловмисників у систему. Низький рівень технічної грамотності спричиняє небажання змінювати налаштування конфіденційності або безпеки в онлайн-сервісах [24].

Також велике значення має онлайн-комунікація. Працівники часто взаємодіють у відкритих каналах – наприклад, коментують професійні форуми або залишають публічні відгуки, що дає атакуючим додаткову інформацію про їхнє місце роботи, сферу діяльності, стиль спілкування. Такі цифрові сліди дозволяють створити ефективніші атаки соціальної інженерії, зокрема методи типу “water holing” або “pretexting” [25].

Небезпечна поведінка часто виникає через відсутність усвідомлення ризиків. Люди не завжди розуміють, що оприлюднена інформація про день народження, імена дітей або домашніх улюбленців може бути використана для генерації паролів або перевірочних запитань. Без відповідного навчання такі дії здаються нешкідливими, але фактично вони формують основу для соціоінженерного впливу [29].

Отже, сприйнятливість до соціоінженерних атак зумовлюється широким спектром чинників – від індивідуально-психологічних до організаційних і поведінкових. Вона формується не лише особистими рисами працівника

(наприклад, емоційною нестабільністю чи низьким рівнем критичного мислення), а й професійними умовами, внутрішньою культурою безпеки в організації, а також цифровими звичками людини у публічному просторі. Виявлення і систематизація цих характеристик дозволяє краще зрозуміти вразливі точки в системі людського фактора та формувати більш ефективні стратегії навчання й протидії. Важливо наголосити, що саме поєднання особистісної обізнаності та підтримки з боку організації створює стійкий бар'єр проти маніпулятивних впливів соціальних інженерів.

Висновки до розділу 1

У розділі розглянуто теоретичні засади протидії соціоінженерним загрозам в контексті забезпечення інформаційної безпеки організацій. Особливу увагу приділено систематизації підходів до розуміння сутності соціальної інженерії, що дозволило надати формалізоване визначення цього поняття як цілеспрямованого використання маніпулятивних технік для отримання несанкціонованого доступу до інформаційних активів через вплив на поведінку співробітників.

Проведена класифікація методів реалізації соціоінженерних атак охоплює як традиційні інструменти (фішинг, претекстинг), так і сучасні гібридні підходи, що поєднують технічні та психологічні засоби, зокрема із використанням штучного інтелекту, соціальних мереж та глибоких фейків. Це дозволяє глибше зрозуміти динаміку еволюції загроз та адаптивність методів атак.

На основі аналізу сучасних підходів, що застосовуються в організаціях для запобігання соціоінженерним атакам, виявлено, що більшість практик залишаються фрагментованими, орієнтованими переважно на формальне навчання або використання окремих технічних засобів. Водночас недостатньо уваги приділяється інтеграції навчальних, організаційних та поведінкових заходів у єдину систему управління інформаційною безпекою.

Оцінка впливу соціоінженерних атак на концепцію управління інформаційною безпекою організацій показала, що ці атаки не лише створюють ризики витоку інформації, а й підривають довіру до засобів безпеки, викликають порушення регламентів, впливають на репутацію та можуть мати юридичні наслідки. Узагальнення чинників сприйнятливості працівників до маніпулятивного впливу засвідчило, що критичними є не лише рівень обізнаності, а й організаційний контекст: культура безпеки, соціальна динаміка в колективі, управління стресовими станами та цифрова поведінка працівників.

Загалом, результати першого розділу сформували комплексне уявлення про соціальну інженерію як багатовимірну загрозу, що вимагає міждисциплінарного підходу до протидії. Теоретичне підґрунтя, викладене у розділі, забезпечує основу для розроблення методологічних і практичних рішень, які будуть розглянуті у наступних частинах дослідження.

Розділ 2 МЕТОДОЛОГІЧНІ ПІДХОДИ ДО РОЗРОБЛЕННЯ НАВЧАЛЬНИХ КАМПАНІЙ ІЗ ПІДВИЩЕННЯ РІВНЯ ОБІЗНАНОСТІ ПЕРСОНАЛУ

2.1 Визначення принципів та етапів побудови навчальної кампанії з протидії соціоінженерним загрозам

Ефективна протидія соціальній інженерії в межах організації значною мірою залежить не стільки від технічних засобів захисту, скільки від якісної та системної підготовки персоналу. Враховуючи, що соціальні інженери експлуатують людський чинник -довіру, неуважність, брак знань або досвіду – найефективнішим способом протидії є впровадження навчальної кампанії, яка охоплює всі рівні працівників і базується на науково обґрунтованих принципах [30].

Успіх кампаній з підвищення обізнаності персоналу як в контексті протидії соціоінженерним загрозам, так і в контексті забезпечення інформаційної безпеки в цілому, як правило, залежить від того, наскільки організація дотримується принципів побудови таких кампанії (рис. 2.1).

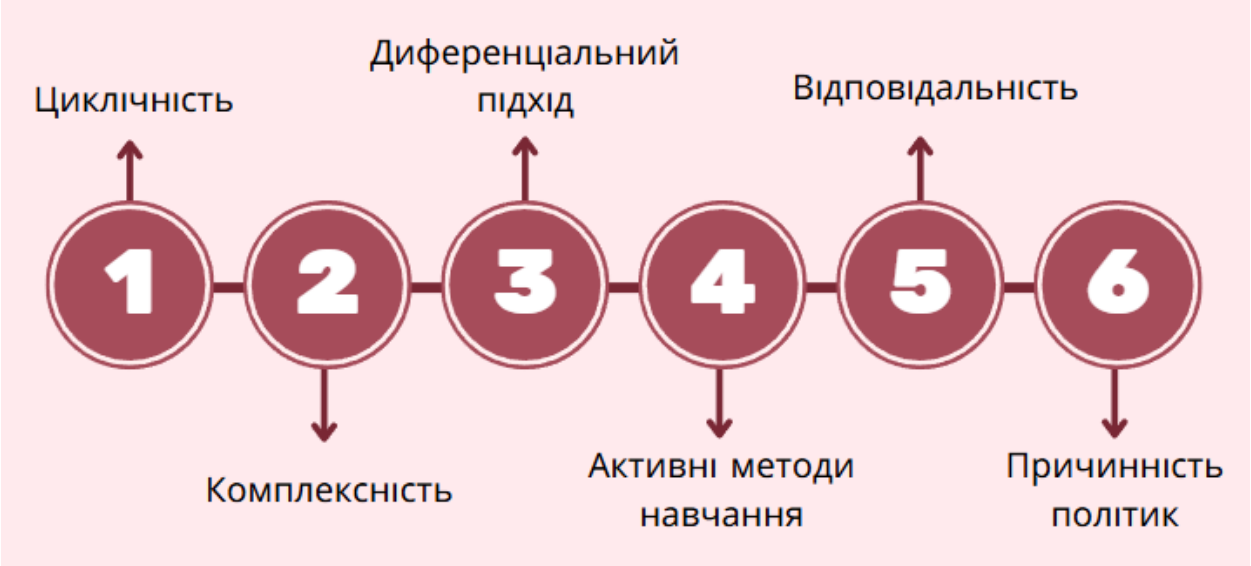

Рис. 2.1. Принципи побудови кампаній з підвищення обізнаності персоналу в контексті протидії соціоінженерним загрозам

Навчання має відбуватися регулярно та з чітко визначеною періодичністю. Оскільки разове інформування не забезпечує формування стійких навичок та свідомого ставлення до інформаційної безпеки. Кожен цикл повинен враховувати нові загрози, інциденти та рівень знань працівників [31].

Кампанія повинна охоплювати не лише ІТ-фахівців чи адміністративний персонал, а всіх працівників, які мають доступ до інформаційних систем або обробляють інформацію. Зокрема, потрібно передбачити окремі модулі для менеджерів, користувачів ПК, технічного персоналу, охоронців тощо [32].

Зміст навчання слід адаптувати відповідно до функціональних обов'язків працівників. Наприклад, менеджери повинні розуміти ризики прийняття рішень під тиском, а ІТ-фахівці – технічні аспекти атак, пов'язаних із соціальною інженерією [30].

Найефективнішим є не пасивне слухання лекцій, а залучення до практичних занять: рольові ігри, симуляції атак, розбір реальних кейсів. Це забезпечує глибше розуміння та розвиток поведінкових навичок.

Працівники мають усвідомлювати особисту відповідальність за дотримання вимог інформаційної безпеки, включаючи санкції за порушення (негативне підкріплення) та заохочення за дотримання політик (позитивне підкріплення).

Працівники краще дотримуються правил, коли розуміють, чому вони запроваджені. Тому навчання має включати обґрунтування вимог безпеки, що сприяє уникненню спроб їх обійти [31].

Для підвищення ефективності навчальних кампаній доцільно використовувати структурований підхід, що передбачає поетапну реалізацію усіх ключових елементів процесу. Такий підхід дозволяє систематизувати дії, уникнути організаційних помилок і забезпечити поступове досягнення навчальних цілей. На рисунку 2.2 наведено послідовність етапів реалізації навчальної кампанії з протидії соціальній інженерії, що базується на сучасних підходах до управління навчальними програмами.

Рис. 2.2. Етапи реалізації навчальної кампанії

Перший етап передбачає оцінку поточного стану інформаційної безпеки в організації, що досягається за допомогою аналізу рівня обізнаності персоналу та виявлення найбільш уразливих місць, пов’язаних із людським фактором. Для цього можуть застосовуватись такі інструменти, як соціальні аудити, опитування та фішингові тести [30].

Після проведення оцінки створюється робоча група, відповідальна за планування й реалізацію навчальної кампанії. До її складу повинні входити представники різних підрозділів – зокрема HR-відділу, IT-служби, служби безпеки та керівництва. Такий міждисциплінарний підхід дозволяє комплексно охопити проблематику соціоінженерних загроз і підвищити ефективність навчання [31].

Наступним кроком є розробка навчально-методичних матеріалів, адаптованих до особливостей окремих груп персоналу. Це можуть бути інформаційні буклети, презентації, відеоуроки, сценарії для рольових ігор, практичних тренінгів, а також тести для оцінювання рівня знань [31].

Після підготовки матеріалів здійснюється проведення теоретичного та практичного навчання. Воно може реалізовуватись у форматі лекцій, онлайн-

семінарів, відеокурсів і рольових ігор, що моделюють реальні сценарії атак, зокрема фішинг, вішинг або претекстинг. Особливу увагу слід приділити практичним елементам, які сприяють формуванню навичок розпізнавання загроз і реагування на них [31].

Завершальним етапом є контроль засвоєного матеріалу, тестування й внутрішні аудити. Зокрема, проводяться контрольовані «диверсії» у вигляді симульованих атак, що дозволяє оцінити готовність персоналу до реальних інцидентів і за потреби коригувати навчальну програму [30].

Кампанія не завершується після першого проходження. Важливо збирати відгуки, аналізувати помилки, оновлювати контент та повторювати навчання циклічно, з урахуванням нових викликів та змін у поведінці персоналу [31].

2.2 Обґрунтування вибору методів і форматів навчання залежно від категорії користувача

Зважаючи на динамічний розвиток соціоінженерних загроз, ефективна стратегія захисту інформаційного середовища неможлива без системного і цільового навчання персоналу. Для досягнення високої результативності така навчальна діяльність має бути побудована за принципами безперервності, адаптивності, практичної орієнтованості та врахування психологічних особливостей сприйняття інформації різними групами співробітників.

У сучасній практиці безпеки ключовим вважається диференційований підхід до навчання, коли зміст, формат та інтенсивність програм адаптуються під конкретні професійні ролі та пов’язані з ними ризики. Для цього здійснюється попередній аналіз функціональних обов’язків працівників, характерних для них векторів атак та рівня технічної грамотності [31, 33]. Класифікація цільових категорій працівників для проведення кампаній з підвищення обізнаності представлена на рисунку 2.3.

Рис. 2.3. Класифікація цільових категорій працівників для проведення навчальної кампанії

Менеджери є вразливою ланкою в контексті цільових атак, зокрема BEC, фішингу та інших соціоінженерних маніпуляцій, орієнтованих на прийняття поспішних рішень, авторизацію фінансових транзакцій чи передачу конфіденційних даних за фальшивими запитами. Для цієї групи найбільш ефективними є тренінги з елементами моделювання реальних ситуацій, кейс-стаді, відеосесії з розбором типових інцидентів, а також семінари з елементами аналізу психологічного впливу. Контент має включати розпізнавання соціального тиску (авторитету, терміновості), верифікацію запитів, політику підтвердження фінансових операцій і використання багатоканальних способів зв’язку для перевірки запитувача [30, 31].

IT-співробітники часто стикаються з соціальною інженерією, замаскованою під технічну взаємодію, наприклад – запити на зміну параметрів мережі, паролів, відновлення доступу до акаунтів або запити на технічну допомогу. Оскільки ця

група володіє високим рівнем технічних знань, навчання має мати більш глибокий рівень складності, орієнтований на практичні аспекти – симуляції інцидентів, розбір складних кейсів, технічні воркшопи, інтерактивне тестування. У фокусі має бути аналіз фальшивих запитів, захист від внутрішніх загроз, політика ідентифікації осіб, виявлення маніпулятивної поведінки в IT-комунікаціях, а також реагування на інциденти, пов'язані з соціальною інженерією [31, 33].

Користувачі ПК становлять основну частку персоналу і часто є мішенню для масових атак типу фішинг, спам, соціальні маніпуляції у соцмережах та месенджерах. Тому для них особливо актуальними є короткі інтерактивні навчальні модулі у форматі e-learning, гейміфіковані курси, періодичне тестування та симульовані фішингові атаки. У зміст навчання мають входити принципи розпізнавання шкідливих листів, перевірка посилань, правила поводження з вкладеннями, основи кібергігієни, безпечне використання соціальних мереж, базові правила автентифікації та зберігання паролів. Практичне спрямування цих тренінгів дозволяє зменшити ризик компрометації облікових записів і витоку інформації внаслідок людської помилки [32, 33].

Обслуговуючий персонал, який може не мати доступу до складної інформаційної інфраструктури, все ж перебуває в зоні ризику через фізичний доступ до приміщень, робочих місць та серверного обладнання. Зловмисники можуть намагатися ввести таких працівників в оману, видаючи себе за технічних спеціалістів, кур'єрів або зовнішніх постачальників, використовуючи правдоподібні вигадані ролі, щоб потрапити до захищених зон. Для такої категорії працівників доцільно проводити короткі інструктажі, демонстраційні відео, друковані пам'ятки з ілюстрованими прикладами. Їх слід навчати розпізнавати спроби обману, правильно реагувати на підозрілі дії, а також оперативно інформувати службу безпеки у випадках нетипових ситуацій [28, 30].

Адміністратори та їх асистенти виконують критично важливі функції, пов'язані з документообігом, доступом до чутливих даних, а також координацією комунікацій між відділами. Через це вони часто стають ціллю

соціоінженерних атак, спрямованих на викрадення внутрішньої інформації, підробку документів або перенаправлення фінансових ресурсів. Навчання для цієї категорії має акцентувати увагу на верифікації запитів, цифровій гігієні, політиках обробки інформації, правилах відповіді на дзвінки та листи, які містять нетипові вимоги. Ефективними форматами можуть бути сценарії і рольові ігри, що моделюють телефонні або email-атаки, короткі інструктажі з контрольними питаннями, а також регулярні розсилки з новими прикладами інцидентів [31].

Технічний персонал відповідає за налаштування та обслуговування телекомунікаційної інфраструктури, тому вразливі до атак, які використовують довіру до технічних спеціалістів. Навчання для них має включати розпізнавання ситуацій, коли хтось, прикриваючись їхньою роллю, намагається отримати доступ до мережевого обладнання або кабельних шаф. З огляду на специфіку роботи, оптимальними є практичні тренінги з фізичної безпеки, політики доступу та реагування на підозрілу поведінку у зоні своєї відповідальності. Важливою складовою є інструктажі щодо взаємодії з невідомими особами у технічних приміщеннях [33].

Охоронці займають ключову позицію у фізичному контролі доступу до об’єктів, однак часто залишаються поза увагою в рамках інформаційної безпеки. Для них доцільно розробити короткий, чітко структурований курс навчання, що охоплює тематику ідентифікації відвідувачів, виявлення підроблених перепусток, протоколів дій у випадку підозрілих ситуацій. Елементи навчання можуть включати відеоінструкції, стендові матеріали на постах охорони, інструкції з контактами відповідальних осіб у разі інциденту [31]. Підготовка охоронців до реагування на сценарії соціоінженерного впливу значно підвищує загальну стійкість організації до комплексних атак, які поєднують технічні й фізичні методи.

Систематизації заходів навчання для різних категорій персоналу доцільно наведено в таблиці 2.1.

Таблиця 2.1

Сегментація навчання з протидії соціальній інженерії за категоріями персоналу

Категорії персоналу	**Типові загрози**	**Формат навчання**	**Методи навчання**
Менеджери	BEC, фішинг, фальшиві запити	Тренінги, семінари, відеосесії	Аналіз соціального тиску, верифікація запитів, політика фінансових операцій
IT-співробітники	Фальшиві технічні запити, внутрішні загрози	Симуляції, воркшопи, інтерактивне тестування	Аналіз запитів, ідентифікація, реагування на інциденти
Користувачі ПК	Масовий фішинг, соцмережеві маніпуляції	E-learning, гейміфікація, тестування, симуляції	Розпізнавання фішингу, кібергігієна, автентифікація, соцмережі
Обслуговуючий персонал	Фізичне проникнення через обман	Інструктажі, відео, пам’ятки	Розпізнавання шахрайства, реакція, інформування служби безпеки
Адміністратори й асистенти	Витік інформації, підробка документів, фінансове шахрайство	Рольові ігри, інструктажі, розсилки	Верифікація запитів, цифрова гігієна, правила реагування на нетипові запити
Технічний персонал	Використання ролі техніка для доступу	Практичні тренінги, інструктажі	Виявлення шахраїв у тех. зонах, політика фізичного доступу
Охоронці	Обхід контролю доступу через соц. інженерію	Короткий курс, відео, стенди	Виявлення підробок, реагування, контакт із відповідальними особами

Загалом, незалежно від посади, всі працівники повинні бути обізнаними щодо базових принципів інформаційної безпеки. Обов’язковим має бути проведення вступного навчання при прийомі на роботу з підписанням політик про нерозголошення та ознайомленням з процедурою автентифікації, внутрішніми правилами доступу та поведінки у випадку інцидентів [33]. Також варто впровадити періодичні повторні інструктажі, тематичні семінари у разі появи нових векторів атак, онлайн-тестування знань, симуляції фішингових кампаній з подальшим аналізом результатів, що сприяє виявленню вразливих точок у поведінці персоналу [30, 32].

Ключовим інструментом підтримки обізнаності є наявність доступних регламентів, політик і пам’яток, де чітко прописано алгоритми дій у різних ситуаціях. Працівники повинні мати змогу у будь-який момент звернутися до цих матеріалів або до відповідальних фахівців з безпеки для консультації. Також важливо запровадити політику обмеження повноважень користувачів, що включає заборону використання знімних носіїв, доступу до потенційно небезпечних вебресурсів та повторне використання службових облікових даних у зовнішніх сервісах [33].

Таким чином, диференційоване навчання з урахуванням посадових обов’язків, рівня доступу до ресурсів та потенційних векторів атак дозволяє сформувати багаторівневу модель захисту організації від соціоінженерних впливів. Комбінація теоретичних знань, практичних навичок та постійного оновлення інформації є основою формування «людського файрволу» – першої лінії оборони у сфері кіберзахисту.

2.3 Систематизація освітніх технологій підвищення обізнаності: інтерактивні, адаптивні та гейміфіковані підходи

Підвищення рівня обізнаності працівників щодо кіберзагроз вимагає використання ефективних освітніх технологій, здатних забезпечити залучення, персоналізацію навчального процесу та мотивацію до засвоєння знань. Сучасна педагогіка, орієнтована на розвиток цифрових компетентностей, висуває вимогу до впровадження новітніх підходів, зокрема інтерактивних, адаптивних і гейміфікованих методів, які дозволяють активізувати когнітивні процеси слухачів, підвищити мотивацію до навчання та адаптувати матеріал до рівня підготовки кожного учасника.

Інтерактивні освітні технології (рис 2.4) є важливим елементом сучасного навчального процесу, орієнтованого на активне залучення учасників до здобуття знань, розвитку критичного мислення та формування практичних навичок у сфері інформаційної безпеки. У контексті підвищення обізнаності щодо

соціоінженерних загроз інтерактивні методи набувають особливої значущості, оскільки дозволяють не лише передати теоретичні знання, а й моделювати поведінку в умовах реальних або наближених до реальних кіберзагроз [34].

Рис. 2.4. Реалізація інтерактивних методів навчання

Сутність інтерактивного підходу полягає у взаємодії між усіма учасниками процесу: особа, відповідальна за проведення тренінгів з інформаційної безпеки не є єдиним джерелом знань, а модерує процес їх спільного створення, обговорення й осмислення. Такий підхід забезпечує глибше осмислення навчального матеріалу, стимулює когнітивну активність слухачів, підвищує їх мотивацію до участі в навчанні та сприяє формуванню відповідальної поведінки у цифровому середовищі [35].

Формат групової роботи та дискусій сприяє спільному аналізу проблем кіберзахисту, обговоренню різних точок зору щодо методів шахрайства, обміну досвідом і виробленню колективних стратегій реагування на інциденти. У ході

таких обговорень учасники не лише поглиблюють розуміння змісту навчального матеріалу, а й вчаться аргументувати свою думку, оцінювати ризики та прогнозувати наслідки потенційних атак [34].

Завдяки моделюванню типових ситуацій соціоінженерних атак, слухачі можуть відчути себе у ролі як зловмисників, так і потенційних жертв. Такий досвід сприяє не лише емоційному залученню до теми, а й формуванню рефлексивного мислення, самоспостереження, критичної оцінки власних дій. Наприклад, рольова гра з інсценуванням фішингової атаки допомагає виявити слабкі місця в поведінці користувачів та закріпити правильні шаблони реагування [35].

Метод аналізу кейсів передбачає детальний розгляд реальних або змодельованих випадків порушення інформаційної безпеки внаслідок соціоінженерного впливу. Аналіз таких кейсів дозволяє слухачам зрозуміти логіку зловмисника, визначити помилки користувачів, оцінити наслідки недотримання політик безпеки та розробити превентивні заходи. Крім того, кейси можуть бути адаптовані до професійної діяльності слухачів, що підвищує релевантність і ефективність навчання [34].

Інтерактивні вправи з виявлення підозрілих електронних листів, повідомлень у месенджерах чи телефонних дзвінків передбачають змодельовані приклади атак з помилками або ознаками шахрайства, які слухачі повинні виявити. Така діяльність формує навички аналітичного мислення, розпізнавання патернів атаки та впевненість у прийнятті рішень у складних ситуаціях.

Використання цифрових платформ для взаємодії (наприклад, Kahoot, Mentimeter, Quizizz) дає змогу проводити миттєве оцінювання знань, створювати інтерактивні опитування, проводити ігрові тести та візуалізувати результати у реальному часі. Такі інструменти є ефективними особливо в дистанційному або змішаному форматі навчання, оскільки підтримують високу динаміку заняття та залученість слухачів [35].

Однією з важливих переваг інтерактивних методів є можливість реалізації принципів андрагогіки – концепції навчання дорослих, яка враховує потреби,

мотивації, досвід та самоорганізацію слухачів. У контексті кампаній з підвищення обізнаності щодо інформаційної безпеки це означає, що навчальний процес має бути практикоорієнтованим, змістовно насиченим і побудованим таким чином, щоб слухачі могли одразу застосовувати здобуті знання у власній професійній діяльності [34].

Крім того, інтерактивний підхід сприяє емоційній залученості, що є важливою складовою у формуванні довготривалих знань. На відміну від традиційного лекційного підходу, інтерактивне навчання викликає внутрішню мотивацію, оскільки слухачі відчувають власну значущість у процесі побудови знань, беруть на себе відповідальність за результати і відчувають безпосередній зв’язок між навчальним змістом та власними професійними завданнями [31].

Загалом, інтерактивні підходи дозволяють досягти високого рівня когнітивної, емоційної та поведінкової залученості слухачів, що значно підвищує ефективність навчальних програм з кібербезпеки. Вони забезпечують багатовекторний розвиток: від формування базових знань до опанування складних моделей поведінки у разі виявлення соціоінженерних атак. Це робить їх незамінним компонентом навчальних кампаній, орієнтованих на стійке підвищення рівня обізнаності працівників у сфері інформаційної безпеки [33, 35].

Адаптивні освітні технології – це підходи до навчання, в яких зміст, складність і форма подачі матеріалу змінюються відповідно до індивідуальних особливостей, потреб і поточного рівня знань конкретного користувача. Їхня мета – створити умови для персоналізованого навчального досвіду, що забезпечує ефективніше засвоєння матеріалу, вищу залученість слухача та оптимізацію освітнього процесу. У сфері формування обізнаності з питань кібербезпеки, зокрема щодо соціоінженерних загроз, адаптивні технології сприяють створенню диференційованих програм, які враховують реальні знання, поведінкові шаблони та професійний контекст користувачів [36].

Адаптивні підходи реалізуються на основі аналізу даних про навчальну діяльність слухача, зокрема результатів тестування, поведінкових індикаторів

під час проходження тренінгів, тривалості виконання завдань, а також рівня помилок. Ці дані використовуються для формування персоналізованої траєкторії навчання, яка постійно коригується у відповідь на зміни в результатах і діях користувача. Таким чином, забезпечується індивідуалізація навчання, що особливо важливо в умовах корпоративних програм з підвищення обізнаності, де аудиторія є різнорідною за знаннями, досвідом і функціональними обов'язками [35].

Адаптивне навчання з кібербезпеки ефективніше, ніж стандартизоване, оскільки воно забезпечує контекстну релевантність матеріалу: працівник отримує лише ті знання і навички, які необхідні для його ролі в організації (наприклад, відрізняється зміст для адміністратора мережі й для офісного менеджера). Завдяки цьому досягається підвищена мотивація до навчання, оскільки слухачі бачать безпосередню практичну користь від отриманої інформації [36].

Одним із прикладів реалізації адаптивного підходу є використання інтелектуальних навчальних платформ, які мають вбудовані алгоритми адаптації контенту. Ці платформи аналізують відповіді слухача, визначають слабкі місця в знаннях і автоматично пропонують додаткові пояснення, вправи чи приклади саме з проблемної теми. Наприклад, у разі помилкових відповідей на питання, пов'язані з розпізнаванням фішингових повідомлень, система може повторно запропонувати модуль із відео-інструкцією, інтерактивною демонстрацією чи коротким мікроуроком на цю тему [35].

Ще однією перевагою адаптивного підходу є можливість поетапної складності: система надає завдання, які відповідають рівню користувача, і поступово ускладнює їх. Такий формат дозволяє уникнути перевантаження, зберігаючи баланс між викликом і підтримкою – ключовий принцип ефективного навчання дорослих. Особливо актуальним це є у сфері кібербезпеки, де надмірна складність матеріалу може призвести до зниження зацікавленості, а надмірна простота – до відчуття марності навчання [36].

Адаптивні системи також можуть враховувати психологічні аспекти навчання, наприклад, темп роботи, час найвищої продуктивності, схильність до візуального чи текстового сприйняття інформації. Наприклад, користувачам, які краще засвоюють матеріал через візуальні засоби, можуть переважно надаватися відео-уроки або інфографіка, тоді як іншим – текстові пояснення або симуляції. Це створює умови для оптимального залучення когнітивних ресурсів слухача [35].

У контексті підвищення обізнаності щодо соціоінженерних загроз адаптивні технології дозволяють не тільки підвищити ефективність навчання, а й сформувати довготривалу зміну поведінкових моделей. Наприклад, система може реагувати на багаторазове повторення критичних помилок і активувати модулі з поглибленим поясненням ризиків, а також пропонувати ситуаційні задачі, що моделюють подібні загрози. Такі дії не просто фіксують знання, а допомагають виробити стійкі навички реагування у випадку соціоінженерної атаки [36].

Таким чином, адаптивні підходи забезпечують гнучкість, індивідуалізацію та динамічність навчального процесу, що є критично важливим у сфері кібербезпеки. Вони дозволяють точно відповідати освітнім потребам працівників, враховувати їх попередній досвід та специфіку професійної діяльності, а також підвищувати ефективність навчальних кампаній шляхом цілеспрямованої роботи з конкретними недоліками в знаннях і навичках [35, 36].

Гейміфікація – це використання елементів і механік ігор у навчальному процесі для підвищення мотивації, залучення слухачів та покращення результатів навчання. Цей підхід базується на принципах ігрового дизайну, таких як баланс між викликами та нагородами, змагання, досягнення та інтерактивні задачі, які стимулюють інтерес до навчання і забезпечують активну участь. У контексті підвищення обізнаності про соціоінженерні загрози, гейміфікація дозволяє створювати динамічні, захоплюючі навчальні середовища, що мотивують співробітників організацій до поглибленого освоєння матеріалу та формування стійких навичок безпеки.

Використання гейміфікації у навчальних кампаніях з кібербезпеки має кілька важливих переваг. Одна з них полягає в тому, що гейміфіковані тренінги дозволяють учасникам безпечно пережити ситуації, що можуть виникнути в реальному житті, такі як фішинг-атаки або спроби маніпуляцій через соціальні мережі. Задачі та сценарії, що моделюють реальні загрози, надають можливість спробувати різні варіанти реакцій без ризику для організації чи користувачів. Це не тільки дозволяє отримати досвід в умовах, наближених до реальних, але й сприяє розвитку критичного мислення, необхідного для виявлення загроз у реальному світі [37].

Одним із основних принципів гейміфікації є використання досягнень і нагород, що стимулює користувачів активно долати виклики та досягати поставлених цілей. Наприклад, у програмі навчання з кібербезпеки співробітники можуть отримувати бали, медалі або сертифікати за успішне виконання завдань, таких як виявлення фішингових листів чи правильне реагування на загрози. Така система стимулів не лише мотивує користувачів, але й забезпечує їх підтримку у процесі навчання, дозволяючи зберігати зацікавленість протягом тривалого часу.

Системи балів та рейтингів є потужними інструментами у гейміфікації, оскільки дозволяють створювати змагальну атмосферу, де учасники можуть порівнювати свої досягнення з іншими. Важливою характеристикою є соціальна складова, коли співробітники змагаються за лідерство в рейтингу або досягнення певних цілей у команді. Це створює елемент колективної взаємодії, що допомагає не лише підвищити інтерес до навчання, але й зміцнити корпоративну культуру безпеки, де співробітники активно обмінюються знаннями та допомагають один одному [35].

Гейміфікація також дозволяє інтегрувати сценарії з реальними загрозами, що дає можливість співробітникам на практиці навчитися розпізнавати фішинг, соціальне маніпулювання, інсайдерські загрози та інші типи соціоінженерних атак. Такий підхід є особливо корисним для розвитку навичок швидкого реагування у стресових ситуаціях, адже за допомогою гейміфікації можна

змоделювати нестандартні ситуації, з якими користувач може зіткнутися в реальному світі [37].

Крім того, в гейміфікації важливим аспектом є персоналізація ігор під індивідуальні потреби користувачів. Зміст завдань, рівень складності та інтерфейс можуть адаптуватися до інтересів та рівня знань кожного співробітника, що дозволяє уникнути ситуацій перевантаження або недооцінки здібностей користувача. Це забезпечує більш ефективне навчання, яке інтегрується у реальні процеси роботи співробітника, а також стимулює його до подальшого розвитку та вдосконалення знань у галузі кібербезпеки [35].

Принципи ігрових механік, що застосовуються в таких програмах, допомагають створити відчуття прогресу та мотивації. У процесі виконання завдань користувачі можуть відслідковувати свої досягнення, бачити, які навички вони вже освоїли, а які ще потребують вдосконалення. Це дає змогу не лише оцінювати свої власні успіхи, але й працювати над слабкими місцями, забезпечуючи постійний процес самовдосконалення [37].

Гейміфікація навчання з кібербезпеки також забезпечує важливу функцію підвищення запам’ятовуваності інформації. Ігрові завдання часто вимагають від користувачів багаторазових повторів певних дій або прийняття рішень у змінних умовах, що сприяє кращому запам'ятовуванню та засвоєнню знань. У той же час, завдяки елементам змагання та досягнень, співробітники мають додаткову мотивацію для повторення матеріалу та вдосконалення своїх навичок [35].

Таким чином, гейміфіковані підходи стають потужним інструментом підвищення обізнаності з питань кібербезпеки, особливо в аспекті соціоінженерних загроз. Вони дозволяють зробити навчання цікавим, інтерактивним і ефективним, сприяючи формуванню у співробітників необхідних навичок для захисту від сучасних загроз в кіберпросторі. Гейміфікація підвищує рівень залученості та мотивації, покращує результативність навчання та створює умови для глибшого і довготривалого засвоєння матеріалу [35, 36].

Інтерактивне навчання формує динамічне освітнє середовище, де знання здобуваються шляхом діалогу, обговорень і практичної діяльності, що дозволяє глибше опрацювати інформацію та застосувати її у реальному контексті [34]. У свою чергу, адаптивні освітні системи забезпечують індивідуалізацію навчального процесу, підлаштовуючи зміст і складність матеріалу під особливості сприйняття конкретного користувача, що підвищує ефективність засвоєння [36]. Гейміфіковані підходи, базуючись на принципах ігрового дизайну, стимулюють інтерес до навчання, сприяють емоційному залученню та створюють додаткову мотивацію до проходження навчального контенту [33]. Систематизація вказаних технологій дозволяє розробити цілісну модель підвищення обізнаності, яка враховує не лише технічні аспекти подачі матеріалу, а й психологічні чинники впливу на поведінку користувачів у сфері інформаційної безпеки [35]. Таким чином, об’єднання інтерактивних, адаптивних і гейміфікованих освітніх практик є перспективним напрямом для формування стійкої культури інформаційної безпеки в організаціях (табл. 2.2).

Таблиця 2.2

Характеристика освітніх технологій підвищення обізнаності

Назва підходу	**Характеристика**	**Засоби реалізації**
Інтерактивний	Активна взаємодія між учасниками та тренером, формування знань через обговорення. Розвиває мислення, мотивацію та поведінкові навички	Дискусії, симуляційні тренінги, групова робота
Адаптивний	Індивідуалізація освітнього контенту відповідно до рівня знань та потреб користувача	Персоналізовані e-learning платформи, алгоритми адаптації
Гейміфікований	Інтеграція елементів ігрового дизайну у навчальне середовище. Підвищує мотивацію, залучення та закріплення знань.	Рейтинги, бали, віртуальні нагороди, сюжетні квести

2.4 Встановлення показників ефективності та методів оцінювання результатів навчання

Ефективність освітніх кампаній, спрямованих на підвищення рівня обізнаності у сфері інформаційної безпеки, визначається не лише якістю наданого матеріалу, а й здатністю впливати на поведінкові установки та практичні навички користувачів. У цьому контексті важливо встановити обґрунтовані та вимірювані показники результативності, що дозволяють об'єктивно оцінити досягнення навчальних цілей. Оцінювання результатів навчання слугує не лише засобом контролю, а й інструментом для постійного вдосконалення змісту та методів подання інформації, забезпечуючи адаптацію освітніх програм до реальних потреб аудиторії.

Ключові показники ефективності (Key Performance Indicators, KPI) становлять основу для якісної оцінки досягнення цілей у межах освітніх програм, зокрема спрямованих на підвищення обізнаності співробітників щодо кіберзагроз. Вони відіграють критичну роль у вимірюванні ефективності впроваджених ініціатив, дозволяючи об'єктивно відстежувати прогрес, аналізувати слабкі місця та ухвалювати стратегічно обґрунтовані рішення щодо подальшого розвитку навчальних заходів.

Попри те, що концепція вимірювання продуктивності бере свій початок ще з давніх часів, лише в другій половині XX століття термін "KPI" набув поширення в управлінській практиці. Становлення цієї концепції стало відповіддю на ускладнення бізнес-процесів і зростання потреби в систематичному контролі досягнення стратегічних цілей. Первинно KPI застосовувалися у сфері фінансів, однак згодом сфера їх використання розширилася до управління людськими ресурсами, маркетингу, інформаційних технологій та освітніх систем [38].

У контексті корпоративного навчання, особливо у сфері кібербезпеки, KPI виконують ряд важливих функцій, що дозволяють комплексно оцінювати результативність кампаній з підвищення обізнаності (Рис. 2.3) [38]:

Рис. 2.5. Роль KPI у контексті оцінки результативності програм з підвищення обізнаності

KPI дозволяють кількісно та якісно оцінювати поступ у реалізації навчальних цілей. Це може охоплювати відсоток співробітників, які пройшли обов'язкові курси, показники завершення навчальних модулів, покращення результатів тестування або рівень зміни поведінки користувачів після завершення навчання. Систематичне вимірювання дає змогу не лише фіксувати факт завершення навчання, а й оцінити глибину засвоєння матеріалу та здатність застосовувати знання на практиці [39].

Ключові показники ефективності сприяють узгодженню навчальних ініціатив з довгостроковими стратегіями організації в галузі інформаційної безпеки. Визначення релевантних KPI дозволяє структурувати навчальний процес відповідно до основних ризиків, загроз та нормативних вимог, що стоять перед організацією. Таким чином, ресурси спрямовуються на ті напрями, які мають найбільший вплив на загальний рівень кіберстійкості.

Аналіз динаміки KPI надає змогу виявляти неефективні компоненти навчального процесу. Наприклад, якщо показники завершення курсу є високими,

але рівень правильних відповідей у посттестуванні залишається низьким – це свідчить про необхідність перегляду змісту або форми подачі матеріалу. Таким чином, KPI стають інструментом безперервного вдосконалення якості навчального контенту та методів.

Встановлення чітких, прозорих та досяжних показників сприяє формуванню внутрішньої мотивації співробітників. Коли працівники усвідомлюють, як саме їхня участь у навчанні відображається у загальній системі оцінювання ефективності організації, вони демонструють вищий рівень зацікавленості та відповідальності. Застосування KPI також дозволяє використовувати механізми гейміфікації (рейтинги, нагороди тощо), що додатково стимулює участь [40].

Однією з ключових переваг використання KPI є їх здатність виявляти потребу у коригуванні навчального процесу відповідно до динаміки зовнішнього середовища. Зміни у законодавстві, зростання нових кіберзагроз або появи нових технологічних інструментів вимагають оперативного реагування. KPI дозволяють зафіксувати невідповідність між наявними компетенціями співробітників та новими викликами, що виникають.

Запровадження KPI сприяє підвищенню якості управління освітніми процесами. Вони забезпечують керівництво релевантною інформацією для прийняття управлінських рішень, дозволяють планувати розвиток навчальних програм, визначати пріоритети інвестування ресурсів та впроваджувати заходи з підвищення загальної ефективності. KPI стають основою для формування циклу постійного вдосконалення освітніх кампаній [41].

Використання KPI сприяє підвищенню прозорості процесів навчання в організації. Завдяки чітко встановленим критеріям успішності кожен співробітник має змогу розуміти свої цілі, очікування щодо результатів та оцінку власного внеску. Це формує атмосферу довіри, відкритості та відповідальності, що є критично важливим для досягнення високого рівня кіберобізнаності в колективі [38].

Таким чином, ключові показники ефективності є багатофункціональним інструментом, що не лише дозволяє оцінити результативність навчальних

кампаній, а й активно впливає на якість їх реалізації, мотивацію учасників та стратегію управління. У межах програм з підвищення обізнаності у сфері кібербезпеки KPI виступають незамінною складовою системного підходу до формування стійкої інформаційної культури.

Підвищення рівня кіберобізнаності персоналу як складова частина його розвитку передбачає цілеспрямоване вдосконалення знань, навичок і поведінкових моделей, що сприяють ефективній протидії кіберзагрозам. Сутність цього процесу полягає у створенні системи заходів, спрямованих на формування необхідних компетентностей і усунення бар'єрів, які можуть заважати ефективному виконанню працівниками своїх обов'язків у сфері кібербезпеки. Таким чином, організація має забезпечити не лише змістовне наповнення навчальних кампаній, а й відповідні умови для засвоєння знань, підтримку мотивації, урахування індивідуального рівня підготовки та особливостей персоналу [42].

Комплексний характер оцінювання ефективності навчальних кампаній полягає у забезпеченні відповідності обраних методів навчання поточній ситуації в організації та її цілям. Через динамічні зміни в зовнішньому середовищі, які складно передбачити, оцінювання результативності навчання повинне враховувати можливість втрати актуальності отриманих знань у разі зміни загальної стратегії організації. Водночас, ефективність навчання не завжди є очевидною одразу після його завершення, оскільки цінність сформованих навичок може проявитися лише в умовах реальної загрози.

Оскільки навчання персоналу в межах кампаній з кіберобізнаності має бути орієнтоване на індивіда, важливо адаптувати як зміст, так і форму навчання під конкретні потреби працівника з урахуванням загальних цілей безпеки. Це передбачає індивідуалізований підхід до оцінювання прогресу, який ґрунтується на порівнянні рівня знань до та після навчання [42]. Проблема полягає в тому, що навіть при ефективному навчанні, оцінити його вплив складно через часову віддаленість використання знань на практиці. Отже, кількісні показники, як-от

результати тестування, не завжди відображають реальну ефективність навчання, оскільки вони не враховують довгостроковий вплив.

Контекст впливу зовнішнього середовища також відіграє важливу роль: саме в ньому набуті знання і навички набувають реальної цінності. В умовах постійних змін у сфері кіберзагроз передбачити ці фактори важко, тому ефективність навчальних кампаній має імовірнісний характер.

Оцінювання результативності після завершення навчального циклу часто є недостатнім, оскільки воно не дозволяє своєчасно внести зміни до програми. Враховуючи, що працівники по-різному реагують на однакові освітні заходи, ефективнішим є коригування кампаній у процесі їх реалізації. Однак поділ навчального процесу на етапи для проміжного оцінювання можливий не завжди, особливо якщо кампанія є короткотривалою або масовою [42].

Для аналізу ефективності навчальних кампаній можуть використовуватись загальні підходи до оцінки управління персоналом, зокрема: співвідношення результатів і витрат, ступінь досягнення цілей, наближення до бажаного стану системи, баланс інтересів зацікавлених сторін, а також Парето-ефективність [43]. Оскільки кампанії з кіберобізнаності складаються з багатьох елементів – інформаційних матеріалів, тренінгів, ігрових симуляцій тощо – доцільним є вивчення впливу кожного з компонентів окремо.

Найпоширенішим способом оцінювання ефективності навчання є визначення рівня досягнення поставлених цілей. Якщо цілі чітко сформульовані на початку кампанії, то можливо оцінити, чи відповідають фактичні результати очікуваним [44]. Для цього широко використовується модель Д. Кіркпатрика, яка охоплює чотири рівні:

Рівень 1. Оцінка реакції – суб'єктивна оцінка рівня задоволеності учасників процесом та результатами навчання.

Рівень 2. Оцінка засвоєння – контроль рівня знань, умінь, навичок, отриманого досвіду, набуття яких було передбачено програмою навчання.

Рівень 3. Оцінка поведінки – частота та тривалість застосування нових форм трудової поведінки в організаційній діяльності.

Рівень 4. Оцінка результатів – порівняння досягнутих організацією результатів зі здійсненими витратами на навчання персоналу [44].

Модифікацією цієї моделі є підхід Д. Філіпса, який доповнив її п’ятим рівнем – оцінкою повернення інвестицій (ROI). Хоча він дає змогу фінансово оцінити ефективність навчання, усе ж він не дозволяє оцінити вплив окремих інструментів (наприклад, фішингових симуляцій або інтерактивних відео) [45]. Тому в практиці часто застосовують часткові показники, як-от зменшення кількості інцидентів, що виникли через людський фактор, або підвищення точності розпізнавання фішингових листів [42].

В умовах великих організацій доцільним є застосування методів типу «центрів оцінки та розвитку». У межах таких центрів працівники проходять серію вправ, що імітують реальні кіберінциденти, з метою оцінювання їхньої поведінки, навичок реагування та здатності до аналізу ситуацій. Експерти оцінюють дії працівників за наперед визначеними критеріями, а зворотний зв’язок виконує не лише інформативну, а й мотиваційну функцію, сприяючи подальшому самонавчанню [42].

Ще одним з ефективних методів оцінювання рівня обізнаності працівників щодо соціоінженерних загроз є проведення тестів на проникнення (пентест) з елементами соціальної інженерії. Таке тестування передбачає імітацію дій зловмисника з метою перевірки вразливостей у системах інформаційної безпеки, а також поведінки співробітників у ситуаціях, наближених до реальних кібератак. Під час проведення подібних оцінювань спеціалісти (пентестери) намагаються отримати доступ до конфіденційної інформації або порушити роботу системи, що дозволяє не лише виявити технічні слабкі місця, а й перевірити готовність персоналу протистояти атакам, зокрема фішинговим [43].

Залежно від рівня обізнаності працівників про тестування, розрізняють відкриті й приховані перевірки. Приховане пентестування є особливо цінним для оцінки реальних дій працівників в умовах несподіваних інцидентів, а також для перевірки ефективності процедур взаємодії між підрозділами безпеки. Відкрите ж тестування, що проводиться за участі технічного персоналу, дозволяє не тільки

уникнути потенційних ризиків для критичних систем, а й виступає додатковим навчальним етапом, під час якого працівники знайомляться з методами атак та алгоритмами реагування [47].

Висновки до розділу 2

У розділі розглянуто методичні підходи до розробки навчальних кампаній, спрямованих на підвищення рівня обізнаності персоналу щодо соціоінженерних загроз. Визначено, що формування сталої інформаційної культури є ключовою умовою ефективної протидії маніпулятивним впливам у сфері кібербезпеки, а системні освітні ініціативи мають бути інтегровані у загальну стратегію управління інформаційною безпекою.

У межах дослідження окреслено принципи побудови навчальних кампаній, які передбачають поетапне впровадження: від визначення цільової аудиторії до оцінювання досягнутих результатів. Здійснено аналіз доцільності застосування різних форматів і методів навчання залежно від типу користувачів – адміністративного, технічного чи загального персоналу. Обґрунтовано, що адаптація змісту до особливостей цільової групи істотно підвищує релевантність і засвоюваність матеріалу.

Окрему увагу приділено інноваційним освітнім технологіям, зокрема інтерактивним, адаптивним та гейміфікованим підходам. Проаналізовано їх потенціал у підвищенні мотивації, залученості та ефективності навчального процесу, що є особливо важливим у контексті формування стійких навичок розпізнавання соціоінженерних впливів.

У результаті систематизації методичних підходів підкреслено необхідність впровадження чітких показників ефективності навчальних кампаній. Визначення метрик охоплення, результатів тестування, показників поведінкових змін дозволяє здійснювати об’єктивний моніторинг динаміки покращення рівня обізнаності та своєчасно коригувати освітню стратегію.

Загалом, результати розділу демонструють, що підвищення рівня кіберобізнаності персоналу вимагає поєднання сучасних освітніх інструментів, глибокого розуміння специфіки цільових груп і наявності системи оцінювання результативності. Такий підхід формує основу для створення цілісної та адаптивної системи навчання, здатної забезпечити стійкість до соціоінженерних атак у довгостроковій перспективі.

Розділ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАЛЬНОЇ КАМПАНІЇ З ПРОТИДІЇ СОЦІОІНЖЕНЕРНИМ ЗАГРОЗАМ

3.1 Аналіз вихідного рівня обізнаності персоналу щодо соціоінженерних загроз

Ефективність будь-якої навчальної кампанії з підвищення обізнаності про соціоінженерні загрози значною мірою залежить від достовірної оцінки початкового рівня знань, умінь і навичок працівників у зазначеній сфері. На цьому етапі важливо ідентифікувати не лише загальний рівень обізнаності, а й конкретні проблемні аспекти, які потребують особливої уваги під час подальшого навчання.

У межах практичної реалізації дослідження було проведено вхідне тестування співробітників компанії, що стала базою практики. Тест складався з питань різного рівня складності та дозволив визначити, наскільки персонал обізнаний щодо методів і прийомів соціоінженерних атак, зокрема фішингу, вішингу, бейтінгу, а також механізмів їх розпізнавання.

Зібрані результати стали основою для побудови інформативних діаграм та подальшого формування індивідуальних і групових рекомендацій щодо навчання. Таким чином, аналіз вихідного рівня є вихідною точкою у процесі впровадження ефективної освітньої програми в сфері кібергігієни та протидії соціоінженерним загрозам.

Для визначення початкового рівня обізнаності працівників щодо соціоінженерних загроз було розроблено анкету-тест, яка містила 6 запитань із кількома варіантами відповідей. Кожне питання стосувалося конкретних аспектів соціальної інженерії, таких як: розпізнавання фішингових повідомлень, методи вішингу, фізичні атаки, атаки через підкинуті пристрої тощо.

Питання мали різний рівень складності та дозволяли оцінити як базові знання, так і глибше розуміння теми. Варіанти відповідей були розраховані на градацію правильності, що дозволило гнучко оцінювати обізнаність (табл. 3.1).

Таблиця 3.1

Шкала оцінювання відповідей у вхідному тестуванні обізнаності щодо соціоінженерних загроз

Оцінка	**Критерій**
1	Повністю правильна відповідь
0,75	Майже правильна відповідь
0,5	Частково правильна відповідь
0,25	Мінімальні ознаки розуміння
0	Неправильна або небезпечна відповідь

З метою виявлення рівня обізнаності персоналу щодо основних соціоінженерних атак було проведено анонімне опитування серед співробітників компанії (загалом 18 осіб), в онлайн-форматі (рис 3.1).

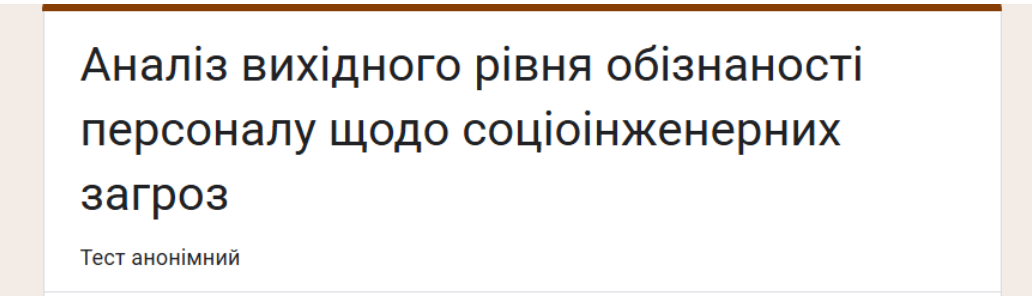

Рис 3.1. Тестування за допомогою Google Forms

Далі наведено аналіз отриманих результатів за кожним із запитань (рис. 3.2-3.7).

Питання 1. Що ви зробите, якщо отримаєте листа від служби безпеки з проханням терміново підтвердити свої облікові дані?

- відкрию посилання та введу дані, щоб уникнути блокування (0);
- видалю листа і повідомлю IT-відділ (1);
- відповім на лист і уточню деталі (0,25);
- зателефоную до банку за офіційним номером для перевірки (0,75);
- перевірю адресу відправника і лише тоді вирішу (0,5).

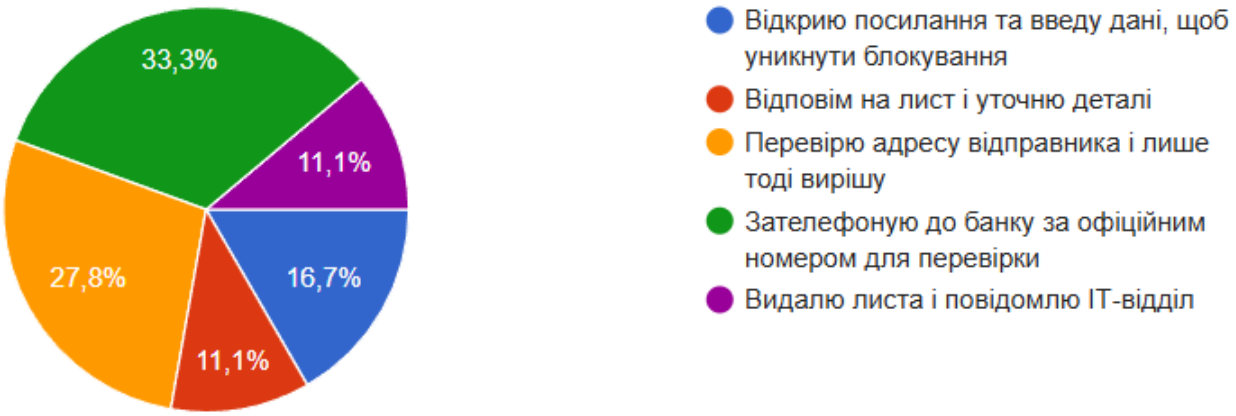

Рис 3.2. Результати відповідей на питання 1

Згідно з отриманими даними, найбільша частка опитаних (33%) обрала відповідь, яка оцінюється у 0.75 бала, що свідчить про часткову поінформованість респондентів щодо необхідності перевірки достовірності листа шляхом прямого звернення до банку. Проте повністю правильну відповідь, яка включає не лише уникнення взаємодії з потенційно шкідливим листом, а й повідомлення IT-відділу, обрало лише 11% співробітників.

Водночас 28% респондентів обрали відповідь, яка демонструє лише базовий рівень настороженості (0.5 бала), зокрема обмеженням перевірки лише адресою відправника, що не гарантує безпечність листа. Відповіді, що свідчать про низький або критично низький рівень обізнаності (0.25 та 0 балів), сумарно обрані 5 учасниками опитування (28%), з яких троє (17%) готові були безпосередньо передати конфіденційну інформацію фішинговому джерелу.

Питання 2. Який із наведених прикладів найімовірніше вказує на фішингову атаку?

- лист із запрошенням на корпоратив (0);
- лист із вкладенням від знайомого колеги (0,25);
- лист із граматичними помилками і терміновим закликом до перевірки акаунту (1);
- лист, у якому просять змінити пароль (0,5);
- лист із інформацією про виграш у лотереї (0,75).

Рис 3.3. Результати відповідей на питання 2

Аналіз відповідей демонструє, що найбільше працівників (7 осіб, або 39%) обрали відповідь, яка оцінюється у 0.5 бала. Це свідчить про часткове розуміння ознак фішингової атаки, оскільки прохання змінити пароль дійсно може бути тривожним сигналом, але без додаткових фішингових ознак – не є однозначним індикатором.

Лише 5 осіб (28%) правильно ідентифікували найбільш типову форму фішингу – лист із граматичними помилками та терміновим закликом до дії, що наближає їхній рівень обізнаності до належного. Ще 3 респонденти (17%) обрали варіант про виграш у лотереї, що є частим фішинговим прийомом, але менш типово оформленим у корпоративному середовищі (0.75 бала).

Найменш ефективні з точки зору безпеки відповіді – запрошення на корпоратив (0 балів) та вкладення від колеги (0.25 бала) – були обрані загалом 3 респондентами (17%), що вказує на потребу в додатковому навчанні щодо контексту корпоративної комунікації та ймовірних векторів атаки через «довірених» осіб.

Питання 3. Ви випадково натиснули на підозріле посилання. Ваші дії?

- нічого не роблю, бо не ввів жодних даних (0);
- перезавантажую комп'ютер (0,25);
- встановлюю антивірус (0,5);
- повідомляю ІТ-відділ та запускаю перевірку системи (1);
- закриваю вкладку браузера (0,75).

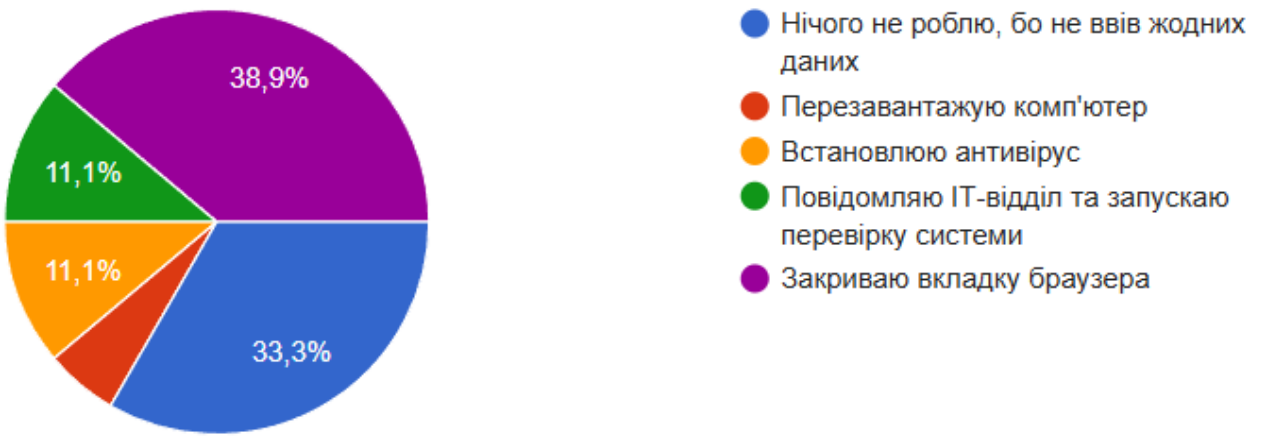

Рис 3.4. Результати відповідей на питання 3

Аналіз відповідей показує, що найпопулярнішим варіантом дій після натискання на підозріле посилання стало закриття вкладки браузера – цей варіант обрало 7 респондентів (39%), що оцінюється у 0.75 бала. Хоча це дієвий перший крок, однак він не є вичерпним з погляду реагування на потенційну загрозу.

Найбільш безпечний і правильний варіант дій – негайне повідомлення IT-відділу та ініціація перевірки системи – був обраний лише 2 учасниками (11%), що свідчить про обмежене розуміння повного алгоритму дій у разі потенційної інфекції системи.

Значна кількість опитаних (6 осіб, або 33%) обрали варіант “нічого не роблю”, мотивуючи це тим, що не вводили жодних даних. Така поведінка є небезпечною, оскільки навіть сам факт переходу за шкідливим посиланням може активувати завантаження шкідливого ПЗ або перенаправлення на фішинговий ресурс.

Решта респондентів (3 особи) розділилися між частково доцільними варіантами: встановленням антивірусу (0.5 бала) та перезавантаженням комп’ютера (0.25 бала). Хоча ці дії можуть мати певний ефект, вони не замінюють обов’язкового інформування спеціалістів з безпеки.

Питання 4. Хто з працівників є потенційною ціллю соціального інженера?

- лише IT-адміністратор (0);
- працівник фінансового відділу (0,25);
- усі співробітники компанії (1);
- менеджери середньої ланки (0,5);
- нові співробітники (0,75).

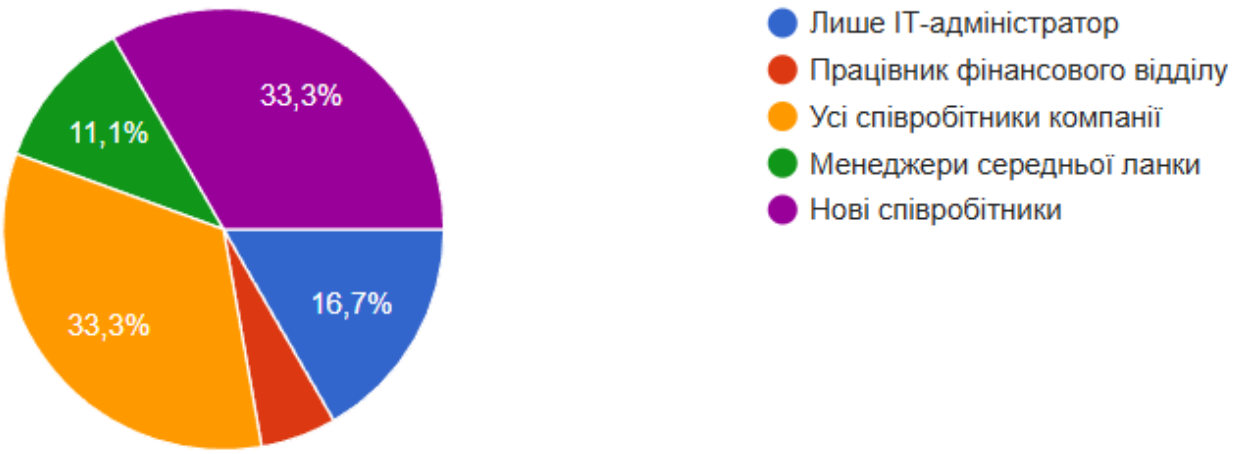

Рис 3.5. Результати відповідей на питання 4

Аналіз відповідей на це питання демонструє загальну тенденцію до часткового усвідомлення масштабності загрози соціальної інженерії. Лише 6 респондентів (33%) обрали цілком правильну відповідь – що усі співробітники компанії можуть бути ціллю зловмисника. Це свідчить про обмежене розуміння того, що соціальна інженерія не обмежується певною посадою чи рівнем доступу.

Ще 6 учасників (33%) відповіли, що ціллю найімовірніше є нові співробітники (0.75 бала). Така відповідь частково коректна, оскільки новачки дійсно є вразливішими через брак досвіду та знань про внутрішні політики безпеки. Водночас це не охоплює всіх потенційних мішеней, що знижує повноту оцінки.

Інші відповіді, зокрема “менеджери середньої ланки” (2 особи, 0.5 бала) та “працівник фінансового відділу” (1 особа, 0.25 бала), також вказують на часткове усвідомлення проблеми, оскільки ці категорії працівників дійсно можуть становити підвищений інтерес для зловмисників через доступ до конфіденційної інформації чи ресурсів.

Найнижчий рівень розуміння демонструють 3 респонденти (17%), які вважають, що лише IT-адміністратор є потенційною ціллю. Такий підхід є хибним і вказує на критичну прогалину в знаннях щодо методів атак, які орієнтовані на людський фактор у найширшому сенсі.

Питання 5. Що таке атака “претекстинг” у соціальній інженерії?

- надсилання повідомлень із шкідливим ПЗ (0);
- маніпуляція жертвою через вигадану ситуацію або фальшиву особу (1);
- злам комп’ютера через фішинг (0,25);
- використання USB-накопичувача для зараження системи (0,5);
- прямий запит до жертви про конфіденційні дані (0,75).

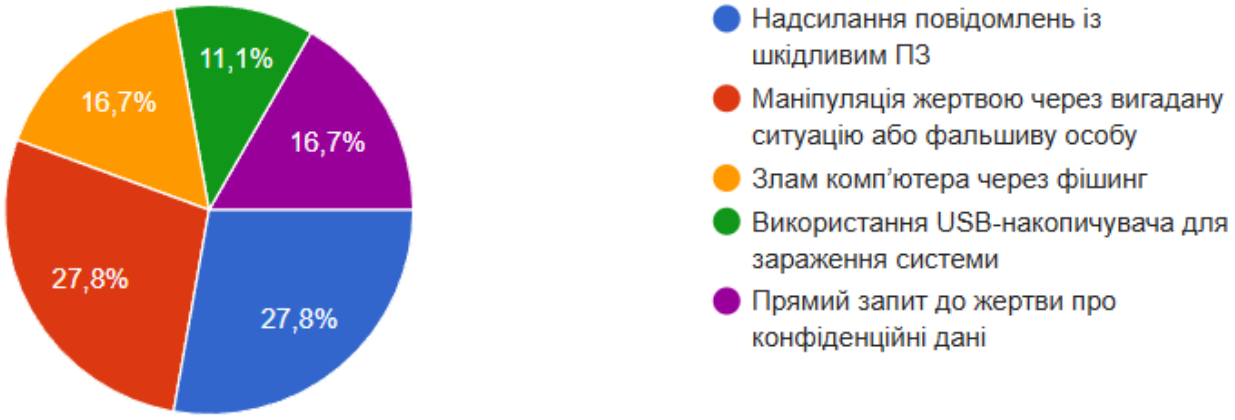

Рис 3.6. Результати відповідей на питання 5

Запитання стосувалося визначення сутності атаки типу претекстинг – однієї з ключових форм соціальної інженерії, що базується на створенні неправдивої передумови для завоювання довіри жертви. Із 18 респондентів лише 5 осіб (28%) змогли чітко ідентифікувати суть цієї атаки, обравши правильну відповідь: маніпуляція через вигадану ситуацію або фальшиву особу.

Решта учасників демонструють різні рівні часткового розуміння. Наприклад, 3 респонденти (17%) обрали варіант прямого запиту про конфіденційні дані (0.75 бала), що справді може мати місце в межах pretexting, проте не охоплює головного – створення переконливої вигаданої ситуації. Ще 2 учасники (0.5 бала) пов’язали претекстинг із використанням USB-носія, що радше стосується фізичних атак.

Найпоширенішою неправильною відповіддю стала – “надсилання повідомлень із шкідливим ПЗ” (5 осіб, 0 балів), що свідчить про плутанину між різновидами соціоінженерних і технічних атак. Така плутанина потенційно

небезпечна, адже у випадку претекстингу найголовнішим фактором є довіра до атакувальника, а не технічна реалізація.

Питання 6. Що з наведеного є найкращим способом перевірки підозрілого листа?

- натиснути на посилання, щоб перевірити, куди воно веде (0);
- відповісти відправнику з уточненням намірів (0,25);
- перевірити текст листа в Google (0,5);
- порівняти адресу відправника з офіційною й звернутись до служби безпеки (1);
- відкрити вкладення в режимі «інкогніто» (0,75).

Рис 3.7. Результати відповідей на питання 6

Це запитання перевіряло здатність співробітників правильно ідентифікувати безпечний метод перевірки потенційно фішингового листа. Правильний варіант відповіді – порівняти адресу відправника з офіційною та звернутись до служби безпеки – обрали 6 осіб (33%), що свідчить про помірний рівень обізнаності з основними принципами верифікації електронних повідомлень.

Більшість респондентів (7 осіб, або 39%) обрали частково безпечну дію – відкрити вкладення в режимі “інкогніто” (0.75 бала). Хоча така дія демонструє обережність, вона не гарантує повного захисту від шкідливого програмного

забезпечення, адже режим інкогніто не запобігає виконанню скриптів або завантаженню вірусів.

Ще 4 співробітники (22%) вважають перевірку тексту листа в Google ефективною (0.5 бала), що може бути корисною допоміжною дією, однак не є самодостатньою. Водночас лише 1 особа (0.25 бала) обрала відповідь на листа, що є ризикованим способом взаємодії з потенційним шахраєм.

Варто відзначити, що жоден з учасників не обрав варіант із натисканням на посилання, що є позитивною тенденцією, оскільки це – один із найнебезпечніших шляхів взаємодії з фішинговими листами.

Проведене опитування дозволило отримати кількісну та якісну оцінку рівня обізнаності співробітників компанії щодо основних соціоінженерних загроз та відповідних заходів кібергігієни. Аналіз відповідей на шість сформульованих запитань виявив як сильні, так і слабкі сторони у знаннях персоналу.

Загалом результати показують середній рівень поінформованості з окремими проявами високої обізнаності (наприклад, значна частина респондентів надала правильні або частково правильні відповіді на питання, пов’язані з ознаками фішингових атак, правильними діями при підозрілих листах, поняттям «претекстинг» тощо). Водночас було зафіксовано декілька небезпечних помилкових уявлень – зокрема, хибні дії після натискання підозрілого посилання або недооцінювання того, що соціоінженер може націлитись на будь-кого з працівників.

Отримані дані свідчать про потребу у структурованому навчальному втручанні, яке дозволить не лише покращити загальну обізнаність, а й закріпити правильні поведінкові моделі у відповідь на різні типи соціоінженерних атак.

3.2 Розробка структури та змістового наповнення навчальної програми

З огляду на високу ефективність соціоінженерних атак, що використовують психологічні прийоми впливу на користувачів з метою отримання конфіденційної інформації, виникає необхідність систематичного навчання персоналу основам інформаційної безпеки. Результати аналітичного огляду засвідчили широкий спектр методів соціальної інженерії та вразливостей, пов'язаних із людським чинником. Водночас аналіз сучасних практик побудови навчальних кампаній та проведене опитування працівників організації підтвердили як наявність критичних прогалин у знаннях, так і потребу в цільовому навчальному контенті.

У зв'язку з цим розробка ефективної навчальної програми має спиратися не лише на загальні принципи інформаційної безпеки, а й на адаптацію до конкретних потреб організації, враховуючи категорії співробітників, особливості їх професійної діяльності та наявний рівень обізнаності щодо загроз соціальної інженерії.

Розроблена навчальна програма має на меті підвищення рівня обізнаності працівників щодо соціоінженерних загроз, що є ключовим елементом у забезпеченні інформаційної безпеки організації. З огляду на результати попереднього аналізу, зокрема вивчення поширених методів соціальної інженерії, аналізу практик компаній щодо протидії цим атакам, а також факторів, які впливають на вразливість працівників, було визначено необхідність створення навчального продукту, що охоплює як теоретичні знання, так і практичні навички.

Програма передбачає поступове формування в співробітників здатності розпізнавати ознаки шахрайства в цифровому середовищі, адекватно реагувати на потенційно небезпечні ситуації, а також усвідомлювати власну роль у підтриманні загального рівня кібергігієни. Зміст програми ґрунтується на адаптації матеріалу до специфіки роботи різних категорій персоналу, з урахуванням їхньої професійної діяльності та рівня доступу до інформаційних систем. Вона також передбачає використання інтерактивних методів, включаючи симуляції фішингових атак, тематичні тести та кейс-завдання, що дозволяє не лише донести матеріал, але й закріпити його у практичному контексті.

Окрему увагу приділено формуванню критичного мислення у співробітників – важливого психолого-поведінкового елементу, який дозволяє знижувати ефективність маніпулятивного впливу. Крім того, у програмі закладено систему оцінювання прогресу учасників, що забезпечує можливість об’єктивного моніторингу динаміки змін у рівні знань та навичок.

Модуль 1. Вступ до соціальної інженерії: атака, що починається з людини.

Мета модуля: формування в учасників цілісного уявлення про природу соціоінженерних загроз, їх психологічні механізми, ключові історичні приклади та причини особливої ефективності таких атак у корпоративному середовищі. Навчальний контент побудований так, щоб одночасно задовольнити вимоги до академічного наповнення та викликати пізнавальний інтерес у слухачів – шляхом демонстрації реальних сценаріїв злому, типових пасток і найпоширеніших помилок поведінки користувачів.

Науково-практичне обґрунтування включення модуля. Соціальна інженерія розглядається сучасними фахівцями як один із найнебезпечніших класів атак, що уникає традиційного виявлення засобами технічного контролю. Включення модуля до навчальної програми дозволяє розпочати формування базової кіберстійкості з найважливішого – усвідомлення ризику на особистісному рівні. Модуль закладає основу для подальшого формування захисної поведінки користувачів в інформаційному середовищі.

Методи викладання та засоби залучення:

- аналіз реальних інцидентів і демонстрація фрагментів шахрайських листів;
- інтерактивне голосування за сценаріями: “Як би ви вчинили?”;
- інфографіка про “життєвий цикл” соціоінженерної атаки;
- короткі тестові блоки (самоконтроль знань) після кожної секції.

Зміст модуля охоплює такі теми:

1.1. Визначення соціальної інженерії та її місце в системі кіберзагроз:

- надано класифікацію соціоінженерних впливів у контексті сучасних ризиків ІБ;

- пояснено, чому, незважаючи на наявність складних систем захисту, атаки через людину залишаються найуспішнішими.

1.2. Еволюція підходів до соціоінженерних атак:

- описано перехід від телефонних шахрайств і підроблених листів до глибоко персоналізованих атак із використанням даних із соцмереж і технологій deepfake;
- подано приклади злому відомих компаній через “звичайні” дії співробітників – відкриття вкладення, відповідь на лист, виконання інструкцій нібито від керівника.

1.3. Механізми впливу: як зловмисники отримують довіру:

- проаналізовано ключові техніки психологічного впливу, що застосовуються при соціоінженерних атаках: авторитет, терміновість, соціальний доказ, страх;
- слухачі дізнаються, чому навіть обізнані фахівці часто потрапляють у пастку.

1.4. Людський чинник як пріоритетна вразливість:

- висвітлено роль користувача в загальній системі інформаційної безпеки;
- обґрунтовано, чому жодна технологія не може повністю нівелювати наслідки помилок людини.

1.5. Аналіз сучасних загроз для гібридного корпоративного середовища:

- розглянуто вплив змішаних форматів роботи (офіс-дистанційна модель) на зростання ризиків соціальної інженерії;
- підкреслено актуальність особистої цифрової гігієни та навичок розпізнавання маніпуляцій.

1.6. Вступне діагностичне опитування:

- здійснюється попередня оцінка знань і поведінкових моделей слухачів щодо фішингу, реагування на запити невідомого походження, виявлення ознак шахрайства;
- результати дозволяють адаптувати темп і складність наступних модулів під рівень аудиторії.

Очікувані результати передбачають, що після проходження модуля слухач:

- розуміє загальні принципи соціоінженерних атак;
- може пояснити психологічні механізми впливу зловмисників;
- усвідомлює, як щоденні дії можуть стати каналом компрометації;

- критично оцінює комунікаційні запити в робочому середовищі;
- підвищує настороженість і сформованість поведінкових “бар’єрів”.

Модуль 2. Класичні техніки соціальної інженерії: розпізнати, передбачити, уникнути.

Мета модуля: надати учасникам структуровані знання про традиційні техніки соціальної інженерії, що найчастіше використовуються в реальному корпоративному середовищі, навчити відрізняти різні види атак за типом взаємодії та формувати навички їх своєчасного розпізнавання.

Наукове обґрунтування включення модуля. Попри швидку еволюцію цифрових загроз, класичні техніки соціальної інженерії залишаються найбільш поширеними каналами первинної компрометації в реальних атаках. Саме завдяки своїй простоті, низькому технологічному бар’єру та високій ефективності вони становлять особливу небезпеку для некритичних користувачів. Включення цього модуля в програму обґрунтовується необхідністю формування у персоналу базового навику розпізнавання типових патернів атак та запобігання їм на ранній стадії.

Методи викладання та засоби залучення:

- візуальні схеми технік (інфографіка: “Тактики маніпуляцій”);
- симуляція фішингового листа з подальшим розбором дій;
- аудіоаналіз запису фішингового дзвінка (vishing-симуляція);
- робота в парах: один “атакує”, інший аналізує – як будуються легенди;
- картки “загроза – контрдія”: швидкий аналіз сценаріїв.

Зміст модуля охоплює такі теми:

2.1. Phishing – фішинг як наймасовіший вектор впливу:

- класифікація фішингових атак: загальний фішинг, spear phishing (цільовий), clone phishing (дублюючий), whaling (на керівників);
- типові риси підроблених листів і повідомлень: терміновість, загроза санкцій, подарунки;
- приклади зламу компаній через фішинг – кейс-аналіз (Google, Facebook);
- практичне завдання: розпізнавання фішингу у прикладах листування.

2.2. Vishing, smishing, QRishing: атаки поза поштовою скринькою:

- голосові дзвінки з імітацією служби підтримки або безпеки (vishing);
- SMS-шахрайство з посиланнями на фейкові сайти або “екстрені” дії;
- використання QR-кодів у зловмисних цілях (QRishing);
- роль соціального тиску: “зараз або ніколи”, “ви останній, хто не підтвердив” тощо.

2.3. Pretexting: атака через легенду:

- сутність підготовленого сценарію взаємодії (“претекст”);
- як створюється переконлива легенда для отримання даних або дій;
- атаки через підроблені службові інструкції, фіктивні анкети, телефонні розмови.

2.4. Baiting і quid pro quo: атаки на базових інстинктах користувача:

- приклади використання USB-носіїв, “подарункових” пропозицій, тестових доступів;
- психологія обміну: “ви допоможете – ми вам дамо бонус” (quid pro quo);
- як інструменти соціальної інженерії перетворюють зацікавленість на вразливість.

2.5. Tailgating та shoulder surfing: атаки в реальному фізичному просторі:

- доступ до приміщень через супровід або “псевдопрацівника”;
- спостереження за введенням паролів, копіювання екранів, знімки ID;
- застосування технік “людського фону”: користування ввічливістю або поспіхом.

2.6. Підсумкова інтерактивна сесія: класифікація та розбір кейсів:

- учасники отримують набір коротких ситуацій (опис атаки) та мають визначити тип техніки; вказати ознаки, що її ідентифікують; запропонувати безпечну реакцію.

Очікувані результати передбачають, що після проходження модуля слухач здатен:

- класифікувати основні типи класичних соціоінженерних атак;

- впевнено розпізнавати ознаки фішингу та маніпуляцій в електронних комунікаціях;
- критично оцінювати підозрілі запити, навіть якщо вони маскуються під “офіційні”;
- аргументовано пояснювати, чому певна дія може бути небезпечною;
- застосовувати моделі реагування (перевірка джерела, подвійне підтвердження, ігнорування тощо).

Модуль 3. Сучасні соціоінженерні атаки: технології, які працюють проти нас.

Мета модуля: ознайомити слухачів з новітніми підходами до реалізації соціоінженерних атак, що ґрунтуються на використанні цифрових платформ, штучного інтелекту, аналітики великих даних та міжплатформної інтеграції. Навчити своєчасно розпізнавати гібридні загрози, які поєднують елементи класичних технік з технологічним посиленням.

Науково-практичне обґрунтування включення модуля. Поширення інструментів штучного інтелекту, а також доступність платформ для генерації текстів, зображень та голосових повідомлень, створює нову хвилю соціоінженерних загроз, що маскуються під легітимну корпоративну комунікацію. Ефективний захист в таких умовах передбачає не лише знання типових технік, але й вміння критично сприймати інформацію незалежно від її форми. Включення модуля дозволяє сформувати у працівників високий рівень обережності щодо довіри до цифрового контенту.

Методи викладання та засоби залучення:

- демонстрація реального deepfake (відеоаналітика з паузами для обговорення);
- вправа: “Склади профіль користувача з відкритих джерел” – симуляція OSINT;
- колективний розбір фейкового бізнес-листа: пошук нетипових сигналів;
- аналіз структури повідомлення в чаті: які ознаки вказують на компрометацію.

Зміст модуля охоплює такі теми:

3.1. Deepfake, voice spoofing, AI-generated personas:

- принципи роботи deepfake-технологій: генерація відео та аудіо з переконливою імітацією особистості;
- сценарії атак: “дзвінок від керівника”, “відеозвернення з терміновим дорученням”;
- практичний кейс: як один deepfake-дзвінок коштував компанії $240 тис.;
- обговорення: чи можемо ми ще довіряти побаченому та почутому?

3.2. Атаки через соціальні мережі: персоналізація на основі OSINT:

- як зловмисники збирають інформацію з відкритих джерел (LinkedIn, Facebook, Instagram, Telegram) для створення максимально переконливого сценарію атаки;
- техніка “social profiling”: створення ілюзії знайомства, авторитету або термінової співпраці.

3.3. Business Email Compromise (BEC) 2.0:

- сучасні атаки BEC із використанням AI-аналізу стилю мовлення (natural language mimicry);
- вбудованість у корпоративні ланцюжки листування;
- алгоритм дій користувача при отриманні фінансового запиту “згідно з новою політикою”;
- анонімізований розбір інцидентів із втратами понад $10 млн.

3.4. Атаки через цифрові інфраструктури: Slack, Zoom, MS Teams, Trello:

- вектори атак у внутрішньокорпоративному середовищі: фейкові профілі, шкідливі посилання у чатах, “перехоплення” запрошень до нарад;
- особливості атак під час віддаленої роботи (Remote Social Engineering);
- сценарій-симуляція: повідомлення в Slack від “служби підтримки IT”.

3.5. Гібридні атаки та автоматизовані фішингові кампанії:

- як поєднуються фішинг, OSINT, генеративні моделі та шаблони масових впливів;

- інструменти з відкритим кодом, які використовують самі зловмисники (GoPhish, Evilginx, Maltego);
- демонстрація прикладу генерації персоналізованого листа за 10 секунд на основі профілю користувача.

Очікувані результати передбачають, що після проходження модуля слухачі:

- розпізнають новітні техніки соціальної інженерії на основі AI та гібридних технологій;
- розуміють логіку атак, побудованих на зборі відкритих даних;
- вміють виявляти “надто персоналізовані” запити як маркер атаки;
- здатні виявити ознаки BEC та підозрілих дій у внутрішньокорпоративних платформах;
- демонструють підвищену обережність до візуальних і голосових повідомлень сумнівного походження.

Модуль 4. Індивідуальний захист і поведінкова гігієна користувача.

Мета модуля: сформувати у працівників стійку модель поведінки в цифровому середовищі, засновану на принципах критичного мислення, персональної відповідальності та цифрової обережності. Навчити учасників оцінювати ризики, пов’язані з їхніми щоденними діями, та запроваджувати звички, які знижують імовірність успішної соціоінженерної атаки.

Наукове обґрунтування включення модуля. Соціоінженерна атака реалізується не лише через технологічні або інформаційні вектори, а й через вразливості у звичайних поведінкових моделях користувачів. Навіть у присутності високотехнологічного захисту, людський фактор залишається критичним. Результати досліджень ENISA, NIST та Verizon DBIR підкреслюють, що саме поведінка користувачів, сформована за умов рутинної взаємодії, є вирішальним чинником у більшості кіберінцидентів. Включення модуля дозволяє перейти від абстрактного знання до особистої цифрової дисципліни, що є необхідною умовою зниження ризиків компрометації.

Методи викладання та засоби залучення:

- інтерактивна міні-гра: “Пройди день в інтернеті, не потрапивши в пастку” (щоденні ризики користувача);
- самооцінка цифрової поведінки за шкалою “кіберстресостійкості”;
- воркшоп: створення особистого набору “цифрових правил”;
- відкрите обговорення: які звички “проти нас” працюють на користь атакуючого?

Зміст модуля охоплює такі теми:

4.1. Цифрова гігієна як основа особистої безпеки:

- базові принципи захисту цифрової особистості: конфіденційність, автентичність, доступність;
- поняття “гігієни паролів”: створення, зберігання, регулярна зміна, MFA;
- налаштування конфіденційності в соціальних мережах: як обмежити “вітрину” для зловмисника;
- практична вправа: перевірка поточних налаштувань власних акаунтів.

4.2. Поведінкова модель користувача в умовах соціоінженерної атаки:

- розпізнавання підозрілих запитів: сигнали небезпеки у комунікаціях;
- принципи “зупинись – перевір – підтвердь” (Stop – Think – Verify);
- поведінкові пастки: як поспіх, страх, авторитет або ввічливість ведуть до компрометації;
- візуалізація моделей прийняття рішень у стресових умовах.

4.3. Емпатійна атака: чому людина відкриває лист, навіть коли знає, що не слід:

- роль емоцій у поведінці: страх втрати, бажання допомогти, відчуття обов’язку;
- кейси, де зловмисник грає на співчутті (“пожертвування”, “допомога колезі”, “діти в небезпеці”);
- практичний аналіз: лист від імені знайомого співробітника з проханням.

4.4. Побудова “цифрових бар’єрів” у щоденній роботі:

- формування особистої кіберзвички: не відкривати одразу, не відповідати миттєво, перевіряти адресанта;

- автоматизація захисту: фільтри, антифішинг, попередження про зовнішні листи;
- ведення цифрового щоденника реакцій (слід дій у разі сумніву);
- індикатори того, що ви – потенційна ціль: підвищена кількість запитів, “анонімні” підписники.

4.5. Практичне моделювання: як реагувати на реальну спробу атаки:

- учасникам пропонується сценарій: вхідний лист / дзвінок / чат-запит з ознаками соціоінженерної атаки;
- визначення послідовності дій: оцінка, перевірка, фіксація, повідомлення ІБ;
- обговорення найбільш ефективних та найнебезпечніших реакцій.

Очікувані результати передбачають, що після проходження модуля слухачі:

- усвідомлюють, як особисті дії можуть сприяти успішній атаці;
- вміють розпізнавати поведінкові маніпуляції та вплив емоцій;
- засвоюють алгоритми безпечної реакції на підозрілі звернення;
- формують власні “бар’єри обережності” у цифровій щоденності;
- демонструють сталу обережність і готовність повідомляти про інциденти.

Модуль 5. Корпоративні процедури та взаємодія у відповідь на соціоінженерні загрози.

Мета модуля: навчити працівників діяти узгоджено й ефективно у разі підозри на соціоінженерну атаку, забезпечити знання внутрішніх процедур, відповідальних осіб, а також сформувати культуру негайного реагування й безпечної комунікації в межах організації.

Наукове обґрунтування включення модуля. Попри високу ефективність технічних засобів захисту, більшість соціоінженерних атак успішні саме завдяки відсутності належного реагування з боку персоналу. Дослідження показують, що до 40% працівників не повідомляють про фішингові інциденти через відсутність зрозумілих процедур або страх наслідків. Таким чином, наявність

структурованого модуля, присвяченого саме діям у разі загрози, є критичним компонентом будь-якої програми з підвищення обізнаності. Цей модуль завершує навчальний цикл, переводячи знання з рівня індивідуального усвідомлення на рівень організаційної практики.

Методи викладання та засоби залучення:

- створення персональної "карти дій" у випадку інциденту;
- симуляція ситуації: керівник надіслав інструкцію змінити рахунок для платежу;
- робота в групах: аналіз внутрішньої комунікації з позиції безпеки;
- презентація: реальні приклади звітів про інциденти, які стали вирішальними.

Зміст модуля охоплює такі теми:

5.1. Канали звітування про підозрілі інциденти:

- кому і як повідомляти про підозрілий лист, дзвінок або повідомлення;
- визначення відповідальних осіб: служба ІБ, локальні координатори безпеки, лінійні керівники;
- формати повідомлень: email, спеціальні форми, кнопка "Report phishing";
- пояснення принципу "краще повідомити зайвий раз, ніж промовчати".

5.2. Алгоритм реагування: модель "STOP – THINK – CONFIRM – REPORT":

- покроковий розбір дій працівника при виникненні сумніву;
- паралелі з реагуванням на інші критичні ситуації (пожежа, евакуація);
- пояснення, чому емоції, страх "виглядати недосвідченим" або "не створювати проблем" – основні бар'єри звітування.

5.3. Корпоративна культура безпеки: що може зробити кожен працівник:

- культура нульової толерантності до ризиків (Zero Trust Mindset);
- відповідальність не тільки за себе, а й за команду: підозри щодо чужих дій – не донос, а захист;
- соціальне підкріплення: відкритість до обговорення, похвала за уважність;

- приклади, коли завдяки звіту простого співробітника вдалося зупинити реальну атаку.

5.4. Типові помилки під час взаємодії в середині організації:

- виконання неавторизованих інструкцій, пересилання підозрілих листів, переадресація “від керівництва”;
- надання доступу до інформаційних ресурсів без верифікації особи;
- обговорення потенційно чутливої інформації у відкритих каналах;
- розбір прикладів: як “внутрішня довіра” використовується атакуючими.

5.5. Заключне узагальнення та оцінювання:

- повторення ключових тез усіх модулів у форматі мапи знань;
- індивідуальне тестування: ситуаційні запитання, мультиваріантні кейси.

Очікувані результати передбачають, що після проходження модуля слухачі:

- чітко розуміють внутрішні процедури звітування та реагування на соціоінженерні загрози;
- засвоюють принципи безпечної взаємодії в межах колективу;
- формують відповідальну поведінку щодо кіберризиків не лише у своїй сфері, а й у колективному контексті;
- уникають найпоширеніших поведінкових помилок;
- здатні підтримувати загальний рівень ІБ в організації завдяки культурі безпеки.

3.3 Проведення експериментального впровадження навчальної програми та оцінювання динаміки змін рівня обізнаності співробітників

На завершальному етапі реалізації навчальної програми доцільним є проведення експериментального оцінювання результатів засвоєння матеріалу, що дозволяє виявити ефективність обраних освітніх підходів та змістового наповнення модулів. Зважаючи на практичні обмеження та етичні міркування, у даному дослідженні відмовлено від моделювання реальної фішингової атаки, що

могло б спричинити небажані ризики для корпоративної IT-інфраструктури. Як альтернатива, обрано метод тестового моделювання ситуаційного аналізу фішингових комунікацій, який дозволяє досягти аналітичної мети експерименту без створення загроз.

Суть експерименту полягає у наданні співробітникам набору з п’яти електронних листів, серед яких три є фішинговими, а два – справжніми (рис 3.8.). Завданням співробітників є визначення типу кожного листа, що дозволяє дослідити рівень сформованості навичок виявлення соціоінженерних загроз. Такий підхід забезпечує об’єктивне оцінювання здатності респондентів застосовувати набуті знання у наближених до реальних умовах ситуаціях.

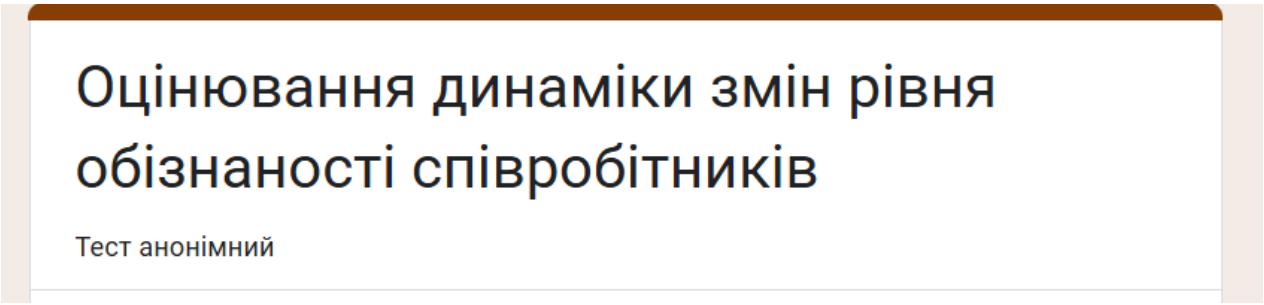

Рис 3.8. Тестування за допомогою Google Forms

Перший сценарій (рис. 3.9) було спрямовано на оцінку здатності працівників розпізнавати фішингове повідомлення у типових умовах. У листі були навмисно вмонтовані ознаки шахрайства, зокрема маніпулятивне формулювання, неспівпадіння адреси відправника з офіційним доменом, орфографічні помилки та заклик до термінової дії.

Визначте тип листа

Тема: [Legal Compliance] Негайно оновіть політику конфіденційності

Шановний користувачу,

Згідно з оновленням GDPR та внутрішніх регламентів ISO/IEC 27001, вам необхідно пройти оновлену політику конфіденційності.

Перейдіть за наступним посиланням та натисніть “Підписати”:

https://secure.docs-legalcorp.com/gdpr2025

У разі невиконання вимоги до 17:00 сьогодні, ваш обліковий запис буде тимчасово деактивований.

Дякуємо за відповідальність.

— Юридичний відділ

- ◯ Фішинговий
- ◯ Справжній

Рис 3.9. Питання 1

Було отримано результати, які показали наступне: більшість респондентів успішно ідентифікували лист як потенційно небезпечний. Зокрема, 16 із 18 учасників (що становить 89%) надали правильну відповідь (рис. 3.10).

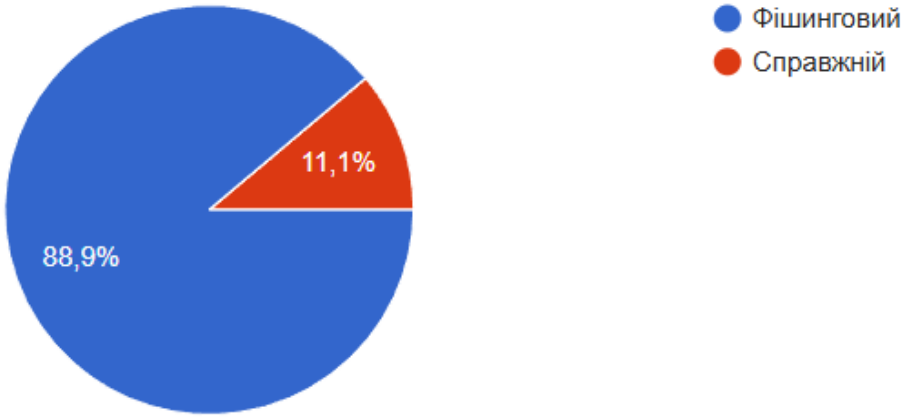

Рис 3.10. Результати відповідей на питання 1

Зазначена тенденція свідчить про загалом високий рівень засвоєння працівниками основних принципів кібергігієни, зокрема здатності до критичної оцінки вхідної електронної кореспонденції та виявлення типових ознак

соціоінженерного впливу. Такий результат підтверджує ефективність розробленої та впровадженої навчальної програми.

Разом з тим, факт надання двох некоректних відповідей свідчить про наявність певної сприйнятливості до фішингових атак серед окремих співробітників. Це підкреслює необхідність подальшого удосконалення навчальних кейсів, зокрема шляхом включення прикладів складніших, контекстуально наближених до реального робочого середовища атак, а також доцільність періодичного повторення навчальних заходів.

Наступний сценарій (рис. 3.11) мав на меті оцінити здатність працівників розпізнавати фішингові повідомлення, замасковані під службову або внутрішню ділову переписку. У тестовому листі використовувались такі елементи, як правдоподібне ім’я відправника, посилання на нібито термінове завдання від колеги, відсутність очевидних граматичних помилок.

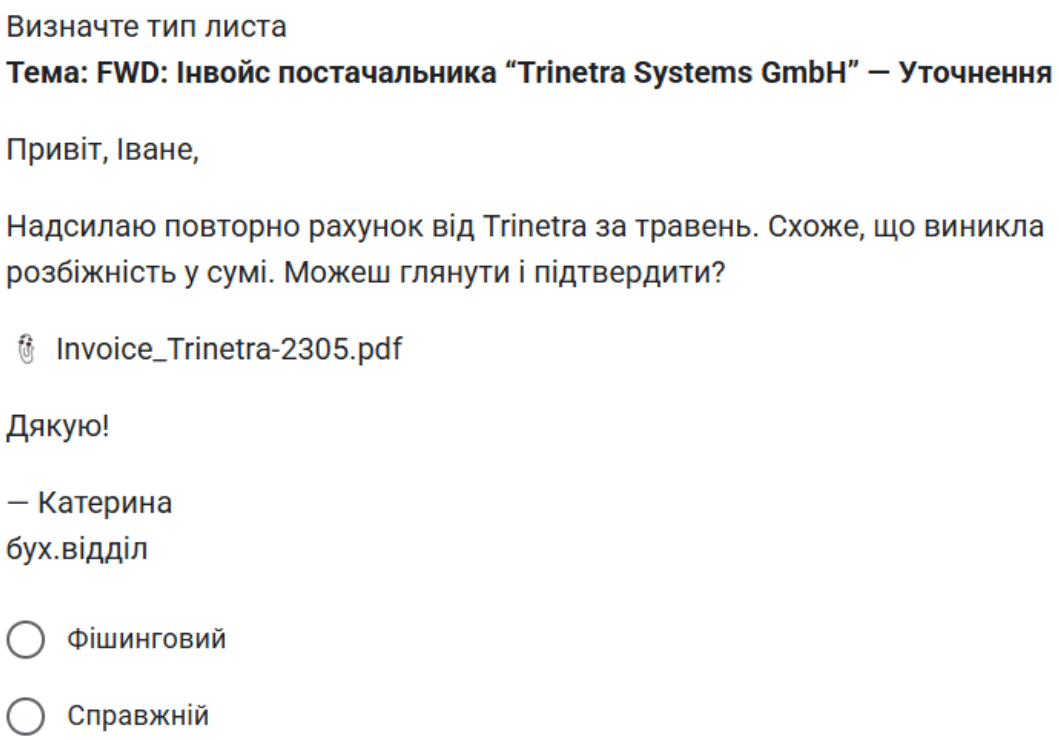

Рис 3.11. Питання 2

Було зафіксовано нижчий рівень розпізнавання фішингового повідомлення у порівнянні з попереднім прикладом: лише 13 із 18 працівників (що становить 72%) правильно класифікували лист як потенційно шкідливий (рис. 3.12).

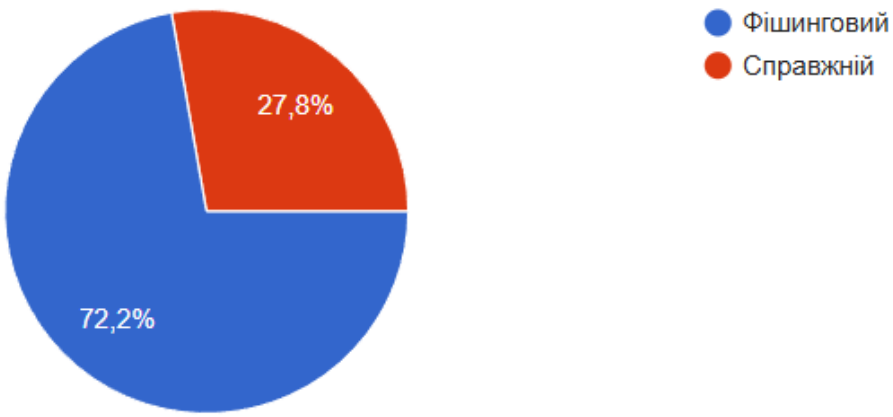

Рис 3.12. Результати відповідей на питання 2

П’ятеро респондентів помилково визначили повідомлення як справжнє, що свідчить про труднощі у виявленні загроз, які імітують звичну ділову комунікацію. Це підкреслює, що фішингові атаки типу Business Email Compromise (компрометація ділової електронної пошти) залишаються особливо небезпечними для співробітників, навіть після проходження базового навчання.

Вказані результати акцентують на важливості включення подібних сценаріїв до майбутніх тренінгів, а також на потребі поглибленого висвітлення технік маскування під легітимну комунікацію в межах навчальної програми. Це дозволить сформувати більш стійкі навички розпізнавання фішингових загроз у реалістичних умовах.

Третій сценарій (рис. 3.13) був спрямований на перевірку здатності респондентів відрізнити справжній службовий лист від фішингового, не спираючись на емоційні тригери чи шаблонні ознаки шахрайства. Повідомлення не містило орфографічних помилок або нестандартних звернень, мало типовий корпоративний стиль і відповідало стандартам внутрішньої електронної комунікації.

Визначте тип листа
Тема: Нагадування: Заповнення щомісячного звіту

Шановні працівники,
нагадуємо, що до **18:00 сьогодні** необхідно заповнити форму звітності за квітень.
Форма доступна у внутрішній системі документообігу:
forms.corp-system.com/reporting

У разі виникнення питань звертайтесь до свого керівника напряму.
Дякуємо за дотримання внутрішніх регламентів.

Відділ операційної підтримки

◯ Фішинговий

◯ Справжній

Рис 3.13. Питання 3

Результати виявили високий рівень обізнаності працівників щодо характерних ознак автентичної електронної кореспонденції: 17 із 18 учасників (94%) правильно класифікували лист як справжній (рис. 3.14).

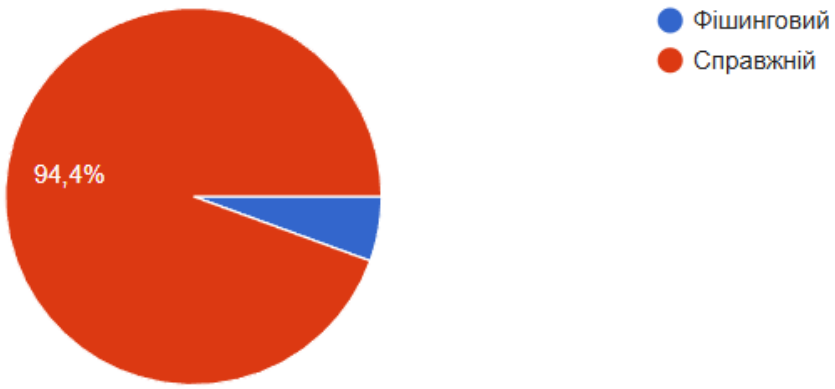

Рис 3.14. Результати відповідей на питання 3

Лише один респондент помилково визначив повідомлення як фішингове, що може свідчити про надмірну настороженість, спричинену окремими елементами тексту — наприклад, стислістю формулювань, закликом до термінового реагування чи наявністю гіперпосилання.

Це підкреслює необхідність формування в учасників навичок критичного аналізу всіх типів вхідних повідомлень, зокрема й цілком легітимних. Такий підхід дозволить уникнути ситуацій, коли через надмірну підозру можуть ігноруватися або блокуватися реальні службові запити, що впливає на ефективність внутрішньої комунікації.

Четвертий сценарій (рис. 3.15) був побудований на прикладі типової внутрішньої комунікації з вкладенням, що містило службову інформацію. Метою було оцінити рівень довіри співробітників до внутрішніх джерел та здатність відрізнити легітимне повідомлення від фішингового, враховуючи наявність вкладеного файлу — елементу, який часто використовується в атаках.

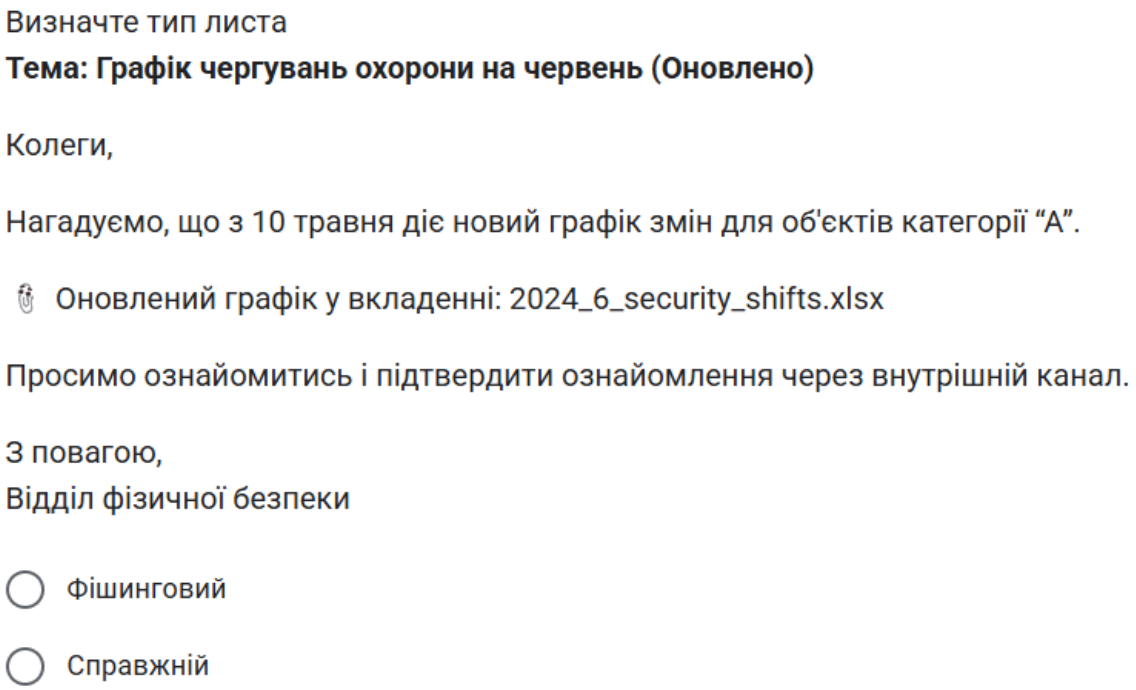

Рис 3.15. Питання 4

Результати демонструють загальну тенденцію до правильного розпізнавання: 14 із 18 респондентів (78%) коректно ідентифікували лист як справжній (рис. 3.16).

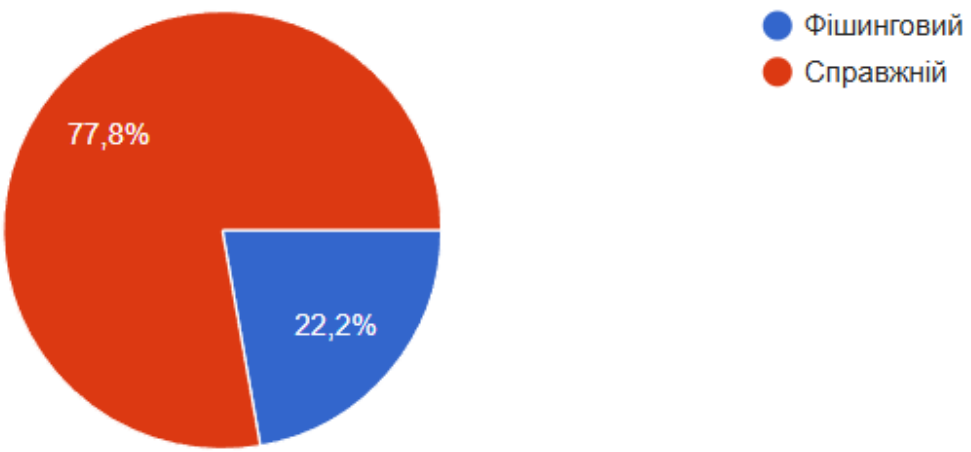

Рис 3.16. Результати відповідей на питання 4

Разом із тим, 4 учасники (22%) класифікували лист як потенційно фішинговий, що свідчить про наявність певної обережності щодо вкладених файлів навіть у внутрішньому інформаційному середовищі. Така реакція може бути наслідком успішного засвоєння попереджувального матеріалу в межах навчальної кампанії.

Однак надмірна настороженість також має свої ризики — вона може призводити до ігнорування або блокування справжніх службових повідомлень, що, у свою чергу, негативно впливає на ефективність робочих процесів. Тому в подальших тренінгах варто зробити акцент на розвитку контекстної оцінки ситуацій, а також формуванні збалансованого підходу до аналізу джерел і змісту листів, що надходять у рамках корпоративної взаємодії.

П’ятий сценарій (рис. 3.17) моделював типовий фішинговий лист, замаскований під повідомлення від корпоративного сервісу, з метою перевірити здатність співробітників виявляти загрози, пов’язані з підробкою службових сповіщень. Особливу увагу в сценарії було приділено перевірці уважності до доменних адрес, стилістики повідомлення та нетипової форми звернення.

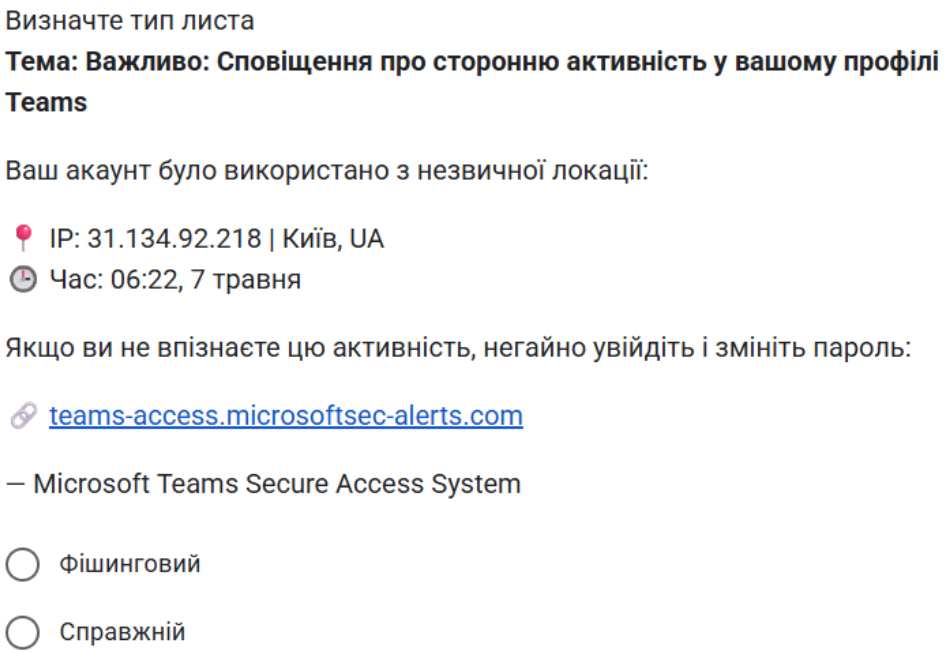

Рис 3.17. Питання 5

Результати оцінки показали найвищий рівень обізнаності серед усіх прикладів: усі 18 респондентів (100%) вірно визначили повідомлення як фішингове (рис. 3.18).

Рис 3.18. Результати відповідей на питання 5

Такий результат свідчить про ефективність навчального впливу та успішне засвоєння ключових ознак фішингових атак, зокрема спроб імітації корпоративних джерел. Учасники продемонстрували здатність до критичного аналізу технічних деталей повідомлення, таких як некоректні доменні імена,

загальні формулювання та невідповідність візуального стилю звичним службовим шаблонам.

Отримані дані підтверджують, що включення подібних кейсів до навчальної програми дозволяє значно підвищити рівень стійкості працівників до типових сценаріїв соціальної інженерії.

Для оцінки ефективності навчальної програми було проведено порівняльний аналіз результатів початкового діагностичного тестування та підсумкового експериментального тестування за ключовими модулями навчального курсу. На рисунку 3.19 наведено стовпчасту діаграму, що відображає середній рівень правильних відповідей співробітників по кожному модулю «до» та «після» проходження навчання.

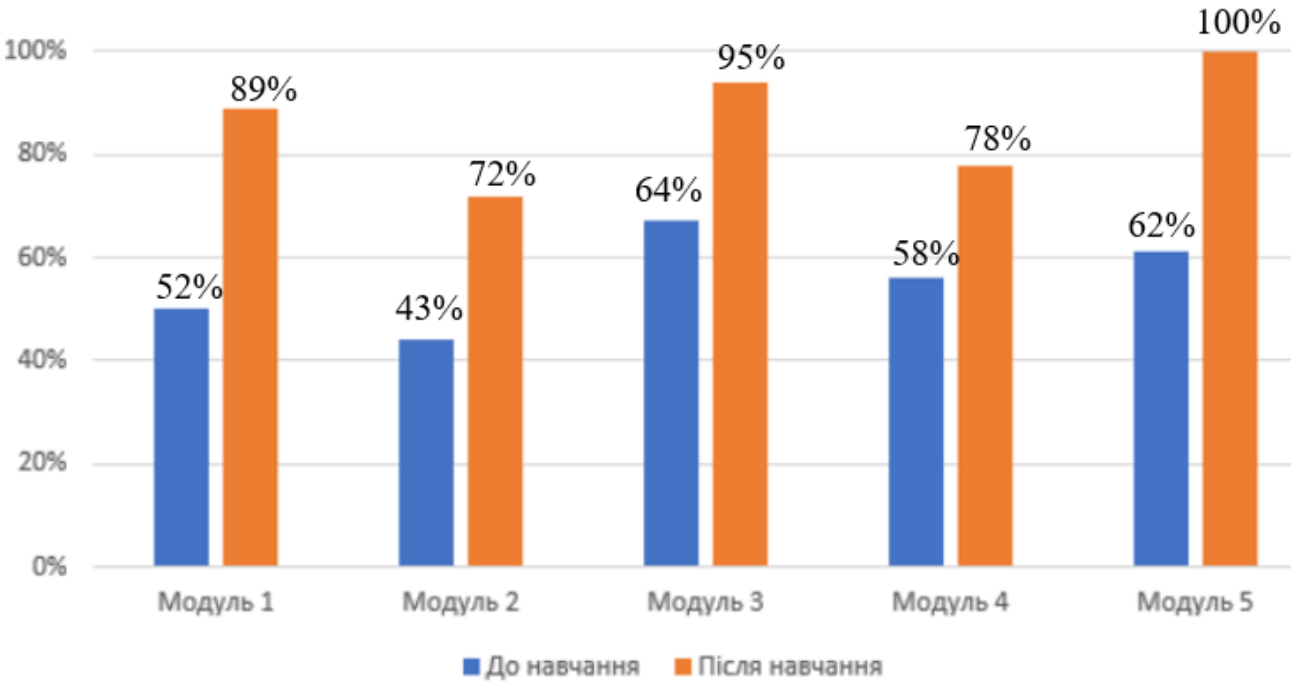

Рис 3.19. Узагальнення результатів навчання

Діаграма наочно демонструє суттєве підвищення рівня обізнаності співробітників по всіх ключових напрямках навчальної програми. Найбільше покращення відзначається у вмінні ідентифікувати фішингові повідомлення з явними ознаками шахрайства, що свідчить про успішне засвоєння базових критеріїв безпеки. Водночас результати по модулю з розпізнавання більш

складних сценаріїв, що імітують внутрішню комунікацію, показують наявність резервів для подальшого удосконалення програми.

Таке наочно подане порівняння дозволяє не лише підтвердити ефективність навчального курсу загалом, але й визначити пріоритетні напрямки для подальших освітніх заходів, що сприятимуть зміцненню культури кібербезпеки в організації.

3.4 Узагальнення результатів впровадження та формування рекомендацій для подальшого вдосконалення

У результаті впровадження розробленої навчальної програми, спрямованої на підвищення обізнаності співробітників щодо соціоінженерних загроз, було досягнуто позитивної динаміки у засвоєнні ключових знань з інформаційної безпеки. Результати підсумкового тестування, яке включало завдання з ідентифікації фішингових листів, засвідчили значне покращення здатності співробітників розпізнавати ознаки соціоінженерних атак. Зокрема, абсолютна більшість працівників успішно ідентифікували фішингові повідомлення, демонструючи сформовані навички критичної оцінки вхідної електронної кореспонденції.

Порівняння результатів з початковим діагностичним тестом свідчить про зростання рівня усвідомлення загроз соціальної інженерії, що є прямим наслідком цільової навчальної взаємодії. Окрім кількісних змін, було зафіксовано і якісні зрушення: працівники виявляли вищий рівень обґрунтованості відповідей, посилалися на ознаки фішингу та продемонстрували краще розуміння типових сценаріїв атак.

Подальший аналіз результатів фінального тестування дозволяє деталізувати динаміку змін у рівні обізнаності співробітників та виявити типові труднощі, з якими вони стикалися. Найвищий рівень правильних відповідей було зафіксовано у випадках, коли фішингові повідомлення містили очевидні ознаки шахрайства – помилки в оформленні, граматичні неточності або підозрілі

посилання. Так, на один із таких листів правильно відреагували всі 18 респондентів, що свідчить про успішне засвоєння базових критеріїв розпізнавання загроз.

Водночас найнижчий рівень правильних відповідей – лише 13 з 18 – спостерігався у випадку листа, який імітував внутрішню корпоративну комунікацію з використанням формально правильного стилю, що ускладнило ідентифікацію потенційної загрози. Цей результат вказує на потребу в подальшому поглибленні навчання щодо розпізнавання складніших форм соціальної інженерії, які апелюють до корпоративного контексту або містять фальсифіковану інформацію з ознаками легітимності.

Серед листів, що були справжніми, найменше помилок було зафіксовано у випадку повідомлення із стандартним шаблоном сервісу – лише один респондент сплутав його з фішинговим. Натомість інший приклад справжнього листа, який мав елементи персоналізації, виявився складнішим для оцінювання: чотири респонденти помилково класифікували його як фішинговий. Це свідчить про залишкову обережність співробітників, що загалом позитивно впливає на безпекову культуру, проте може спричиняти хибно-позитивні оцінки у звичайній корпоративній комунікації.

Результати тестування до та після навчання зведені в таблиці 3.2.

Таблиця 3.2

Порівняльний аналіз результатів до та після навчання

Модуль	**Відсоток правильних відповідей**		**Абсолютний приріст (п.п)**	**Відносне зростання**
	До навчання	**Після навчання**		
1	52%	89%	37	71.2%
2	43%	72%	29	67.4%
3	64%	95%	31	48.4%
4	58%	78%	20	34.5%
5	62%	100%	38	61.3%

Отже, після впровадження запропонованої навчальної кампанії середній відносний приріст частки правильних відповідей становив 56.6% порівняно з початковим рівнем, що свідчить про суттєве підвищення рівня обізнаності працівників щодо соціоінженерних загроз.

Враховуючи виявлені під час реалізації навчальної програми результати, постає необхідність формулювання низки обґрунтованих рекомендацій, спрямованих на вдосконалення змісту та організаційного наповнення освітнього процесу. Зокрема, доцільним видається поступове ускладнення навчальних матеріалів – особливо тих, що стосуються розпізнавання фішингових повідомлень, адаптованих до внутрішньокорпоративного стилю комунікації. Розширення набору кейсів за рахунок прикладів, які імітують справжні службові листи з мінімальними відхиленнями, дозволить посилити стійкість персоналу до більш витончених атак.

Окремої уваги потребує систематичне оновлення змісту навчальних модулів відповідно до динаміки розвитку соціоінженерних загроз. З урахуванням змін у шаблонах шахрайських повідомлень, включення новітніх прикладів сприятиме підтриманню високої релевантності навчання. Рекомендується також запровадження періодичного повторного тестування з метою не лише контролю ефективності засвоєння матеріалу, а й виявлення окремих категорій співробітників, які потребують додаткової підтримки в опануванні теми.

Зазначені заходи, інтегровані у загальну політику підвищення кібергігієни працівників, забезпечать сталий розвиток культури інформаційної безпеки на рівні організації. У результаті впровадження запропонованих змін навчальна програма з протидії соціальній інженерії набула б не лише гнучкості й адаптивності, а й здатності ефективно реагувати на виклики сучасного цифрового середовища.

Висновки до розділу 3

У розділі представлено результати практичної реалізації та оцінювання ефективності навчальної кампанії, спрямованої на підвищення рівня обізнаності персоналу щодо соціоінженерних загроз. Було здійснено комплексний аналіз вихідного стану кіберобізнаності співробітників, який виявив наявність

критичних прогалин у здатності розпізнавати основні маніпулятивні техніки, зокрема фішингові повідомлення, що імітують внутрішню комунікацію.

На основі ідентифікованих потреб було розроблено структуру та змістове наповнення адаптивної навчальної програми, що враховує рівень підготовки користувачів і специфіку корпоративного середовища. До програми включено різноманітні освітні формати, зокрема інтерактивні кейси, симуляції атак, тестування та мультимедійні матеріали, що дозволило забезпечити високу залученість учасників і покращити запам’ятовування інформації.

Впровадження навчальної програми супроводжувалося експериментальним оцінюванням змін у рівні обізнаності співробітників. Результати аналізу продемонстрували суттєве покращення (на 56.6%) здатності розпізнавати фішингові повідомлення, зменшення кількості критичних помилок, а також формування навичок критичного оцінювання вхідної інформації. Водночас були виявлені зони підвищеної уваги, зокрема труднощі у класифікації складних повідомлень та схильність до хибно-позитивних оцінок.

Узагальнення результатів дозволило сформулювати практичні рекомендації щодо вдосконалення навчальної програми, зокрема: поступове ускладнення навчальних сценаріїв, регулярне оновлення контенту відповідно до новітніх схем атак, періодичне тестування для збереження набутих навичок, а також впровадження механізмів зворотного зв’язку.

Загалом, результати третього розділу підтверджують ефективність інтеграції освітніх технологій у систему управління інформаційною безпекою. Запропоновані підходи сприяють формуванню адаптивної та гнучкої освітньої моделі, що відповідає сучасним викликам цифрового середовища та сприяє зміцненню культури інформаційної безпеки в організації.

ВИСНОВКИ

У ході проведеного дослідження здійснено комплексне вивчення соціальної інженерії як одного з найбільш поширених та ефективних векторів атак у сфері інформаційної безпеки. Встановлено, що успішність таких атак переважно зумовлена експлуатацією поведінкових та психологічних особливостей користувачів, що перетворює людський фактор на найбільш вразливу ланку захисту інформаційних систем. Формалізовано поняття соціальної інженерії та здійснено її класифікацію за ключовими ознаками: каналами реалізації, рівнем ризику, технічними характеристиками та спрямованістю впливу. Це дозволило структурувати основні загрози й визначити техніки, які потребують пріоритетної уваги в рамках заходів захисту.

Проведено критичний аналіз підходів до протидії соціоінженерним атакам, що застосовуються в організаціях різного профілю. З'ясовано, що найбільш ефективними є моделі захисту, які поєднують технічні та організаційно-освітні компоненти. Зокрема, наголошено на важливості розбудови системи підвищення обізнаності персоналу, що базується на сучасних принципах кібергігієни, критичного мислення та практичних навичках розпізнавання загроз. Обґрунтовано, що без впровадження цілісної політики навчання жодна система управління інформаційною безпекою не здатна ефективно протистояти соціоінженерним впливам.

У межах другого розділу розроблено методичну основу навчальної кампанії, спрямованої на протидію соціоінженерним атакам. Визначено принципи побудови навчального процесу – адаптивність, контекстуалізація, поступовість, варіативність подачі матеріалу. Обґрунтовано доцільність використання інтерактивних, гейміфікованих та адаптивних освітніх технологій, які сприяють підвищенню залученості персоналу та кращому засвоєнню навчального матеріалу. Розроблено узагальнену структуру програми з урахуванням різних категорій працівників та запропоновано систему показників для об’єктивного оцінювання її результативності.

Практична реалізація запропонованої навчальної програми в умовах конкретної організації дозволила здійснити експериментальне оцінювання змін рівня обізнаності співробітників. Первинне тестування продемонструвало наявність типових вразливостей – зокрема, труднощів у розпізнаванні фішингових повідомлень та імітованої внутрішньої комунікації. Після завершення навчання було зафіксовано позитивну динаміку: співробітники демонстрували суттєво вищу здатність до виявлення соціоінженерних загроз, а також підвищену обережність у цифровій поведінці. Узагальнення результатів дозволило сформулювати низку рекомендацій щодо вдосконалення та масштабування програми, включаючи регулярне оновлення контенту, ускладнення кейсів, проведення повторного тестування та підтримку зворотного зв’язку.

Отримані результати підтверджують доцільність поєднання науково обґрунтованих підходів до формування навчального контенту з практично орієнтованим впровадженням навчання в реальному корпоративному середовищі. Сформовані рекомендації мають як прикладне значення – для удосконалення внутрішніх політик інформаційної безпеки та програм підготовки персоналу, так і наукове – як підґрунтя для подальших досліджень у сфері поведінкової інформаційної безпеки та моделювання стійкості користувачів до соціоінженерних впливів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бєлєвич В.М. Соціальна інженерія: основні техніки атаки та методи протидії. *Матеріали наук.-практ. конф. Відкритий міжнародний університет розвитку людини «Україна»*, м. Київ, 28–29 березня 2025 р. С. 2–3.

2. Звіт за 2023 рік про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. URL: https://scpc.gov.ua/api/files/9c21855d-74da-45d1-90f9-5d4f6795996a

3. Qishing, або як захиститися від фішингу через QR-коди. *HackYourMom.* URL: https://hackyourmom.com/kibervijna/kvishyng-abo-yak-zahystytysya-vid-fishyngu-cherez-qr-kody/

4. Що таке соціальна інженерія. *Journal.gen.tech.* URL: https://journal.gen.tech/post/sho-take-socialna-ingeneria

5. Франчук В.М. Захист даних. Соціальна інженерія. *Науковий часопис НПУ імені М.П. Драгоманова*. 2015. № 2. С. 20-26. URL: https://vfranchuk.fi.npu.edu.ua/images/files/statty/56.pdf

6. Гринько Л. П. Фішинг як спосіб вчинення шахрайства у мережі Інтернет. *Полтавський правовий часопис.* 2022. № 4. С. 16-29. URL: https://plr.nlu.edu.ua/article/view/287956/285644

7. Lutkevich B., Casey C., Sharon S. Whaling attack (whaling phishing). *TechTarget*. URL: https://www.techtarget.com/searchsecurity/definition/whaling

8. Ваврик Ю.Л., Опірський І.Р. Штучний інтелект: кібербезпека нового покоління. *Ukrainian Scientific Journal of Information Security*. 2024. Том 30, № 2. С. 244-255. URL: https://doi.org/10.18372/2225-5036.30.19235

9. Cloudflare. The phishing implications of AI chatbots. *Cloudflare blog*. URL: https://www.cloudflare.com/ru-ru/the-net/chatgpt-phishing/

10. Сагун А.В. Методи боротьби та попередження атак типу «соціальна інженерія». *Modern research in science and education*: proceedings of III International Scientific and Practical Conference, Chicago, USA, 9-11 November 2023. P. 316-323.

URL:https://scholar.google.com.ua/citations?view_op=view_citation&hl=uk&user=NG7ER34AAAAJ&citation_for_view=NG7ER34AAAAJ:M3ejUd6NZC8C

11. Hadnagy C. Social engineering. The science of human hacking. Indiana: John Wiley & Sons, Inc. 2018. URL: https://theswissbay.ch/pdf/Books/Computer%20science/socialengineering_thescienceofhumanhacking_2ndedition.pdf

12. Threat Landscape: Social Engineering Attacks 2023. *European Union Agency for Cybersecurity (ENISA).* URL: https://www.enisa.europa.eu/publications/threat-landscape-social-engineering-attacks

13. State of the Phish Report. *Proofpoint.* URL: https://www.proofpoint.com/us/resources/threat-reports/state-of-phish

14. Parsons K., McCormac A., Butavicius M., Pattinson M., Jerram C. The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*. 2017. Vol. 66. P. 40-51. URL: https://doi.org/10.1016/j.cose.2017.01.004

15. ДСТУ ISO/IEC TR 15446:2024 Інформаційна технологія. Методи безпеки. Настанови щодо створення профілів захисту та цілей безпеки (ISO/IEC TR 15446:2017, IDT)

16. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. Дата оновлення: 15.11.2024. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

17. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР. Дата оновлення: 20.04.2025. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

18. ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT)

19. ДСТУ ISO/IEC 27002:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки (ISO/IEC 27002:2022, IDT)

20. Reference Incident Classification Taxonomy. *The European Union Agency for Cybersecurity.* URL: https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

21. Яковів І. Кібернетична модель APT атаки. *Information Technology and Security.* 2018. Том 6, № 1. С. 46-58. URL: http://nbuv.gov.ua/UJRN/inftech_2018_6_1_7

22. Капелюшна Т. В. Врахування впливу загроз соціальної інженерії при управлінні безпекою підприємства. *Інвестиції: практика та досвід.* 2023. № 8. С. 125–129. URL: https://doi.org/10.32702/2306-6814.2023.8.125

23. Фалько Н. Соціальна інженерія: зброя масового психологічного впливу в цифрову епоху. *Науково-інформаційний супровід професійної підготовки фахівців в умовах невизначеності:* тези наук.-практ. семінару з міжнародною участю, м. Миколаїв, 25 квітня 2024 р. С. 171–177. URL: https://dspace.chmnu.edu.ua/jspui/bitstream/123456789/2630/1/Наук.-інформ.%20супровід%20професс.%20підготовки%20фахівців%20в%20умовах%20невизначеності.pdf#page=171

24. Неклеса О. М. Особливості прояву схильності до маніпуляції у межах професійної діяльності. *Практична психологія у сучасному вимірі:* матеріали XV Міжнар наук.-практ. конф. науковців та студентів, м. Дніпро, 26 березня 2024 р. С. 202–202. https://duan.edu.ua/wp-content/uploads/2024/04/3birnyk-2024-psykholohy_.pdf#page=202

25. Селіванова А. В., Левитський Ю. О. Дослідження методів соціальної інженерії. Частина І. Вплив на здоров'я людини. *Automation Technological and Business Processes*. 2022. № 14 (2). С. 56-62. URL: https://doi.org/10.15673/atbp.v14i2.2334

26. Мохор В., Цуркан О. Негативний інформаційно-психологічний вплив на індивідуальну свідомість за соціоінженерним підходом. *Collection "Information Technology and Security"*. № 5 (2). С. 13-19. URL: https://doi.org/10.20535/2411-1031.2017.5.2.136929

27. Атаманчук П. С., Мендерецький В. В., Панчук О. П. Чорна О. Г. Безпека життєдіяльності. Навч. посіб. – К.: Центр учбової літератури, 2011. – 276 с. URL: https://shron1.chtyvo.org.ua/Atamanchuk_Petro/Bezpeka_zhyttiediialnosti.pdf?PHPSESSID=734f9bugtnovloqs7hbqph8go1

28. Психологія професійної безпеки: технології конструктивного самозбереження особистості : кол. моногр. / О. Лазорко, Ж. Вірна, Л. Акімова [та ін.] ; за заг. ред. Ж. Вірної. – Луцьк : Вежа-Друк, 2015. – 588 с. URL: https://pedagogy.lnu.edu.ua/wp-content/uploads/2016/09/monografiya_luck_2015.pdf

29. Бурячок В.Л., Грищук Р.В., Хорошко В.О. Політика інформаційної безпеки: підручник. В. Л. Бурячок, Р. В. Грищук, В. О. Хорошко / За заг. ред. докт. техн. наук, проф. В.О. Хорошка. К. : ПВП «Задруга», 2014. - 222 с. URL: http://library.hneu.edu.ua/storage/new-arrivals-books/February2021/politics.pdf

30. Микитенко В. І., Черненко О. О. Соціальна інженерія як інструмент кібер атак: виклики та протидія // ІТ-простір сьогодення: тенденції, інновації та перспективи розвитку : зб. тез доп. Всеукр. наук.-практ. студ. конф., м. Харків – 2024. – С. 47–48.

31. Безпека інформації : конспект лекцій / укладач О. С. Кушнерьов. – Суми: Сумський державний університет, 2021. – 99 с. URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/85989/3/Kushnerov.pdf

32. Жмурко О. Соціальна інженерія як загроза кібербезпеці: методи запобігання та захисту. *Педагогіка безпеки.* 2024. Том 9, № 1. С. 37-42. URL: https://doi.org/10.31649/2524-1079-2024-9-1-037-042

33. Собчук В. В., Лаптєв О. А. Метод захисту даних наукових досліджень від атак за допомогою алгоритмів соціальної інженерії. *Третій рівень освіти в Україні: становлення та тенденції :* матеріали VI Міжнар. наук.-практ. конф., с. Світязь, 20 листопада 2022 р. С. 106-114. – Режим доступу: https://files.znu.edu.ua/files/Bibliobooks/Inshi68/0050141.pdf#page=106

34. Староста В. Технології інтерактивного навчання: сутність, класифікація. *Педагогічні науки.* 2019. № 1 (64). С. 232-236. URL:

https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/29610/1/2019_Starosta%20Volodymyr_Nauk_visnik%20ped%201%2864%292019%20s.230-237.pdf

35. Крамаренко І. С., Галегова О. В. Інноваційні підходи до навчання в умовах воєнного стану. *Проблеми сучасних трансформацій. Серія: Педагогіка та психологія*. 2024. № 5. С. 3. URL: https://doi.org/10.54929/2786-9199-2024-5-06-01

36. Харламова Л.Д. Адаптивне навчання та засоби його реалізації *Особистісно-професійна компетентність педагога: теорія і практика:* матеріали Всеукр. наук.-практ. конф., м. Суми, 30 березня 2023 р. С. 185-188. URL: https://www.soippo.edu.ua/images/Конференції_Проекти_Гранти/Конференції/2023/30.03.2023%20ЗБІРНИК.pdf#page=185

37. Саган О. В. Гейміфікація як сучасний освітній тренд. *Збірник наукових праць*. 2022. № 100. С. 12-18. URL: https://doi.org/10.32999/ksu2413-1865/2022-100-2

38. Семененко Ю. Роль KPI та OKR в ефективності діяльності компанії *Вісник Хмельницького національного університету. Серія: Економічні науки*. 2023. Том 324, № 6. С. 227–235. URL https://doi.org/10.31891/2307-5740-2023-324-6-37

39. Цалко Т. Р., Невмержицька С. М. Система ключових показників ефективності як запорука ефективного управління бізнес-процесами в компанії. *Проблеми системного підходу в економіці*. 2019. № 6 (74). С. 160-167. URL: https://er.knutd.edu.ua/handle/123456789/14888

40. Цюцюра С. В., Криворучко О., Цюцюра М. І. Ключові показники ефективності. Принципи розробки ключових показників для бюджетної сфери. *Управління розвитком складних систем*. 2012. № 10. С. 87-91. URL: http://nbuv.gov.ua/UJRN/Urss_2012_10_173

41. Кошельок Г., Чаплинська О. Ключові показники ефективності. *Трансформація економіки та права в умовах системних реформ України*: матеріали Всеукр. наук.-практ. конф., м. Одеса, 27 жовтня 2017 р.

42. Ушкальов В.В. Особливості оцінки ефективності процесу розвитку персоналу. *Економіка та управління підприємствами*. 2018. № 23. С. 326-329. URL: http://global-national.in.ua/archive/23-2018/64.pdf

43. Гавкалова, Н. Л. Управління ефективністю менеджменту персоналу : монографія / Н. Л. Гавкалова, Т. А. Власенко. – Харків : Вид. ХНЕУ, 2011. – 296 с.

44. Kirkpatrick, D. I. Evaluating training programs / D. I. Kirkpatrick. – San Francisco : Berret-Koehler, 2006. – XVII, 379 p.

45. Phillips, J. J. Handbook of training evaluation and measurement methods / J. J. Phillips. – Houston : Gulf Pub. Co., Book Division, 1983. – XI, 316 p. URL: https://api.pageplace.de/preview/DT0400.9781317632566_A26861078/preview-9781317632566_A26861078.pdf

46. Кальченко В. В. Огляд методів проведення тестування на проникнення для оцінки захищеності комп'ютерних систем. Системи управління, навігації та зв'язку. 2018. Том 4, № 50. С. 109-114. URL: https://doi.org/10.26906/SUNZ.2018.4.109

47. Стефінко Я.Я. Використання відкритих операційних систем для тестування на проникнення в навчальних цілях. *Вісник Національного університету «Львівська політехніка». Комп'ютерні системи та мережі*. 2014. № 806. С. 258–263. URL: http://nbuv.gov.ua/UJRN/VNULPKSM_2014_806_41