Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«КИЄВО-МОГИЛЯНСЬКА АКАДЕМІЯ»

Кафедра інформатики факультету інформатики

Методи протидії використанню соціальної інженерії в кіберпросторі

Текстова частина до курсової роботи
за спеціальністю 122 “Комп’ютерні науки”

Керівник курсової роботи
Кандидат технічних наук, доцентка
Савченко Т.В.
(підпис)
“____” _____ 2025 р.

Виконала
студентка 3 року навчання
Немилостива П.В.
“____” _____ 2025 р.

Київ – 2025

Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«КИЄВО-МОГИЛЯНСЬКА АКАДЕМІЯ»

Кафедра інформатики факультету інформатики

ЗАТВЕРДЖУЮ
Зав. кафедри інформатики,
доцент, кандидат наук
С.С. Гороховський
_____
(підпис)

“ ” _____ 2025 р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ
на курсову роботу

студентці 3 року навчання факультету інформатики
Немилостивій Поліні Валентинівні
ТЕМА “Методи протидії використанню соціальної інженерії в кіберпросторі”

Зміст ТЧ до курсової роботи:

Вступ
1. Аналіз наукових досліджень у сфері протидії соціальній інженерії
2. Теоретична розробка засобів протидії соціальній інженерії
3. Практична реалізація запропонованих заходів
Висновки
Перелік літератури
Додаток

Дата видачі “ ” _____ 2025 р. Керівниця _____
(підпис)
Завдання отримала _____
(підпис)

Календарний план виконання курсової роботи

Тема: Методи протидії використанню соціальної інженерії в кіберпросторі

№п/п	Назва етапу курсової роботи	Термін виконання	Примітка
1.	Отримання завдання на курсову роботу	06.10.2024	
2.	Формування структури курсової роботи та затвердження теми	18.10.2024	
3.	Пошук і систематизація джерел за темою	14.02.2025	
4.	Написання теоретичної частини курсової роботи	10.03.2025	
5.	Реалізація програмного інструменту на мові C++	22.03.2025	
6.	Надання курсової роботи науковій керівниці для перевірки	14.04.2025	
7.	Внесення правок відповідно до зауважень керівниці	03.05.2025	
8.	Створення презентації	13.05.2025	
9.	Захист курсової роботи	15.05.2025	

“16” жовтня 2025 р.

Студентка Немилостива П.В. _____
Керівниця доц. Савченко Т.В. _____

ЗМІСТ

АНОТАЦІЯ 5
ВСТУП 6
РОЗДІЛ 1. АНАЛІЗ НАУКОВИХ ДОСЛІДЖЕНЬ У СФЕРІ ПРОТИДІЇ СОЦІАЛЬНІЙ ІНЖЕНЕРІЇ 8
1.1. Аналіз поняття соціальної інженерії та її ролі в кіберпросторі 8
1.2. Класифікація методів атак соціальної інженерії 24
1.3. Проблемні аспекти існуючих досліджень та їх недоліки 32
1.4. Пропозиції щодо напрямків подальших досліджень 33
РОЗДІЛ 2. ТЕОРЕТИЧНА РОЗРОБКА ЗАСОБІВ ПРОТИДІЇ СОЦІАЛЬНІЙ ІНЖЕНЕРІЇ 36
2.1. Постановка завдання: мета та завдання власних досліджень 36
2.2. Розробка теоретичної моделі реагування на загрози соціальної інженерії 38
2.3. Опис алгоритмів для навчання користувачів протидії атакам 41
РОЗДІЛ 3. ПРАКТИЧНА РЕАЛІЗАЦІЯ ЗАПРОПОНОВАНИХ ЗАХОДІВ 48
3.1. Створення програмного інструмента для навчання користувачів 48
3.2. Реалізація консольного додатка на C++ 48
3.3. Тестування програмного інструмента та його застосування у різних сценаріях 49
ВИСНОВКИ 53
ПЕРЕЛІК ЛІТЕРАТУРИ 55
ДОДАТОК 57

АНОТАЦІЯ

Курсова робота присвячена дослідженню методів протидії використанню соціальної інженерії в кіберпросторі. У роботі проаналізовано сучасні типи соціально-інженерних атак, їхню класифікацію та особливості впливу на інформаційну безпеку. На основі виявлених вразливостей було розроблено теоретичну модель реагування на соціально-інженерні загрози, а також алгоритми підвищення обізнаності користувачів. Для перевірки практичної ефективності запропонованих рішень створено програмний інструмент на мові C++, який імітує типові сценарії атак і забезпечує інтерактивне навчання користувача. Запропоновані підходи орієнтовані на зниження рівня успішності фішингових, вішингових та інших психологічно-орієнтованих атак за рахунок профілактики людського фактору.

ВСТУП

З ростом цифрової взаємодії та переходом до онлайн-комунікацій, коли технології проникають у всі сфери життя, питання кібербезпеки набуває все більшого значення. Використання психологічних маніпуляцій для обману людей і отримання доступу до конфіденційної інформації, часто через фішингові листи, вішингові дзвінки та інші шахрайські методи, є постійною проблемою для організацій та індивідуальних користувачів. Науковці, зокрема, фахівці в галузі кібербезпеки та психології, активно досліджують методи боротьби з такими атаками, проте результати не завжди встигають за швидкими темпами розвитку технологій та еволюцією методів атак. Тому вирішення цієї проблеми є критично важливим для забезпечення безпеки і стабільності сучасного цифрового середовища, а дослідження методів протидії соціальній інженерії в кіберпросторі є надзвичайно актуальним для захисту інформаційних систем та особистих даних.

Основною метою цього дослідження є розробка ефективних методів протидії соціальній інженерії в кіберпросторі. Для досягнення цієї мети необхідно виконати наступні завдання:

1. Проаналізувати основні методи соціальної інженерії, що використовуються в кіберзлочинності.
2. Дослідити наявні методи захисту від атак соціальної інженерії.
3. Оцінити ефективність сучасних засобів протидії соціальній інженерії в контексті інформаційної безпеки.
4. Розробити рекомендації для покращення захисту користувачів від таких атак.

Об’єкт дослідження: процес захисту інформаційних систем від атак, заснованих на соціальній інженерії.

Для проведення дослідження будуть використані методи аналізу літературних джерел, порівняння існуючих методів захисту, експертні оцінки

та практичні кейси для оцінки ефективності заходів протидії соціальній інженерії.

Джерела дослідження: аналіз базуватиметься на наукових статтях, книгах з інформаційної безпеки, звітах з кіберзлочинності, інтернет-ресурсах, форумах і блогах, що висвітлюють нові тенденції в кіберзагрозах, а також практичних прикладах соціальної інженерії.

Наукова новизна одержаних результатів: розробка рекомендацій щодо підвищення обізнаності користувачів та застосування сучасних технологій захисту для ефективної протидії соціальній інженерії. Оцінка ключових факторів, що сприяють успішним атакам, і пропозиція нових методів боротьби з ними.

Практичне значення одержаних результатів: результати дослідження можуть бути використані при розробці інструментів для підвищення безпеки інформаційних систем, у навчальних програмах для підвищення обізнаності користувачів, а також для створення політик безпеки в організаціях, що допоможуть знизити ризик успішних атак за допомогою соціальної інженерії.

РОЗДІЛ 1. АНАЛІЗ НАУКОВИХ ДОСЛІДЖЕНЬ У СФЕРІ ПРОТИДІЇ СОЦІАЛЬНІЙ ІНЖЕНЕРІЇ

1.1. Аналіз поняття соціальної інженерії та її ролі в кіберпросторі

Сфера кібербезпеки в умовах сучасних глобальних змін стикається з дедалі складнішими викликами, які виникають унаслідок швидкої еволюції технологій та зміни геополітичних і геоекономічних обставин. Водночас ці зміни викликають нові загрози, зокрема, в кіберпросторі, де постійно виникають нові методи атак та активізуються нові учасники на світовій арені. Ці учасники можуть застосовувати як традиційні, добре відомі тактики, так і новітні, які використовуються для досягнення своїх стратегічних цілей, зокрема, у політичній, економічній або військовій сферах.

Одним із найбільш важливих аспектів у сучасному контексті є співпраця між державами, організаціями та приватними підприємствами на інтегрованих платформах. Такі платформи дозволяють забезпечити взаємодію між різними учасниками у сфері кібербезпеки, що, в свою чергу, сприяє досягненню важливих політичних або економічних цілей. Спільні зусилля можуть допомогти протистояти складним і динамічним загрозам, які з’являються внаслідок використання кіберзброї для ведення війни або інших стратегічних цілей.

З огляду на цю ситуацію, постійний моніторинг та оцінка кіберзагроз стають необхідними завданнями для всіх організацій і держав, щоб своєчасно виявляти нові загрози та запобігати можливим атакам. Постійний аналіз ситуації в кіберпросторі, а також швидке реагування на нові тенденції є важливим елементом для ефективного управління ризиками. Інноваційним драйвером розвитку кіберзагроз стають геостратегічні амбіції глобальних акторів, які часто включають використання нових технологій для досягнення своїх цілей.

Зокрема, дезінформація, шпигунство та навіть підривні операції можуть бути використані як інструменти для підриву стабільності державних і економічних систем, що ставить під загрозу не тільки національну безпеку, а

й цивільне життя. Використання кіберпростору для таких цілей впливає на правову сферу, порушуючи міжнародні угоди та нормативно-правові акти. Це вимагає від держав і організацій постійного вдосконалення своїх стратегій кіберзахисту та надання більшої уваги розробці комплексних систем безпеки, здатних оперативно реагувати на нові загрози [1].

Окрім цього, кіберзагрози починають набирати глобальних масштабів, що ускладнює боротьбу з ними. Кожен новий кіберінцидент може мати далекі наслідки для економік країн, їхніх державних структур та суспільств загалом. Тому міжнародна співпраця, створення спільних платформ для обміну інформацією та технологіями між державами, а також між державними і приватними установами, є важливим фактором у протидії кіберзагрозам.

У світлі зростаючих геополітичних напружень і швидких технологічних змін кіберзагрози набувають нових форм, які вимагають від країн і організацій вдосконалення своїх підходів до кіберзахисту. Дезінформація, яка поширюється через кіберпростір, стає потужним інструментом для маніпулювання громадською думкою, дискредитації політичних лідерів, а також для створення соціальних і політичних конфліктів. Це створює додаткову небезпеку для демократичних процесів, виборчих систем і громадської безпеки. Зокрема, зловмисники можуть активно впливати на електоральні процеси, маніпулюючи виборчими результатами, що ставить під загрозу саму основу демократичних інститутів.

Крім того, в умовах глобалізації та взаємозв’язку світових економік кіберзагрози мають тенденцію до транснаціонального характеру. Атаки можуть бути здійснені з будь-якої точки світу, що значно ускладнює ідентифікацію та нейтралізацію зловмисників. Важливим елементом у цій ситуації є розвиток міжурядових угод і партнерств між різними державами для боротьби з кіберзлочинністю та тероризмом. Зокрема, країни повинні об'єднувати свої зусилля для розробки спільних стандартів кібербезпеки та обміну інформацією, що дозволить створити ефективну систему протидії кіберзагрозам на глобальному рівні.

У свою чергу, технології, які використовуються для здійснення атак у кіберпросторі, постійно вдосконалюються. Зокрема, штучний інтелект і машинне навчання все більше інтегруються в методи кібернападів, дозволяючи створювати більш складні і швидко адаптовані атаки, що може ускладнити їх виявлення та відбиття. Крім того, зловмисники можуть використовувати новітні технології для автоматизації атак, що дозволяє їм вчиняти напади в масштабах, які раніше були недосяжними. Це також створює додаткові виклики для організацій та урядів, які повинні оновлювати свої методи захисту, забезпечуючи швидке виявлення і нейтралізацію таких атак.

Крім боротьби з кіберзагрозами, важливо також вживати заходів щодо зниження їхнього потенційного впливу на критичні інфраструктури. Інфраструктури, які забезпечують життєво важливі послуги, такі як енергетичні системи, системи водопостачання, транспорт та фінансові установи, повинні бути особливо захищені від кібернападів. У разі успішного нападу на такі об'єкти можуть виникнути значні економічні втрати, соціальна нестабільність і навіть загроза життю громадян.

Підвищення рівня кібербезпеки вимагає інтеграції передових технологій захисту, включаючи засоби для виявлення, реагування та запобігання загрозам, таких як розширене виявлення та реагування (XDR), а також застосування новітніх методів, що базуються на штучному інтелекті та аналітиці великих даних. Такі технології дозволяють швидше реагувати на атаки, оптимізувати процеси захисту та підвищувати ефективність боротьби з кіберзагрозами.

Особливу тривогу викликає стрімка еволюція програм-вимагачів, які набувають більш складної структури та функціональності, розширюються за масштабом, оскільки зусилля з їх створення об'єднуються в рамках прихованих форумів [2]. Це ускладнює виявлення загроз, вимагаючи від інструментів безпеки більшої унікальності. Проблема захисту кіберпростору стає все більш актуальною в умовах швидкого розвитку інформаційних технологій і інтеграції платформ з різних сфер діяльності, а також через

зацікавленість сторонніх осіб у порушенні захисту конфіденційної інформації з політичних або економічних мотивів. Це підштовхує компанії в сфері кібербезпеки до пошуку нових способів захисту та розробки технологій для протистояння сучасним кібервикликам.

Для забезпечення стабільного та ефективного функціонування інформаційних систем необхідний надійний захист від кібератак, які здійснюються з боку зловмисників. Враховуючи зростання та еволюцію кіберзагроз, організаціям важливо регулярно здійснювати моніторинг новітніх технологічних рішень у сфері кібербезпеки, як на міжнародному рівні, так і в межах національних стратегій і ініціатив. Такий моніторинг дозволяє об'єктивно оцінювати поточний стан інформаційної безпеки, виявляти потенційні вразливості та розробляти плани щодо їх усунення. В умовах стрімкого розвитку кіберзагроз та появи нових методів атак, цей процес стає надзвичайно важливим для успішної протидії сучасним загрозам.

Безперервний аналіз сучасних рішень та тенденцій у кібербезпеці дозволяє своєчасно впроваджувати інноваційні технології, такі як Endpoint Detection and Response (EDR), які допомагають виявляти та реагувати на атаки на кінцеві точки. Багато наукових досліджень і публікацій рекомендують впровадження таких передових технологій для ефективного захисту інформаційних систем від різноманітних кіберзагроз [3]. Проте досягнення належного рівня безпеки вимагає не лише застосування вже розроблених рішень, але й детального вивчення глибинних причин виникнення загроз, аналізу нових методів їх подолання, а також дослідження особливостей інформаційного контенту, який може сприяти формуванню ефективних стратегій кіберзахисту [4].

Забезпечення ефективного кіберзахисту вимагає від організацій не тільки впровадження новітніх технологій, а й розробки динамічних, адаптивних стратегій безпеки, що враховують постійно змінювані умови кіберзагроз. Зокрема, важливою складовою цих стратегій є регулярний аналіз поведінки загроз і потенційних вразливостей, а також зниження часу реакції

на атаки через автоматизацію виявлення та реагування. Системи безпеки, які спираються на машинне навчання і штучний інтелект, можуть значно поліпшити здатність виявляти аномалії та запобігати атакам ще до того, як вони будуть здійснені, що дозволяє організаціям оперативно реагувати на нові загрози.

Одним із важливих аспектів є інтеграція різних елементів кіберзахисту на рівні організації: системи виявлення загроз, антивірусні програми, захист кінцевих точок, моніторинг мереж і поведінки користувачів повинні працювати в єдиній скоординованій системі. Оскільки кіберзлочинці часто використовують комплексні стратегії для обходу традиційних засобів захисту, важливо мати багаторівневий підхід до безпеки, який зможе адаптуватися до нових типів атак. Використання технологій, таких як інтегроване виявлення і реагування (XDR), дозволяє зібрати дані з різних джерел, таких як кінцеві точки, мережі, хмарні сервіси та інші компоненти, що дає змогу отримати повну картину загроз і своєчасно вжити необхідних заходів.

Крім того, важливим є розвиток культурної складової кібербезпеки в межах організації. Успішний захист від кіберзагроз неможливий без обізнаності співробітників, оскільки навіть найсучасніші технології не зможуть повністю захистити систему, якщо самі користувачі організації не дотримуються базових правил безпеки, таких як створення складних паролів, перевірка підозрілих електронних листів або відмова від використання невідомих пристроїв у корпоративних мережах. Регулярне навчання співробітників і тренування на основі реальних сценаріїв дозволяють формувати необхідну кіберкультуру, що значно знижує ймовірність успіху атак, заснованих на соціальній інженерії.

Таким чином, для ефективного кіберзахисту необхідно поєднувати передові технології з постійною адаптацією до змінюваного кіберсередовища, комплексними стратегіями безпеки, підвищенням обізнаності користувачів та ефективним управлінням ризиками. Тільки в такому випадку можна забезпечити надійний захист від новітніх кіберзагроз і забезпечити

стабільність та безпеку інформаційних систем у сучасному цифровому середовищі.

Наразі важливо не лише застосовувати технології захисту, але й постійно адаптувати стратегії безпеки відповідно до нових викликів, які з’являються через інновації у сфері кіберзлочинності. Це передбачає не тільки технічне оновлення систем безпеки, а й інтеграцію більш комплексних підходів до управління ризиками, таких як аналіз поведінки користувачів, вивчення патернів атак і інтеграція штучного інтелекту для покращення виявлення аномалій. Таким чином, для забезпечення високого рівня захисту інформаційних систем необхідний комплексний підхід, що включає використання передових технологій, моніторинг новітніх загроз і постійну адаптацію до змінюваного цифрового середовища.

Цифровізація охоплює всі сфери сучасного суспільства, включаючи політику, економіку, медицину та освіту. З цієї причини питання управління якістю цифрових процесів та забезпечення безпеки кіберпростору стає все більш актуальним. Зі стрімким розвитком технологій і зростаючим використанням цифрових рішень в усіх галузях постійно з'являються нові загрози, які потребують комплексного та ефективного управління. В рамках цього дослідження було застосовано кілька наукових підходів, що дозволили сформулювати основні принципи системного підходу до оцінки загроз інформаційній безпеці. Метою цих підходів є своєчасне визначення ефективних інструментів для захисту кіберпростору організацій і підприємств.

Методологічною основою дослідження стали дані щорічних і щомісячних моніторингових досліджень, що проводяться провідними рейтинговими агентствами і комерційними компаніями, які спеціалізуються на кібербезпеці. Окрім того, авторське компаративне дослідження допомогло визначити основних лідерів на ринку кібербезпеки та підтвердити теоретичні припущення щодо особливостей застосування різних засобів і методів захисту організацій [5].

Експерти з кібербезпеки, зокрема, команда Trellix Advanced Research Center, надали прогнози щодо нових тенденцій, тактик і загроз, які організаціям слід враховувати у 2024 році. Ось деякі з них:

1. Загроза з боку штучного інтелекту (ШІ):

- Небезпека використання шкідливих великих мовних моделей (LLM) для кібератак.
- Воскресіння "Script Kiddies", які використовують доступне безкоштовне програмне забезпечення для автоматизації атак.
- Зловживання ШІ для шахрайства, зокрема, у сфері голосових атак в соціальній інженерії.

2. Зміни в поведінці суб'єктів загрози:

- Атаки на ланцюги постачання з використанням рішень керованої передачі файлів.
- Розвиток шкідливого програмного забезпечення, яке підтримує різні операційні системи, що ускладнює його виявлення та нейтралізацію.

3. Нові виникаючі загрози та методи атак:

- Інсайдерські загрози стають більш непомітними, їх важче виявити на ранніх етапах.
- Активізація використання QR-кодів у фішингових атаках.
- Атаки на периферійні пристрої та нові вектори атак, наприклад, використання Python у середовищі Excel [6].
- Зміна механізмів захисту завдяки новим методам, таким як драйвера LOL, що можуть ускладнити традиційні методи захисту від атак.

Завдяки цьому дослідженню стає можливим вироблення обґрунтованих стратегій кіберзахисту, що дозволяють організаціям своєчасно реагувати на новітні загрози і зберігати цілісність своїх інформаційних систем.

Одним із важливих досягнень у сфері ШІ є розробка великих мовних моделей (LLM), які можуть не лише генерувати текст для корисних застосувань, але й стати інструментом для зловмисних цілей, наприклад, для створення фішингових кампаній за допомогою FraudGPT і WormGPT.

Застосування таких моделей дозволяє створювати масштабні фішингові атаки без необхідності великого досвіду.

З появою доступних інструментів для автоматизованих атак, як-от ChatGPT, Bard або Perplexity AI, зловмисники можуть створювати шкідливий код, фальшиві відео та здійснювати соціальну інженерію [7]. Однак варто зазначити, що інструменти штучного інтелекту, такі як ChatGPT, Bard, мають вбудовані механізми безпеки, які запобігають написанню шкідливого коду.

QR-коди стали одним із популярних інструментів фішингових атак, зокрема, після пандемії COVID-19, коли безконтактні платежі та інші дії, що потребують сканування QR-кодів, стали поширеними. Невідомі або підозрілі QR-коди можуть призвести до серйозних наслідків, тому користувачам слід бути обережними при їх використанні.

Таким чином, організаціям необхідно ретельно підходити до вибору рішень для керованої передачі файлів, запроваджувати політики захисту даних, такі як DLP, і шифрувати конфіденційну інформацію для забезпечення високого рівня кібербезпеки.

Ландшафт загроз у кібербезпеці поступово зосереджується на вразливостях периферійних пристроїв, зокрема, таких, як брандмауери, маршрутизатори, VPN, комутатори, мультиплексори та шлюзи, які не завжди здатні виявляти вторгнення. Шлюзи, які мають бути першою і останньою лінією захисту, водночас стають як мішенню для атак, так і своєрідною «сліпою зоною», через їхню архітектурну складність. Це вказує на необхідність більш детального вивчення вразливостей у таких компонентах, що в свою чергу зумовлює потребу в розробці нових інструментів для захисту кіберпростору організацій. Такі аспекти безпеки, як надійність шлюзів, маршрутизаторів і VPN, стають все більш важливими для забезпечення безпеки на всіх етапах роботи з даними.

З іншого боку, вразливі драйвери, які використовуються для зламування засобів безпеки на ранніх стадіях атак, стають серйозною загрозою. Наприклад, через використання сертифікованих драйверів зловмисники

можуть отримати привілеї ядра системи, що дозволяє їм отримувати максимальний доступ до системних ресурсів і маніпулювати ними. Прикладом таких атак є використання інструментів, таких як ZeroMemoryEx Blackout, The Terminator від Spyboy і AuKill, які застосовують вразливі драйвери для обходу заходів контролю безпеки та виконання шкідливого коду. У відповідь на ці загрози, великі компанії, зокрема Microsoft, вже впровадили інструменти для захисту від таких атак, зокрема списки вразливих драйверів та проекти, спрямовані на мінімізацію ризиків [8].

Аналіз безпеки кінцевих точок (Endpoint Protection Platform, EPP) є одним з основних напрямків у боротьбі з сучасними кіберзагрозами, адже з кожним роком ці загрози стають все складнішими і масштабнішими. Захист кінцевих точок, таких як персональні комп'ютери, сервери, мобільні пристрої, а також будь-які інші пристрої, що підключаються до корпоративних мереж, є надзвичайно важливим елементом забезпечення кібербезпеки. Ці пристрої є точками входу для багатьох кібератак, тому їх захист є критично важливим для запобігання широкому спектру загроз — від шкідливого програмного забезпечення до атак на рівні мережі.

Встановлення спеціалізованих агентів або датчиків безпеки на кінцевих точках дозволяє забезпечити раннє виявлення загроз і швидко реагувати на потенційні інциденти. Платформи EPP здатні автоматично виявляти, досліджувати і реагувати на інциденти, що дозволяє організаціям миттєво вжити заходів для нейтралізації загроз та мінімізації потенційних збитків. Це дозволяє значно знизити ризик успішних атак і забезпечити більш ефективний захист критично важливих даних і систем.

Не менш важливим компонентом сучасної стратегії кібербезпеки є інтеграція технологій виявлення та реагування на кінцеві точки (Endpoint Detection and Response, EDR). Це рішення дозволяє організаціям ще ефективніше боротися з кіберзагрозами, забезпечуючи комплексний захист на всіх рівнях інфраструктури. Технології EDR допомагають виявляти навіть найскладніші загрози, включаючи ті, що використовують нові методи обходу

традиційних засобів захисту, і дозволяють швидко реагувати на інциденти в реальному часі.

До 2025 року очікується, що близько 80% компаній типу C почнуть активно застосовувати послуги керованого виявлення та реагування (MDR). Це дозволить не лише знизити потенційні ризики, але й значно покращити рівень захисту завдяки інтеграції передових технологій і досвідченому моніторингу з боку експертів. Послуги MDR надають організаціям можливість використовувати найсучасніші інструменти для виявлення та нейтралізації загроз, без необхідності створювати власну команду кібербезпеки, що дозволяє зекономити ресурси та підвищити ефективність реагування на кіберзагрози.

Більше 50% компаній типу B планують інтегрувати рішення EDR у свій портфель постачальників безпеки, що дозволить оптимізувати їхні операційні процеси та підвищити рівень захисту від кіберзагроз. Інтеграція таких рішень допоможе компаніям не лише запобігати атакам, але й ефективно знижувати час реагування на інциденти, що є важливим аспектом при захисті від швидко еволюціонуючих загроз у кіберпросторі.

Таким чином, використання передових технологій EPP і EDR є важливими кроками для забезпечення надійного і комплексного захисту кінцевих точок, що дозволяє організаціям оперативно реагувати на кіберзагрози і значно знижувати рівень ризиків.

Зважаючи на швидкий розвиток кіберзагроз і зростаючий рівень складності атак, інтеграція технологій EPP та EDR стає не лише необхідністю, а й стратегією для досягнення стійкості інформаційних систем. Вони забезпечують багаторівневий захист, що охоплює не тільки відомі загрози, а й нові, раніше невідомі методи атак, включаючи ті, що використовують штучний інтелект для автоматизації атак чи маніпулювання поведінкою користувачів.

Для організацій, які використовують передові технології EPP і EDR, важливо також звертати увагу на інтеграцію таких рішень у їхню загальну

стратегію управління кібербезпекою. Це дозволяє не лише забезпечити належний захист кінцевих точок, а й інтегрувати їх в єдину інфраструктуру безпеки, де дані з різних джерел можуть бути синхронізовані для кращого виявлення та управління загрозами. Це дозволяє забезпечити більш ефективну оборону від атак, які можуть проникати через традиційні системи безпеки.

Що також важливо, зростаюча популярність керованих послуг MDR (Managed Detection and Response) стає важливим фактором для малих та середніх підприємств, які не мають змоги інвестувати в повноцінні внутрішні команди кібербезпеки. Використання послуг MDR дозволяє отримати доступ до передових інструментів і технологій без необхідності великих витрат на їх розробку та впровадження. Це значно знижує витрати на підтримку безпеки, але при цьому дає змогу мати високий рівень захисту, відповідно до останніх стандартів кібербезпеки.

Інтеграція рішень EPP та EDR також дозволяє організаціям краще відповідати на нові виклики, пов'язані з роботою в хмарних середовищах та з використанням мобільних пристроїв. Зокрема, захист таких точок доступу стає важливим у випадках, коли співробітники працюють з дому або мають доступ до корпоративних систем через несанкціоновані пристрої. Технології EDR здатні виявляти та реагувати на аномалії в поведінці користувачів, навіть коли ті використовують зовнішні мережі або працюють поза корпоративною мережею, що надає додаткову безпеку в умовах змішаної або віддаленої роботи.

Оскільки кіберзлочинці постійно вдосконалюють свої методи та використовують нові тактики, організаціям необхідно не лише впроваджувати сучасні технології для захисту кінцевих точок, а й постійно оновлювати свої стратегії реагування на загрози. Це включає регулярне навчання персоналу, проведення тестів на стійкість систем до кібернападів, а також активну співпрацю з постачальниками послуг безпеки для швидкого виявлення та нейтралізації загроз.

Для досягнення належного рівня кіберзахисту організації мають приймати комплексний підхід до вибору і впровадження технологій, інтегруючи рішення EPP та EDR у свою загальну стратегію безпеки. Це дозволяє забезпечити захист не тільки на рівні кінцевих точок, а й на всіх етапах корпоративної інфраструктури, що знижує ризики і підвищує ефективність захисту від складних і постійно змінюваних кіберзагроз.

Дослідження, проведене американською аналітичною компанією Gartner, стало важливим інструментом для оцінки основних постачальників рішень у сфері кібербезпеки. Окрім того, було створено так званий «магічний квадрант», який дозволяє здійснити чітке поділення постачальників на чотири категорії: «лідери», «претенденти», «провидці» та «нішеві гравці». Під категорією «лідери» розуміються компанії, які займають провідні позиції на ринку, демонструючи високі оцінки як за «повноту бачення», так і за «здатність реалізації». Ці компанії задають основні технологічні тренди та визначають напрямки розвитку індустрії кібербезпеки.

Натомість, постачальники в категорії «претенденти» активно впроваджують інноваційні технології та продовжують вдосконалювати свої рішення в різних сферах, зокрема в захисті кінцевих точок. Ці компанії, хоча й не є лідерами на ринку, мають великий потенціал для зростання та розвитку нових рішень.

Серед компаній, які займають високі позиції в категорії «лідери» у «магічному квадранті» за версією Gartner, варто відзначити таких глобальних гравців, як Microsoft, CrowdStrike, SentinelOne та Cybereason. Ці компанії пропонують передові технології та рішення для забезпечення безпеки кінцевих точок і є основними постачальниками інновацій у галузі кіберзахисту. Вони активно розвивають і вдосконалюють свої платформи, що дозволяє їм залишатися на передовій боротьби з кіберзагрозами, встановлюючи нові стандарти в індустрії.

Загалом, забезпечення безпеки кіберпростору вимагає застосування комплексного підходу, що включає в себе як вдосконалення захисту

периферійних пристроїв, так і інтеграцію технологій виявлення та реагування на кінцеві точки в загальну стратегію безпеки організацій. Це дозволить створити багаторівневу систему захисту, здатну ефективно реагувати на новітні кіберзагрози.

«Магічний квадрант» від Gartner є важливою аналітичною платформою для оцінки постачальників рішень у галузі кібербезпеки, зокрема для XDR (розширене виявлення та реагування). Цей квадрант дозволяє здійснити всебічну оцінку постачальників, враховуючи їх здатність ефективно виявляти, досліджувати та реагувати на загрози за допомогою даних з різних джерел, таких як кінцеві точки, мережі, додатки та хмарні середовища. Метою такої оцінки є не тільки визначення готовності постачальників до боротьби з різноманітними кіберзагрозами, але й оцінка їх здатності забезпечити безпеку на всіх рівнях інфраструктури організації, що є необхідним для підтримки високих стандартів кіберзахисту.

Графічна форма квадранта дозволяє чітко класифікувати постачальників за чотирма основними категоріями: «Лідери», «Претенденти», «Провидці» та «Нішеві гравці». Це дає можливість користувачам швидко визначити постачальників, які показують найкращі результати в інноваціях і ефективності реалізації своїх рішень, що значно спрощує вибір постачальників для інтеграції передових технологій у стратегію кіберзахисту організації.

• «Лідери» — це компанії, які досягли найвищих результатів за двома основними критеріями: «повнота бачення» та «здатність реалізації». Вони мають чітку стратегію розвитку і здатні ефективно впроваджувати її на практиці, завдяки чому є домінуючими гравцями на ринку.

• «Претенденти» — компанії, які володіють сильною здатністю до реалізації, але їх стратегічне бачення може бути менш розвиненим порівняно з лідерами. Вони активно інтегрують новітні технології, однак їх рівень інноваційних рішень не такий високий, як у лідерів ринку.

• «Провидці» — постачальники, що мають сильне стратегічне бачення і пропонують інноваційні рішення, але їм часто не вистачає ефективності в реалізації цих рішень або стабільності їхніх результатів.

• «Нішеві гравці» — компанії, які не досягли високих результатів за основними критеріями. Вони можуть бути зосереджені на вузьких ринках або мати обмежену здатність до реалізації, що робить їх менш конкурентоспроможними на більш широкому ринку [10].

Магічний квадрант допомагає організаціям обирати постачальників, які найкраще відповідають їхнім потребам в області кібербезпеки, забезпечуючи ефективний захист на всіх етапах операційної діяльності. Це важливий інструмент для стратегічного планування та вибору технологій, які допомагають забезпечити надійний захист від постійно зростаючих кіберзагроз.

На основі аналізу останніх звітів Gartner можна визначити провідних постачальників в області XDR, таких як Microsoft, CrowdStrike, SentinelOne, що є беззаперечними лідерами, а також інші компанії, які займають свої місця в інших квадрантах, що дозволяє зробити висновки щодо загальних тенденцій розвитку ринку і найбільш перспективних рішень для захисту кінцевих точок [12].

Дослідження, проведені компанією Gartner, мають значний вплив на розвиток можливостей організацій у сфері виявлення кіберзагроз, надаючи важливу інформацію про сильні та слабкі сторони постачальників послуг кібербезпеки, зокрема щодо здатності виявляти нові загрози. Цей процес дозволяє організаціям зосередитися на виявленні можливих прогалин в їхній існуючій безпековій інфраструктурі та приймати обґрунтовані рішення щодо інвестування в нові технології та послуги, які можуть ефективно закрити ці прогалини. Одним із важливих аспектів є також удосконалення реагування на інциденти. Вивчення досвіду дозволяє розробити ефективні стратегії реагування на інциденти, що зменшують втрати та час відновлення систем.

Оцінка постачальників за допомогою магічного квадранта Gartner також включає критерії, що стосуються здатності компаній швидко та ефективно розслідувати та реагувати на загрози. Постачальники, що потрапляють до квадранту «Лідери», зазвичай мають доступ до передових інструментів та технологій, що дозволяють оптимізувати процеси реагування на інциденти. Ці рішення зазвичай інтегруються з уже існуючою інфраструктурою безпеки, що дозволяє організаціям швидко корелювати сповіщення з різних джерел, автоматизувати дії реагування та скорочувати час на виявлення та усунення загроз.

Відповідно до мінливого ландшафту загроз, організації повинні будувати свої стратегії безпеки з урахуванням довгострокового бачення постачальників та їхньої стратегії. Рішення постачальників, які впроваджують інноваційні підходи та технології, мають суттєвий вплив на загальний рівень безпеки організацій, що робить використання таких інструментів, як магічний квадрант Gartner, необхідним для вибору найбільш ефективних рішень.

Таке стратегічне планування забезпечує ефективне зниження ризиків та дозволяє організаціям адаптувати свої ініціативи з кібербезпеки до постійно змінюваного середовища кіберзагроз. З огляду на швидкий розвиток кіберзагроз, використання рішень, таких як XDR (розширене виявлення та реагування), є необхідним кроком для того, щоб випередити кіберзлочинців і забезпечити захист критичних даних [11].

У сучасних умовах компанії стикаються з безпрецедентними загрозами в кіберпросторі, що зумовлює необхідність використання передових технологій для захисту кінцевих точок від атак та злому. Якщо раніше технології виявлення та реагування на кінцеві точки (EDR) стали стандартом, то тепер наступним етапом еволюції в цій галузі є XDR (розширене виявлення та реагування). Це дозволяє значно покращити інтеграцію різних систем для виявлення загроз і зменшити час на реагування.

Наразі нові технології, такі як UES (уніфіковані служби безпеки), DaaS (безпека як послуга), ASCA (автоматизоване сканування контенту), EASM

(безпека при зовнішньому моніторингу активів), BAS (система активних атак на інфраструктуру), EM (управління вразливостями), ITDR (управління ризиками на рівні IT), EAI (інтеграція безпеки в автоматизовані процеси) та AMTD (аналітика для моніторингу та розслідування загроз), пропонують нові підходи до подолання сучасних кіберзагроз, що дозволяють досягти вищого рівня безпеки та забезпечити ефективну протидію атакам.

Також, Gartner оновлює свої підходи до інновацій в галузі кібербезпеки через Hype Cycle, який ілюструє актуальні технології та їх розвиток. Одним із ключових напрямків є автоматизоване виявлення та запобігання загрозам, а також інтегроване розширене виявлення та реагування (XDR), що дозволяє надавати більш точні й швидкі відповіді на кіберзагрози. До того ж, важливим є використання технологій ізоляції кінцевих точок, браузерів, а також впровадження концепції нульової довіри для забезпечення надійного захисту організацій.

У таблиці 1.1 наведено список світових лідерів у галузі кібербезпеки кінцевих точок, а також їхніх партнерів в Україні, які використовують ці технології для посилення безпеки своїх інформаційних систем. Ці компанії активно застосовують інноваційні методи захисту, що дозволяють оперативно виявляти загрози, реагувати на них і забезпечувати надійний захист інформації в умовах постійно зростаючих ризиків.

Таблиця 1.1 – Світові лідери в кібербезпеці кінцевих точок

Світові лідери в кібербезпеці кінцевих точок	Партнери в Україні
Microsoft	DataGroup
CrowdStrike	Infopulse
SentinelOne	SoftServe
Cybereason	Miratech
Palo Alto Networks	Luxoft

1.2. Класифікація методів атак соціальної інженерії

Соціальна інженерія — це метод, за допомогою якого зловмисники отримують несанкціонований доступ до інформації або ресурсів без використання технологічних засобів, а через маніпуляції з людським фактором. Вона використовує психологічні принципи для маніпулювання поведінкою людей, часто з метою введення їх в оману або переконання в необхідності вчинити певні дії, які надають зловмисникам доступ до цінної інформації чи систем [13].

Основою соціальної інженерії є здатність впливати на когнітивні процеси, такі як довіра, співчуття, страх чи поспіх. Люди часто схильні довіряти іншим, надавати допомогу, навіть не усвідомлюючи, що таким чином можуть порушувати безпеку своїх особистих або корпоративних даних. Зловмисники використовують ці природні схильності, створюючи ситуації, де їхні жертви роблять те, чого вони не повинні були б робити в звичайних умовах.

Такий підхід робить соціальну інженерію надзвичайно ефективною, навіть при відсутності складних технічних навичок або інструментів. Замість того, щоб зламувати паролі чи обходити системи безпеки, зловмисники можуть отримати потрібну інформацію через прості маніпуляції з людьми, що значно підвищує ймовірність успіху атаки. У результаті, організації повинні приділяти велику увагу навчанням і тренуванням співробітників, щоб вони могли виявляти спроби соціальної інженерії і уникати небезпечних ситуацій.

Соціальна інженерія може застосовуватися як у незаконних цілях, наприклад, для отримання конфіденційної інформації, так і у правомірних, наприклад, для переконання певних осіб виконувати необхідні дії. Найчастіше ці методи використовуються для доступу до цінних даних, обходячи навіть найсучасніші системи захисту. Успішні атаки соціальних інженерів демонструють, що навіть при наявності складних технічних заходів безпеки основною вразливістю організацій залишаються їхні співробітники [14].

Організації, незважаючи на впровадження новітніх технологій, навчання персоналу та забезпечення фізичної охорони, все ще залишаються вразливими до соціальної інженерії. Зловмисники використовують людський фактор як слабке місце в системі безпеки. Чим складніша та розгалуженіша ІТ-інфраструктура організації, тим більше ризиків виникає через людську діяльність.

Соціальна інженерія також ґрунтується на технологіях впливу на підсвідомість, таких як гіпноз і нейролінгвістичне програмування (НЛП). Дослідження демонструють, що свідомі рішення часто випереджаються підсвідомими реакціями, що дозволяє зловмисникам маніпулювати людьми, змушуючи їх розкривати конфіденційну інформацію. Це підкреслює важливість розуміння природи таких методів і навчання персоналу протидії їм.

Багато ІТ-фахівців вважають, що серйозні технічні заходи, такі як брандмауери, системи автентифікації чи біометричні пристрої, забезпечують достатній захист. Однак проблема кібербезпеки часто лежить у площині людського фактору та управління. Тому однією з ключових умов ефективного захисту є систематична робота з персоналом, включаючи навчання технік протидії соціальній інженерії та впровадження політик безпеки.

Атаки соціальних інженерів зазвичай поділяються на три етапи: розробка плану дій, моральна підготовка та тренування, під час яких створюються сценарії та психологічно обґрунтовані моделі взаємодії з потенційними жертвами. Успішність атак зловмисників пояснюється використанням ретельно продуманих стратегій обману, які спрямовані на вразливості людської психіки [15].

Тому організаціям слід приділяти увагу не лише технічним засобам захисту, а й систематичному підвищенню обізнаності працівників, проведенню регулярних тренінгів і тестувань. Це дозволить створити комплексний захист, що враховує як технічні, так і психологічні аспекти загроз.

На рис. 1.1. наведено аналіз вразливостей соціальної інженерії представлена (рис.1.1).

Рис. 1.1 – Аналіз вразливостей соціальної інженерії

Соціальна інженерія, як інструмент маніпуляції, базується на комбінації технічних знань та психологічних методів, що дозволяє зловмисникам досягати таких цілей, як збір конфіденційної інформації, отримання доступу до захищених систем або змушення жертви виконувати необхідні для соціального інженера дії. Цей процес може включати як короткострокові, так і довготривалі взаємодії з жертвою, залежно від складності та тривалості реалізації атаки.

Однією з ключових цілей соціальної інженерії є збір інформації про потенційну жертву, який здійснюється через обман, довготривалі відносини

або імітацію довіри. На цьому етапі зловмисник може використовувати практичні приводи, наприклад, удаване бажання допомогти або потребу в консультації, щоб отримати конфіденційну інформацію. Зібрані дані дозволяють зловмиснику здійснити несанкціонований доступ до систем (НСД) або ж змусити об'єкт виконувати певні дії, які в кінцевому результаті призведуть до розвитку нових загроз або порушення безпеки.

Атаки соціальної інженерії можуть бути короткостроковими та довготривалими. Короткострокові атаки проводяться у стислі терміни, не потребують значних часових чи матеріальних ресурсів, але їх недолік полягає у меншій ефективності, оскільки зловмисник не завжди має змогу досягти складних цілей або змусити жертву здійснити серйозні дії. Довготривалі атаки, навпаки, вимагають значних зусиль, часу та підготовки, але забезпечують зловмиснику більше можливостей для маніпуляції, зокрема створення довірчих відносин із жертвою.

Соціальна інженерія застосовується не лише у сфері кіберзлочинності, але й для досягнення інших цілей, серед яких:

- Отримання прибутку через маніпуляції або обман;
- Збір статистичних даних для подальшого аналізу;
- Підвищення рівня довіри з боку клієнтів чи партнерів;
- Конкурентна боротьба, наприклад, за клієнтів у бізнесі (як це часто трапляється у сфері послуг, зокрема таксі).

Ефективність атаки залежить від рівня підготовки соціального інженера та ступеня доступу, який він може отримати. Успішні атаки класифікуються за рівнями доступу до систем чи даних, які визначаються статусом жертви в ієрархії організації. Найвищий рівень доступу отримується при маніпуляції адміністраторами систем, потім начальниками, звичайними користувачами, і, в кінці, знайомими чи пересічними контактами жертви. Чим вищий рівень доступу, тим серйозніші наслідки може мати атака.

Соціальна інженерія залишається важливим викликом у сфері кібербезпеки, оскільки навіть найдосконаліші технічні засоби захисту можуть

бути обійдені через психологічний вплив на людину. Це підтверджує важливість систематичного навчання персоналу, впровадження заходів підвищення обізнаності та розвитку навичок протидії маніпуляціям.

Розглянемо найпоширеніші техніки та типи атак, які активно використовуються соціальними інженерами. Ці методи базуються на психологічних особливостях людини, зокрема на когнітивних упередженнях, які є типовими помилками в процесі прийняття рішень. Соціальні інженери майстерно маніпулюють цими упередженнями, використовуючи їх у різних комбінаціях, щоб створити максимально ефективну стратегію обману в кожній окремій ситуації. Головною метою цих методів є введення людини в оману, щоб спонукати її здійснити дії, які вигідні зловмиснику.

Однією з найбільш поширених і ефективних тактик є фішинг (від англійського слова "fishing" – риболовля). Фішинг – це вид інтернет-шахрайства, основна мета якого полягає в отриманні доступу до конфіденційних даних користувачів, таких як логіни, паролі або інформація про банківські рахунки. Ця атака часто реалізується через розсилку електронних листів або повідомлень, що видають себе за офіційні запити від імені популярних брендів, фінансових установ, соціальних мереж або інших відомих сервісів.

Листи або повідомлення фішерів зазвичай містять посилання, яке перенаправляє користувача на підроблений вебсайт, що зовні виглядає ідентично справжньому. Потрапивши на цей сайт, користувача переконують ввести свої персональні дані, використовуючи різноманітні психологічні прийоми, такі як створення відчуття терміновості (наприклад, повідомлення про заблокований рахунок) або підвищення довіри (імітація офіційних повідомлень). Основними цілями фішингових атак є клієнти банків, користувачі електронних платіжних систем, а також учасники соціальних мереж.

Соціальні мережі є особливо привабливим середовищем для шахраїв, оскільки вони дозволяють збирати велику кількість персональної інформації

про користувачів. Через це платформи на кшталт Facebook, Instagram або Twitter часто стають мішенню фішингових атак. Шахраї використовують підроблені посилання, що ведуть на фальшиві сайти, для отримання доступу до облікових записів користувачів. За оцінками експертів, понад 70% фішингових атак у соціальних мережах є успішними, що свідчить про високу ефективність цього методу.

Важливо зазначити, що фішинг є лише одним із численних інструментів, які застосовують соціальні інженери. Підхід до кожної атаки залежить від мети, рівня підготовки зловмисника та психологічних характеристик жертви. Тому навчання користувачів основам кібергігієни, підвищення обізнаності щодо методів шахрайства та регулярна перевірка безпеки є ключовими елементами у боротьбі із соціальною інженерією.

Принцип роботи IVR системи зображений на рисунку 1.2.

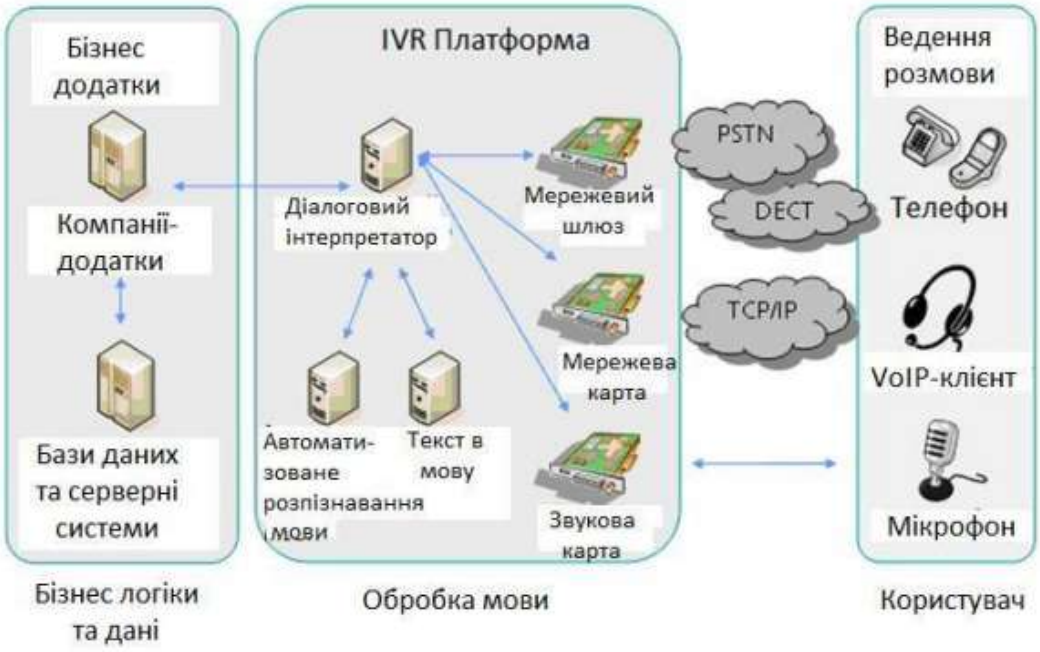

Рис. 1.2 - Принцип дії IVR систем [14]

Троянські програми використовують схожі методи впливу, які застосовують маркетологи, однак їх мета – не залучення клієнтів, а компрометація системи та отримання конфіденційної інформації. Розробники

шкідливого програмного забезпечення майстерно маніпулюють людськими слабкостями, експлуатуючи такі психологічні особливості, як:

Бажання переглянути цікавий або провокативний контент. Наприклад, заголовки на кшталт «Шокуюче відео» чи «Ексклюзивні фото» стимулюють користувача відкрити вкладення або посилання.

Інтерес до дефіцитних товарів або послуг. Люди частіше відкривають підозрілі файли чи посилання, якщо це виглядає як пропозиція придбати щось унікальне чи важкодоступне.

Захоплення швидкими методами збагачення. Фінансові піраміди, обіцянки миттєвого заробітку або «гарантованого успіху в бізнесі» часто стають наживкою для наївних користувачів.

Один із найпоширеніших способів поширення троянів – через вкладення в електронних листах. Коли працівник відкриває файл, прикріплений до повідомлення, він несвідомо встановлює на свій комп’ютер шкідливе програмне забезпечення, яке надає соціальному інженеру доступ до конфіденційної інформації організації.

Зловмисники також використовують такі техніки, як:

Подвійне розширення файлів. Наприклад, файл із розширенням "document.jpg.exe" може виглядати як зображення, однак насправді це виконуваний файл, здатний завдати шкоди. У таких випадках поштові сервіси або користувачі часто не помічають справжнього характеру вкладення.

Приховування назви файлу. Зловмисники можуть додавати довгі назви файлів, щоб реальне розширення залишалося поза полем зору користувача.

Ще одним ефективним середовищем для поширення троянів є миттєві повідомлення та чати. Завдяки невимушеному формату спілкування, користувачі часто ігнорують ризики, не підозрюючи, що перед ними потенційна кіберзагроза. Функція створення псевдонімів у месенджерах додає анонімності та підсилює можливості зловмисників для обману.

Для прикладу, під час фішингової атаки або атаки через миттєві повідомлення, користувачу може надійти посилання на нібито «цікавий

матеріал» або «ексклюзивну пропозицію». Переходячи за таким посиланням, жертва несвідомо активує шкідливе програмне забезпечення, що запускає процес компрометації системи.

На рисунку 1.3 можна побачити схему, яка ілюструє, як працює механізм атаки через електронну пошту та обмін миттєвими повідомленнями. Основний акцент у цій схемі – взаємодія між користувачем, троянською програмою та зловмисником, який отримує доступ до інформації через маніпуляції.

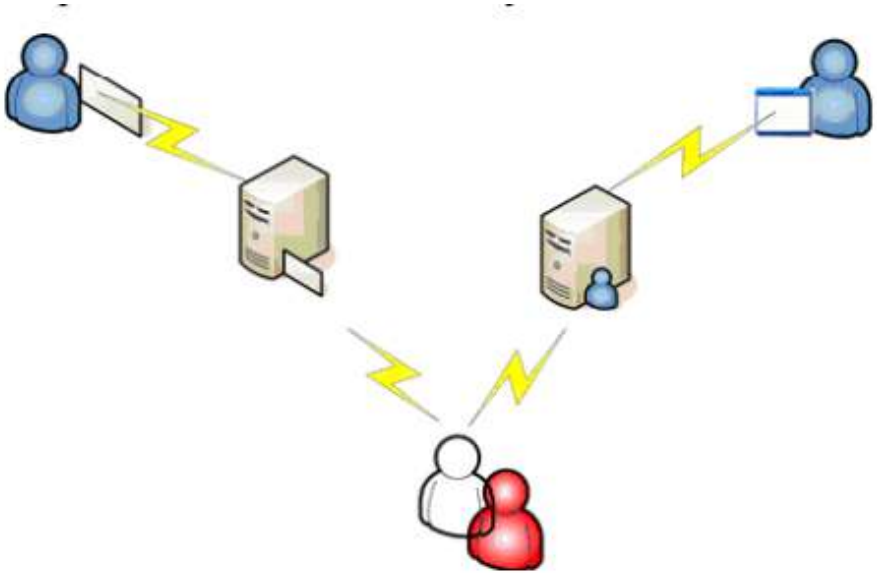

Рис. 1.3 – Візуалізація при використанні IM і e-mail [15]

Таким чином, основна стратегія соціального інженера полягає у використанні емоцій, довіри та необізнаності користувачів для досягнення своїх цілей. Ефективність таких атак можна зменшити завдяки регулярному навчанню працівників, впровадженню багаторівневої системи захисту та постійній перевірці безпеки організаційних систем.

Соціальний інженер (позначений червоним на ілюстрації) виступає під виглядом знайомого користувача, розсилаючи електронні листи або миттєві повідомлення. Його мета – змусити отримувачів прийняти ці повідомлення за кореспонденцію від довірених осіб.

Згідно з ДСТУ ISO/IEC 27004:2018 "Обчислення. Методи захисту. Системи управління інформаційною безпекою", організації повинні

використовувати стандартизовані заходи, засоби контролю та управління, рекомендовані ISO/IEC 27001, для ефективного виявлення та протидії таким атакам [16].

1.3. Проблемні аспекти існуючих досліджень та їх недоліки

Результати дослідження підтверджують, що організації все активніше впроваджують IT-стратегії, спрямовані на протидію атакам соціальної інженерії, серед яких особливе місце займають стратегії навчання працівників, управління ризиками та плани реагування на кіберзагрози. Однак для забезпечення комплексного захисту інформаційних систем та постійного вдосконалення практик кібербезпеки необхідно провести більш детальну оцінку поточного стану кібербезпеки організації. Така оцінка повинна включати детальне виявлення та аналіз можливих ризиків, оцінку вразливостей різних інформаційних активів, а також розробку ефективної стратегії, яка дозволить оперативно виявляти, мінімізувати та нейтралізувати потенційні загрози [17].

Одним з основних елементів комплексної стратегії безпеки є створення та впровадження плану реагування на кіберзагрози. Цей план повинен містити не тільки чіткі інструкції щодо відновлення IT-послуг і даних після порушення безпеки чи технічного збою, а й визначати конкретні ролі та обов’язки відповідальних осіб, організовувати регулярні тренінги для персоналу з питань, пов’язаних із соціальною інженерією. Важливим є також забезпечення механізмів для ізоляції уражених систем, щоб запобігти подальшому поширенню загрози. Крім того, необхідно впровадити регулярне резервне копіювання даних та створити план безперервності бізнесу, що дозволить організації зберегти функціонування ключових бізнес-процесів навіть у кризових ситуаціях. У разі кіберзагроз доцільно також розглянути можливість використання кіберстрахування для покриття витрат на відновлення після інцидентів.

Окремо варто акцентувати увагу на розробці стратегічного плану кібербезпеки, який включатиме впровадження багатофакторної автентифікації. Ця технологія, яка використовує поєднання паролів, фізичних пристроїв (смартфонів, смарт-карт) і біометричних даних, дозволяє значно підвищити рівень захисту інформаційних систем від несанкціонованого доступу. Крім того, варто використовувати політики доступу на основі ролей, що дозволить контролювати та обмежувати доступ до критичних даних. Постійний моніторинг систем у реальному часі, регулярне оновлення програмного забезпечення, а також проведення детальних аудитів безпеки допоможуть своєчасно виявляти вразливості і знижувати ймовірність виникнення кіберінцидентів [18].

Не менш важливим є впровадження спеціалізованих освітніх програм для персоналу, спрямованих на підвищення обізнаності працівників щодо ризиків соціальної інженерії. Регулярне навчання допоможе співробітникам не лише розпізнавати потенційні загрози, але й адекватно реагувати на підозрілі ситуації, що виникають у повсякденній роботі. Важливою частиною таких програм має бути інформування працівників про новітні методи та техніки, що використовуються зловмисниками для обходу систем захисту [19].

1.4. Пропозиції щодо напрямків подальших досліджень

Враховуючи швидко змінювану природу загроз у сфері інформаційної безпеки, подальші дослідження мають бути спрямовані на кілька важливих напрямків, кожен з яких може значно підвищити ефективність захисту організацій від атак соціальної інженерії та інших кіберзагроз. Одним з основних завдань є розвиток інноваційних методів протидії соціальній інженерії, зокрема шляхом удосконалення існуючих систем виявлення та запобігання таким атакам [20]. У цьому контексті велике значення має інтеграція когнітивних та поведінкових моделей у технології штучного інтелекту (ШІ), що дозволяють автоматизувати процес верифікації та попередження потенційно небезпечних взаємодій. Використання ШІ для

аналізу патернів поведінки користувачів і виявлення аномалій допоможе своєчасно ідентифікувати спроби маніпуляцій і шахрайства, що може значно підвищити рівень безпеки в організаціях.

Іншим важливим напрямком є розвиток нових методів навчання та підвищення обізнаності серед співробітників організацій щодо ризиків, пов’язаних з соціальною інженерією. Розробка інноваційних підходів до тренінгів, зокрема використання віртуальних симуляцій, інтерактивних навчальних платформ і гейміфікаційних елементів, дозволить більш ефективно навчати співробітників виявляти техніки обману в реальному часі. Такі підходи можуть бути набагато ефективнішими, ніж традиційні методи навчання, оскільки вони забезпечують більш практичний досвід у контексті реальних загроз.

Додатково, значну увагу необхідно приділяти вивченню взаємодії між технологічними системами захисту і людським фактором. Як показує практика, саме людський фактор є однією з основних вразливих ланок в системах кібербезпеки, і тому інтеграція психологічних, когнітивних і соціальних аспектів у комплексні стратегії безпеки стане ключем до створення більш надійних захисних механізмів. Це включає не лише адаптацію технологій, але й розробку таких програм навчання та підтримки співробітників, які допоможуть мінімізувати ризики, пов’язані з людськими помилками [21].

Важливим є розвиток і тестування нових технологій автентифікації та шифрування, які можуть знизити ймовірність успішного обходу безпеки за допомогою маніпуляцій з боку зловмисників. Зокрема, багатофакторна автентифікація, використання біометричних даних та інтеграція нових методів шифрування допоможуть створити більш захищені інформаційні системи, здатні протистояти навіть складним атакам, спричиненим соціальною інженерією [22].

Не менш важливим напрямком є вивчення правових та етичних аспектів боротьби з соціальною інженерією в умовах швидко змінюваного

кіберпростору. Це включає розробку міжнародних стандартів та законодавчих ініціатив, які можуть посилити заходи безпеки, забезпечити належний захист персональних даних та створити правові рамки для запобігання і протидії кіберзлочинності. Тільки в межах міжнародної співпраці та узгоджених стандартів можна досягти ефективного та сталого вирішення проблеми соціальної інженерії та інших кіберзагроз у глобальному масштабі.

Загалом, успішна протидія атакам соціальної інженерії вимагає комплексного підходу, який поєднує передові технології, ефективне навчання персоналу, врахування людського фактору та постійну адаптацію до нових загроз. Впровадження цих напрямків у практику дозволить створити більш захищену і стійку інфраструктуру для боротьби з кіберзлочинцями в умовах сучасного інформаційного середовища [23].

РОЗДІЛ 2. ТЕОРЕТИЧНА РОЗРОБКА ЗАСОБІВ ПРОТИДІЇ СОЦІАЛЬНІЙ ІНЖЕНЕРІЇ

2.1. Постановка завдання: мета та завдання власних досліджень

Метою дослідження є розробка консольної програми на мові програмування C++, яка продемонструє основи фішингу як одну з основних загроз у сфері інформаційної безпеки. Програма створюється з метою навчання та аналізу можливих вразливостей, які можуть виникнути в результаті атак соціальної інженерії. Це дослідження також передбачає оцінку різних методів фішингу з точки зору їх ефективності, а також сприятиме підвищенню обізнаності щодо загроз та способів захисту від них.

Для досягнення цієї мети буде розроблено програму, що імітує фішинг-атаку, наприклад, через створення підроблених веб-сторінок або фальшивих електронних листів, що можуть обманювати користувачів та змушувати їх вводити конфіденційну інформацію. Особлива увага приділяється вивченню методів запобігання таким атакам, як багатофакторна автентифікація та навчання користувачів розпізнавати фішинг-атаки. Наочно це представлено на рис. 2.1.

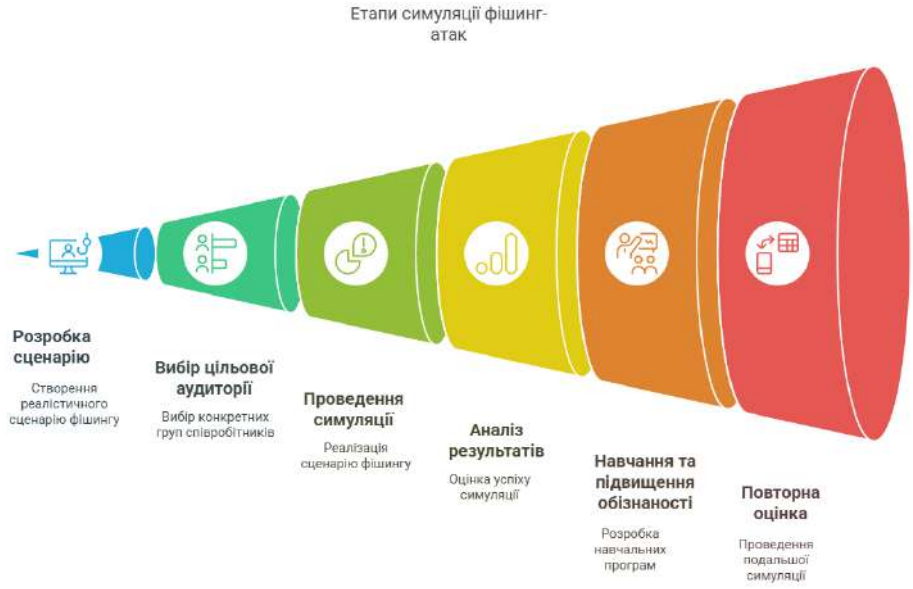

Рис. 2.1 – Етапи симуляції фішинг-атак

Програма також повинна містити механізми збору і збереження введених даних, таких як логіни та паролі, для подальшого аналізу успішності атаки.

Важливою частиною дослідження є проведення тестів на створеній програмі, щоб оцінити її ефективність у симулюванні фішинг-атак і визначити найбільш уразливі місця для таких атак. Після завершення тестування будуть підготовлені рекомендації щодо покращення кібербезпеки та навчання користувачів для запобігання фішинг-атакам (рис.2.2).

Рис. 2.2 – Вдосконалення кібербезпеки для запобігання фішингу

У ході дослідження буде розроблено консольну програму на мові C++, яка демонструватиме основи фішингу як загрози інформаційній безпеці.

Програма дозволятиме імітувати фішинг-атаки, досліджувати їхню ефективність та аналізувати вразливості користувачів до таких атак.

Результати тестування створеної програми покажуть потенційні слабкі місця у сфері кібербезпеки, що підтвердить необхідність застосування додаткових заходів захисту, зокрема, багатофакторної автентифікації та навчання користувачів розпізнавати фішингові загрози.

Отримані результати та розроблені рекомендації сприятимуть підвищенню рівня обізнаності про фішинг-атаки та допоможуть розробити ефективні стратегії захисту від них.

2.2. Розробка теоретичної моделі реагування на загрози соціальної інженерії

Розробка теоретичної моделі реагування на загрози соціальної інженерії передбачає створення структури, яка допоможе організаціям систематично підходити до виявлення, оцінки та нейтралізації загроз, що виникають внаслідок атак соціальних інженерів. Така модель повинна враховувати ключові аспекти інформаційної безпеки та адаптуватися до швидко змінюваного кіберсередовища.

Першим етапом у створенні теоретичної моделі є визначення основних типів загроз соціальної інженерії, таких як фішинг, вішинг (голосові фішингові атаки), смишинг (SMS-фішинг), а також атаки через соціальні мережі та фальшиві вебсайти. Важливо не тільки виявити ці загрози, а й зрозуміти механізми їхнього впливу на організацію та її працівників.

Наступним етапом є розробка стратегії виявлення цих загроз. Це може включати використання інструментів аналізу поведінки користувачів, інтелектуальних систем, які на основі алгоритмів штучного інтелекту аналізують підозрілі дії в мережах і надають сигнали про можливі атаки. Важливим аспектом є також моніторинг усіх комунікаційних каналів, через які можуть здійснюватися атаки (електронна пошта, повідомлення в месенджерах, соціальні мережі).

Третім етапом є розробка процедур реагування на загрози. Це повинно включати в себе не лише інструкції для працівників, але й формалізовані кроки для ІТ-відділів та спеціалістів з кібербезпеки, які повинні оперативно реагувати на інциденти. Наприклад, у випадку виявлення фішингового листа, співробітники повинні негайно припинити його поширення, а також попередити інших користувачів організації про потенційну загрозу.

Також важливим елементом є навчання персоналу. Оскільки людський фактор залишається основною вразливістю у боротьбі з соціальною інженерією, регулярні тренінги та симуляції фішингових атак є необхідною частиною моделі реагування. Це дозволить співробітникам розпізнавати та уникати загрозливих ситуацій, що знижує ймовірність успішної атаки.

Крім того, важливо включити етапи відновлення та реагування після інциденту. Всі виявлені інциденти повинні бути задокументовані та проаналізовані для вдосконалення стратегії захисту. Це включає відновлення доступу до систем і даних, оцінку можливих витоків інформації, а також удосконалення систем безпеки для уникнення повторення подібних атак.

Завершальним етапом є постійний моніторинг і вдосконалення моделі реагування. Графічно це представлено на рис. 2.3. Загрози соціальної інженерії постійно еволюціонують, тому організаціям необхідно регулярно переглядати та оновлювати свої стратегії, проводити аудит існуючих захисних механізмів і навчальних програм, адаптуючи їх до нових технологічних та соціальних викликів [24].

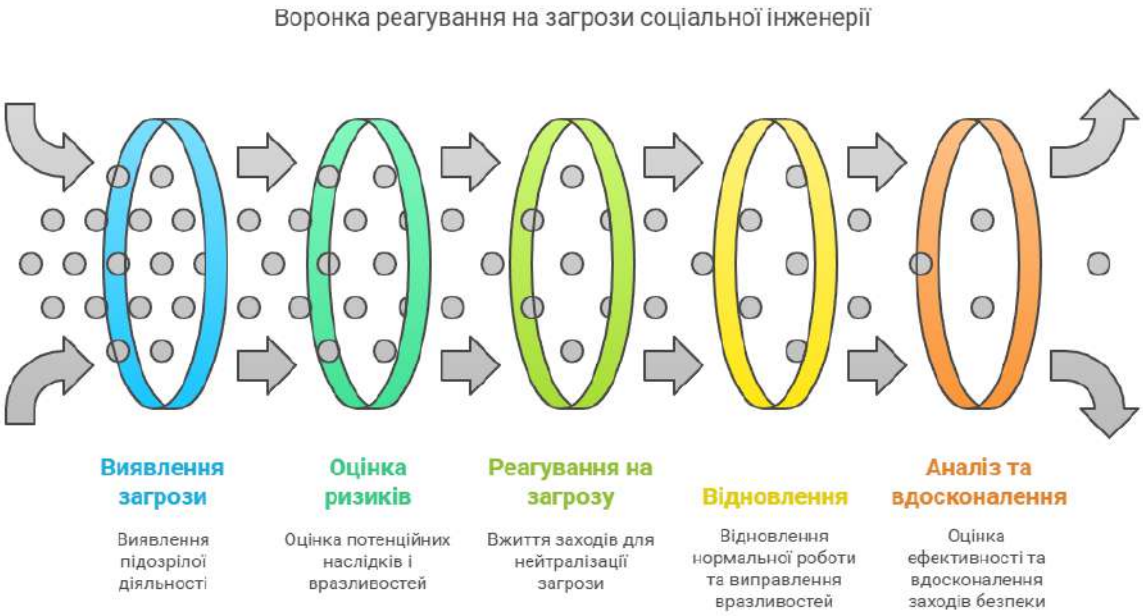

Рис. 2.3 – Етапи реагування на загрози соціальної інженерії

Розроблена теоретична модель реагування на загрози соціальної інженерії дозволяє організаціям системно підходити до виявлення, аналізу та нейтралізації таких атак. Вона охоплює всі ключові етапи: ідентифікацію загроз, розробку механізмів їхнього виявлення, створення ефективних процедур реагування, навчання персоналу та постійний моніторинг кіберзагроз.

Одним із найважливіших аспектів цієї моделі є врахування людського фактору, оскільки соціальна інженерія спрямована переважно на маніпуляцію людьми, а не на технологічні вразливості. Тому впровадження навчальних програм і регулярних тестувань є необхідним заходом для підвищення загального рівня інформаційної безпеки організації.

Окрім цього, модель передбачає швидке реагування на інциденти та ефективне відновлення після атак. Це дозволяє зменшити потенційні збитки та запобігти повторенню подібних загроз у майбутньому. Постійне оновлення підходів та адаптація до нових викликів гарантує актуальність запропонованих заходів захисту в умовах динамічного розвитку кіберзагроз.

Таким чином, реалізація цієї моделі сприятиме підвищенню стійкості організацій до атак соціальних інженерів та створенню більш безпечного цифрового середовища.

2.3. Опис алгоритмів для навчання користувачів протидії атакам

Опис алгоритмів для навчання користувачів протидії атакам соціальної інженерії має на меті створення ефективних і зрозумілих стратегій для підвищення обізнаності працівників організацій щодо можливих загроз та навчання їх правильним діям у разі виявлення підозрілих ситуацій. Це включає в себе розробку інтерективних підходів, використання віртуальних симуляцій та гейміфікації, що дозволяють практично закріпити навички.

Алгоритм ідентифікації фішингових атак (рис.2.4):

Крок 1: Визначення параметрів підозрілих електронних листів чи повідомлень.

- Шукайте ознаки неперсоналізованих або загальних повідомлень.
- Перевіряйте домен відправника на наявність підозрілих або неприємних елементів (наприклад, відмінності в іменах або додаткові літери).
- Перевіряйте URL посилань, чи не перенаправляють вони на підозрілі ресурси.

Крок 2: Навчання розпізнавання підозрілих запитів на особисті дані.

- Обов'язково нагадувати, що жоден авторитетний сервіс не запитуватиме конфіденційну інформацію через електронну пошту або повідомлення.
- Окремо підкреслювати важливість перевірки URL-сайтів, що надаються в листах.

Крок 3: Оцінка і обробка підозрілих листів.

- Перевірка ідентичності відправника за допомогою офіційних каналів (замість натискання на посилання).

- Інструктаж щодо правильного реагування на підозрілі повідомлення (наприклад, повідомлення команди з кібербезпеки або IT-відділ).

Крок 4: Проведення тренінгів для співробітників, включаючи реалістичні симуляції фішингових атак, щоб закріпити ці навички.

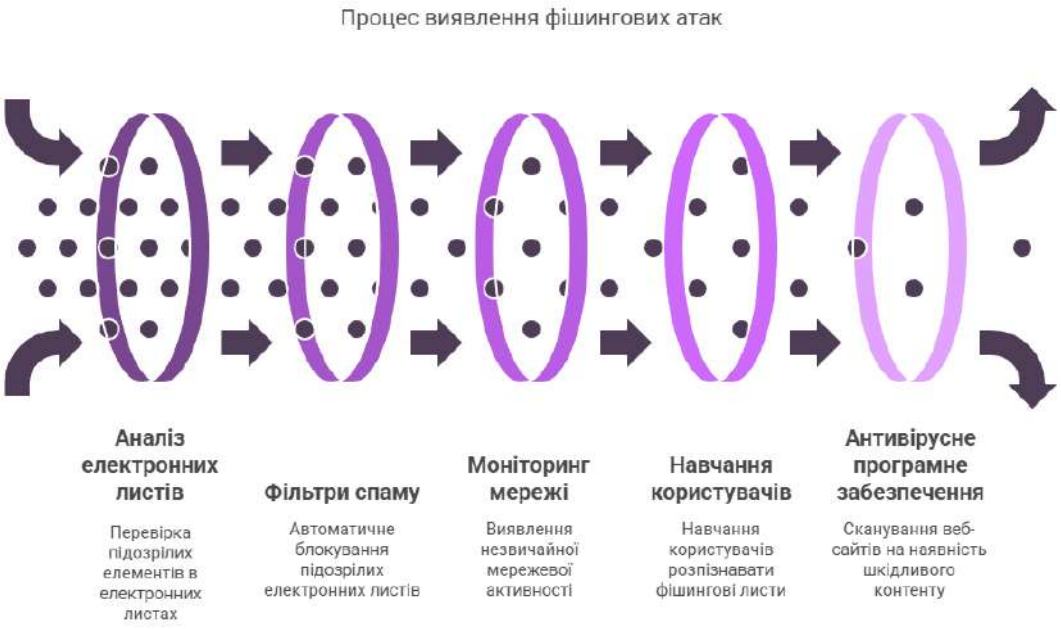

Рис. 2.4 – Процес виявлення фішингових атак

Алгоритм навчання використанню багатофакторної автентифікації (рис.2.5):

Крок 1: Ознайомлення користувача з принципами багатофакторної автентифікації (BFA).

Пояснити, що це механізм, який використовує два або більше методів підтвердження особи (пароль + одноразовий код або біометричні дані).

Крок 2: Налаштування багатофакторної автентифікації для основних ресурсів.

Демонстрація процесу активації BFA на прикладах акаунтів (електронна пошта, банківські акаунти, соціальні мережі).

Крок 3: Навчання користувачів використанню різних методів BFA.

Введення QR-кодів, застосування фізичних ключів для автентифікації, використання мобільних додатків для генерації кодів.

Крок 4: Оцінка та відпрацювання практичних випадків несанкціонованого доступу і реагування на них через багатофакторну автентифікацію.

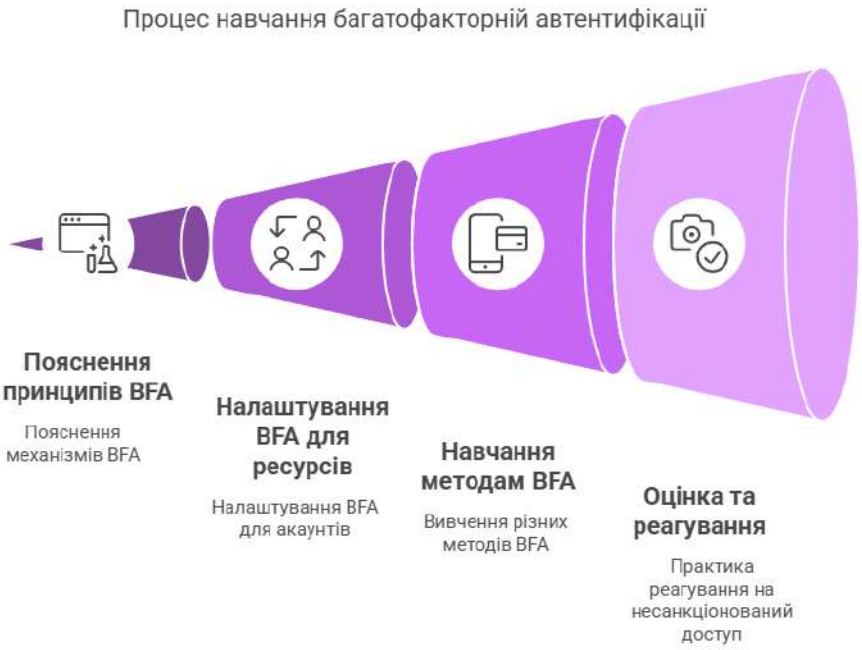

Рис. 2.5 – Навчання багатофакторній автентифікації

Алгоритм реагування на вішинг (голосові фішингові атаки) (рис.2.6):

Крок 1: Ознайомлення користувачів із методами вішингу.

Пояснення, як зловмисники можуть видавати себе за представників організації або знайомих для збору особистих даних через телефонні дзвінки.

Крок 2: Навчання користувачів основним ознакам вішинг-атак.

Визначення підозрілих запитів, таких як терміновість, натиск на розголошення конфіденційної інформації, вимога дій без перевірки.

Крок 3: Розробка процедури реагування на вішинг.

Вказати, що користувач повинен не надавати жодної інформації на запит телефонного дзвінка, перевіряти інформацію за допомогою офіційних каналів та звертатися до керівництва чи команди з кібербезпеки.

Рис. 2.6 – Ефективне реагування на вішинг

Алгоритм виявлення та запобігання соціальним маніпуляціям через соціальні мережі (рис.2.7):

Крок 1: Пояснення основних загроз через соціальні мережі.

Навчання розпізнаванню підозрілих профілів та маніпуляцій у чатах.

Крок 2: Розробка настанов з безпеки в соціальних мережах.

Включення налаштувань конфіденційності, визначення параметрів доступу до особистої інформації.

Крок 3: Своєчасне реагування на підозрілі повідомлення та зв'язок з адміністраторами соціальних мереж для блокування шахраїв.

Рис. 2.7 – Виявлення та запобігання маніпуляціям у соціальних мережах

Гейміфікація навчання:

Враховуючи важливість практичних навичок для виявлення та запобігання соціальним атакам, гейміфікація може стати ефективним методом навчання (рис.2.8). Працівники можуть пройти серію інтерактивних тестів і сценаріїв, де їм пропонується вибір реакцій на різні фішингові атаки, голосові маніпуляції, та інші форми соціальної інженерії. Гейміфікація дозволяє не тільки теоретично освоїти навички, а й вчитися реагувати в умовах, максимально наближених до реальних.

Алгоритми навчання користувачів повинні бути інтерактивними, доступними та практично орієнтованими на реальні загрози. Важливо, щоб співробітники не тільки ознайомлювалися з теоретичними аспектами, а й

практично відпрацьовували навички розпізнавання та ефективного реагування на соціальні інженерії в реальному часі.

Рис. 2.8 – Посилення навичок боротьби зі соціальною інженерією через гейміфікацію

Розробка алгоритмів навчання користувачів протидії атакам соціальної інженерії є надзвичайно важливим етапом у створенні ефективної системи кібербезпеки в організаціях. Атаки соціальної інженерії, такі як фішинг, вішинг, маніпуляції через соціальні мережі та інші види шахрайства, використовують людські слабкості для досягнення зловмисних цілей. Тому підвищення обізнаності працівників та формування в них навичок безпечної поведінки є критичним для зниження вразливості організацій до таких атак.

Методи навчання, що включають розпізнавання фішингових атак, використання багатофакторної автентифікації, реагування на вішинг і виявлення маніпуляцій у соціальних мережах, спрямовані на зміцнення

кіберзахисту. Вони дозволяють співробітникам розпізнавати потенційно небезпечні ситуації і відповідним чином на них реагувати, не надаючи зловмисникам можливість скористатися їхньою недосвідченістю або неуважністю. Важливою частиною навчання є також інструкції з правильної поведінки під час роботи з конфіденційною інформацією та вміння розпізнавати підозрілі дії.

Застосування інтерактивних підходів, таких як віртуальні симуляції, гейміфікація та практичні тренінги, значно покращує ефективність навчання. Ці методи не тільки дозволяють засвоїти теоретичні знання, але й надають можливість співробітникам практикувати свої навички в реальних умовах, що істотно підвищує рівень готовності до реальних кіберзагроз. Наприклад, віртуальні симуляції дозволяють користувачам проходити через сценарії кібератак, де вони можуть помітити загрози і правильно на них відреагувати, без ризику шкоди для реальних систем організації.

Гейміфікація в свою чергу стимулює працівників до активного навчання та взаємодії з матеріалом, використовуючи елементи ігор, що робить процес навчання більш захопливим і менш монотонним. Це сприяє кращому засвоєнню інформації і дозволяє розвивати навички швидкого реагування на різні типи атак.

Таким чином, алгоритми і методи навчання, які сприяють підвищенню обізнаності співробітників щодо соціальної інженерії, є ключовими для формування стійкої кіберкультури в організаціях. Вони допомагають не лише знижувати ризики від атак соціальної інженерії, а й формують проактивне ставлення до безпеки. Справжній захист інформаційних систем починається з людей, їх готовності до виявлення загроз і вміння реагувати на них у будь-який момент. Тому створення системи безпеки, яка включає регулярне навчання і тренування персоналу, є важливою складовою на шляху до створення стійкої кіберзахисної культури.

РОЗДІЛ 3. ПРАКТИЧНА РЕАЛІЗАЦІЯ ЗАПРОПОНОВАНИХ ЗАХОДІВ

3.1. Створення програмного інструмента для навчання користувачів

Розробляється програма на C++ призначена для навчання користувачів виявляти фішингові та вішингові атаки, а також використовувати багатофакторну автентифікацію. Вона пропонує три основні тренувальні режими.

Перший режим перевіряє електронні листи на наявність підозрілих фраз, які часто використовуються в фішингових атаках. Користувач вводить текст листа, і програма аналізує його на наявність цих фраз. Якщо вони є, програма попереджає про можливу фішингову атаку.

Другий режим зосереджений на вішингових дзвінках. Користувач вводить текст повідомлення з дзвінка, і програма визначає, чи містить воно фрази, характерні для вішингових атак, що можуть бути спробою шахрайства.

Третій режим тренує користувача правильно використовувати багатофакторну автентифікацію. Користувач вводить код, і програма перевіряє, чи він правильний, і повідомляє про успіх або помилку в процесі автентифікації.

Програма допомагає підвищити обізнаність про кіберзагрози і дає практичні навички для виявлення та реагування на потенційно небезпечні ситуації.

3.2. Реалізація консольного додатка на C++

Для реалізації консольного додатка на C++ з описаним функціоналом, спершу потрібно визначити основні компоненти програми та їх взаємодію. У цьому випадку, створимо програму, що навчить користувача ідентифікувати фішинг та вішинг, а також правильно використовувати багатофакторну автентифікацію. Програма буде інтерактивною, з чітким меню, яке дозволяє вибрати один із трьох тренувальних режимів.

Опис програми:

1. Функція для перевірки фішингових листів.

2. Функція для перевірки вішингових дзвінків.
3. Функція для навчання багатофакторної автентифікації.
4. Основне меню для вибору режиму тренування.

Програма містить три основні функції для тренування користувачів:

- Перевірка фішингових листів.
- Перевірка вішингових дзвінків.
- Навчання багатофакторної автентифікації.

Користувач може вибрати один із цих режимів через меню.

3.3. Тестування програмного інструмента та його застосування у різних сценаріях

Запустимо програму (рис. 3.1).

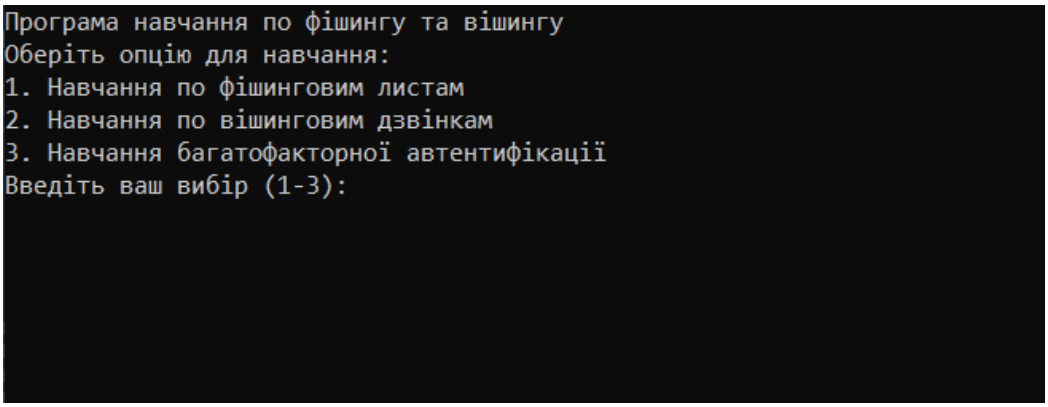

Рис. 3.1 – Запущена програма

З меню оберемо «навчання по фішинговим листам» (рис. 3.2).

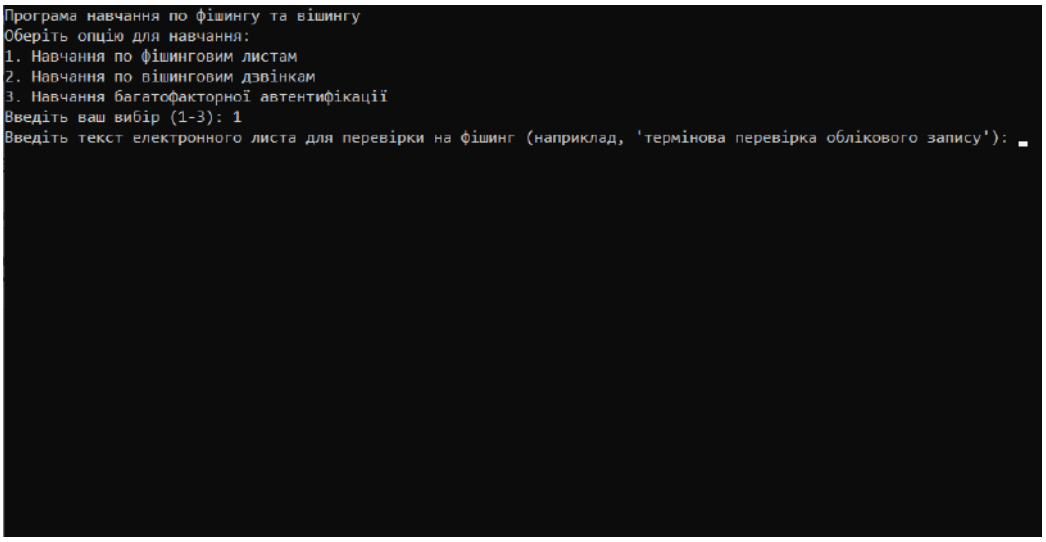

Рис. 3.2 – «Навчання по фішинговим листам»

Заповнимо інформацією (рис. 3.3).

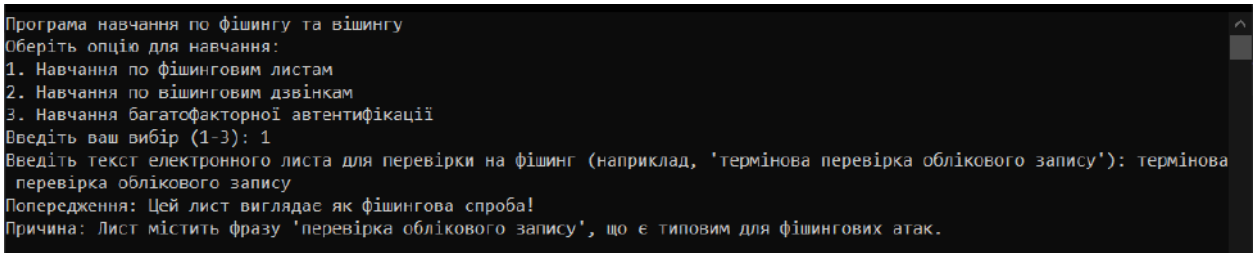

Рис. 3.3 – Результат «Навчання по фішинговим листам»

Запустимо ще раз і уведемо інший текст (рис. 3.4).

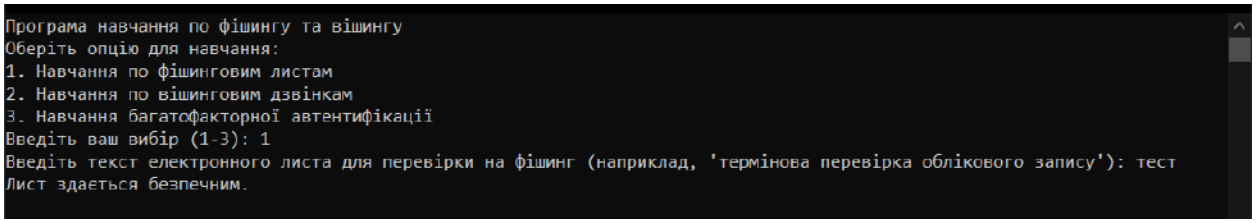

Рис. 3.4 – Результат «Навчання по фішинговим листам»

Перейдемо до пункту «Навчання по вішинговим дзвінкам» (рис. 3.5).

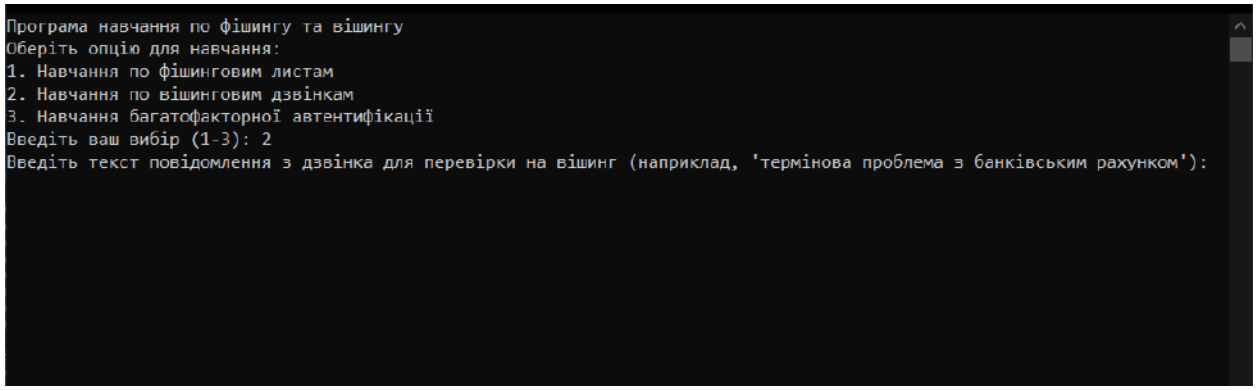

Рис. 3.5 – «Навчання по вішинговим дзвінкам»

Заповнимо інформацією (рис. 3.6).

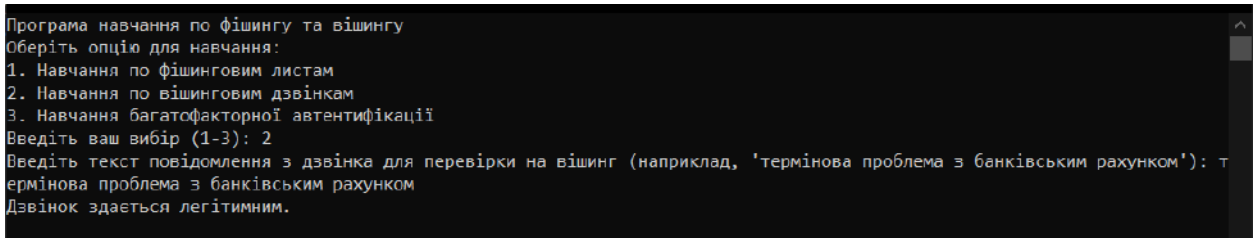

Рис. 3.6 – Результат «Навчання по вішинговим дзвінкам»

Оберемо «Навчання багатофакторної автентифікації» (рис. 3.7).

Рис. 3.7 – Результат «Навчання багатофакторної автентифікації»

У цьому підрозділі було детально розглянуто процес використання програми для навчання користувачів з виявлення фішингових листів, вішингових дзвінків та застосування багатофакторної автентифікації.

Після запуску програми користувач отримує головне меню, в якому є три основні варіанти для навчання. Кожен з них спрямований на підвищення обізнаності про різні типи кіберзагроз.

Вибравши опцію для навчання з фішингових листів, користувач вводить текст листа, який програма аналізує на наявність підозрілих фраз. Якщо такі фрази знайдені, програма видає попередження або повідомлення про безпеку. Цей процес було повторено для іншого тексту, що підтвердило правильність роботи функціоналу.

Далі, при виборі навчання по вішинговим дзвінкам, користувач вводить текст повідомлення з дзвінка, і програма перевіряє його на підозрілі фрази, знову видаючи попередження про можливу загрозу.

Останній етап передбачає навчання багатофакторної автентифікації. Користувач вводить код, який програма перевіряє на правильність, повідомляючи про успішну автентифікацію або помилку.

Програма ефективно виконує функцію навчання користувачів, дозволяючи їм на практиці перевіряти фішингові листи, вішингові дзвінки та проходити тестування на багатофакторну автентифікацію. Інтерфейс є інтуїтивно зрозумілим, а процес навчання — доступним і наочним. Це

допомагає підвищити рівень безпеки користувачів і їхню здатність розпізнавати потенційно небезпечні ситуації.

ВИСНОВКИ

У процесі виконання курсової роботи було досліджено ключові аспекти соціальної інженерії в кіберпросторі, а також розроблені теоретичні та практичні засоби для її протидії.

У першому розділі були проаналізовані наукові дослідження, що стосуються соціальної інженерії та її ролі в кіберзагрозах. Було визначено, що соціальна інженерія є однією з найбільших загроз для інформаційної безпеки, оскільки вона експлуатує людський фактор, що робить її складною для виявлення і захисту. Класифікація методів атак дозволяє більш детально вивчити різноманітні способи маніпулювання людьми, які використовуються зловмисниками для досягнення своїх цілей. Аналіз існуючих досліджень виявив важливі проблеми та недоліки в наявних підходах, зокрема недостатню увагу до постійного оновлення методів протидії в умовах швидко змінюваного цифрового середовища.

Другий розділ присвячено розробці теоретичних засобів боротьби з соціальною інженерією. У цьому розділі була запропонована теоретична модель реагування на загрози соціальної інженерії, що включає поетапну стратегію захисту користувачів і організацій. Описані алгоритми навчання користувачів для запобігання атак, які покликані підвищити їх обізнаність та навички виявлення шахрайства.

У третьому розділі було реалізовано програмний інструмент для навчання користувачів на прикладі консольного додатку на C++. Створення і тестування цього інструмента дозволило оцінити ефективність запропонованих методів навчання в умовах реальних сценаріїв. Програмний інструмент показав свою здатність надавати корисну інформацію та інтерфейс для тренування користувачів, що може бути використано як основа для подальших розробок в сфері підвищення обізнаності про кіберзагрози.

Таким чином, виконане дослідження підтвердило важливість розробки нових підходів та інструментів для протидії соціальній інженерії, а також продемонструвало можливості використання програмних засобів для

навчання користувачів. Розроблені методи та інструменти можуть бути ефективно використані в освітніх і корпоративних програмах для підвищення рівня безпеки та зменшення ризиків від соціальних атак у кіберпросторі.

ПЕРЕЛІК ЛІТЕРАТУРИ

1. Легомінова С., Гайдур Г. Аналіз сучасних загроз інформаційній безпеці організацій та формування інформаційної платформи протидії їм // Кібербезпека: освіта, наука, техніка. 2023. №2(22). С. 54–67. URL: https://doi.org/10.28925/2663-4023.2023.22.5467 .

2. Trellix. 2024 Threat Predictions. URL: https://www.trellix.com/about/newsroom/stories/research/trellix-2024-threat-predictions .

3. Tripathi S. Underground Development of Malicious LLMs // Trellix. URL: https://www.trellix.com/about/newsroom/stories/research/trellix-2024-threat-predictions .

4. Ajeeth S. The Resurrection of Script Kiddies // Trellix. URL: https://www.trellix.com/about/newsroom/stories/research/trellix-2024-threat-predictions .

5. Phuc P. The Stealthy Assault on Edge Devices // Trellix. URL: https://www.trellix.com/about/newsroom/stories/research/trellix-2024-threat-predictions .

6. Gartner. Hype Cycle for Endpoint Security, 2023. URL: https://www.gartner.com/en/documents/4589999 .

7. Kersten M. Python in Excel Creates a Potential New Vector for Attacks // Trellix. URL: https://www.trellix.com/about/newsroom/stories/research/trellix-2024-threat-predictions .

8. Chandra A. LOL Drivers Are Becoming a Game Changer // Trellix. URL: https://www.trellix.com/about/newsroom/stories/research/trellix-2024-threat-predictions

9. Gartner. Magic Quadrant for Endpoint Protection Platforms, 2022.

10. Штонда Р., Черниш Ю., Мальцева І., Чайка Є., Поліщук С. Практичні підходи до кіберзахисту мобільних пристроїв за допомогою рішення endpoint detection and response // Кібербезпека: освіта, наука, техніка. 2023. №1(21). С. 17–29.

11. Palo Alto Networks. Annual Report & Proxy Statement, 2022. URL: https://investors.paloaltonetworks.com/static-files/137ede42-9e7b-4eac-9a6d-197f697bd96d .

12. Microsoft. Gartner Named Microsoft a Leader in the 2021 Endpoint Protection Platforms Magic Quadrant. URL: https://www.microsoft.com/en-us/security/blog/2021/05/11/gartner-names-microsoft-a-leader-in-the-2021-endpoint-protection-platforms-magic-quadrant/ .

13. Шудрова К. Соціальна інженерія в інформаційній безпеці // Директор з безпеки. 2012. №10. С. 13–17.

14. Бойко О. М. Розробка методології захисту інформації від атак соціальної інженерії: дипломна робота магістра. Тернопіль : ТНТУ, 2020. 63 с.

15. Митник К. Д. Мистецтво обману. NYC : Wiley Books, 2008. 273 с.

16. Хорошко В. О., Чекатков А. А. Методи і засоби захисту інформації: підручник для ВНЗ. Київ : Юніор, 2013. 504 с.

17. Інформаційні моделі, системи та технології: матеріали VI наук.-техн. конф., 12–13 грудня 2018 р. Тернопіль : ТНТУ, 2018. 80 с.

18. Ткачук М. Ф. Виявлення та попередження атак соціальної інженерії. Ужгород : УжНУ, 2023. 230 с.

19. Грищенко О. І. Аналіз і протидія кібератакам: теорія та практика. Київ : Видавництво КПІ, 2022. 280 с.

20. Федорчук Ю. Л. Захист персональних даних в епоху ШІ. Івано-Франківськ : ІФНТУНГ, 2021. 198 с.

21. Кравченко В. С. Класифікація соціальних інженерних атак: підходи та рішення. Чернівці : ЧНУ, 2023. 315 с.

22. Стеценко Н. Г. Інформаційна культура та кібербезпека. Херсон : ХДУ, 2020. 200 с.

23. Голуб О. В. Інтеграція великих мовних моделей у системи захисту. Миколаїв : МНУ, 2023. 250 с.

ДОДАТОК

```
#include <iostream>
#include <string>
#include <vector>
#include <algorithm>
using namespace std;

bool checkPhishingEmail(string email, string& reason) {
    transform(email.begin(), email.end(), email.begin(), ::tolower);
    email.erase(remove_if(email.begin(), email.end(), ::isspace), email.end());

    vector<string> suspiciousPhrases = {
        "терміново", "підтвердити", "попередження", "необхідно",
"заблоковано", "аккаунт",
        "перевірка", "фінансові", "дані", "безпека", "повідомлення", "пароль",
"оновлення",
        "підтвердження", "платіж", "інформація", "переказ", "код", "рахунок",
"підтримка",
        "банківський", "депозит", "запит", "відновлення", "покупка", "приз",
"контроль",
        "зміни", "оплата", "повторно", "платіж", "порушення", "транзакція",
"виплата",
        "підтвердження", "акція", "повторіть", "запит на платіж", "скасування",
"підтвердьте",
        "платіжний", "підозрілість", "відновити", "повернення", "повідомлення
від банку",
        "пошкодження", "міжнародний", "помилкова операція", "скидання",
"кредитна картка",
        "необхідно діяти", "награда", "погашення", "запит на підтвердження",
"доступ", "введення коду",
        "картка заблокована", "попереднє повідомлення", "запит на гроші",
"повернення коштів",
        "зареєструйте", "вхід", "оголошення", "спроба доступу", "запит на
верифікацію",
        "підозріла активність", "помилкова транзакція", "запит на відновлення",
"термінове підтвердження",
        "щодо вашого акаунту", "система безпеки", "потрібно перевірити",
"несподівана перевірка",
        "активний запит", "довіри", "неочікуваний вхід", "повідомлення про
заборону", "термінова відповідь",
        "відкликання", "термінова перевірка", "відновлення доступу",
"міжнародні виплати", "рекомендація змінити",
        "усунення помилки", "актуалізація", "оплата за товар", "відновлення
рахунку", "підтвердження оплати",
```

```
        "нагадування про операцію", "отримання бонусів", "перевірити дані",
"сервіс підтвердження",
        "доступ до інформації", "нещодавня транзакція", "ознайомлення з
результатами", "зміна карти",
        "небезпека акаунта", "запит на виплату", "відновлення доступу до
акаунту", "повідомлення від вашого банку"
    };

    for (const auto& phrase : suspiciousPhrases) {
        if (email.find(phrase) != string::npos) {
            reason = "Лист містить фразу '" + phrase + "', що є типовим для
фішингових атак.";
            return true;
        }
    }
    return false;
}

bool checkVishingCall(string phoneCall, string& reason) {
    transform(phoneCall.begin(), phoneCall.end(), phoneCall.begin(), ::tolower);
    phoneCall.erase(remove_if(phoneCall.begin(), phoneCall.end(), ::isspace),
phoneCall.end());

    vector<string> suspiciousPhrases = {
        "терміново", "ваш рахунок", "рахунок заблоковано", "підтвердіть",
"терміново зателефонуйте",
        "необхідно оновити інформацію", "гарантований виграш", "платіж за
рахунком", "відновлення рахунку",
        "неправомірні дії", "необхідно повідомити код", "ви виграли в лотереї",
"проблеми з вашим акаунтом",
        "термінова перевірка", "повідомлення від служби безпеки",
"підтвердження особистих даних",
        "ваш доступ заблоковано", "проблеми з фінансовою інформацією",
"потрібно змінити пароль",
        "картка заблокована", "проблема з вашим рахунком", "необхідно
підтвердити дані", "відновлення доступу",
        "операція в небезпеці", "ми спостерігаємо підозрілу активність",
"податкова перевірка", "термінова перевірка",
        "вам потрібно ввести код", "замороження рахунку", "невідомі витрати",
"підтвердження операцій",
        "виплата через код", "помилка обробки платежу", "запит на перевірку",
        "кредит на картці", "неправомірні платежі", "зміни в умовах операцій",
"виплата на картку", "платіж за товар",
```

```
        "нове поповнення", "терміново сплатити борг", "зміна платіжних даних",
"повторний платіж", "виплата через SMS",
        "повідомлення про вашу картку", "надіслано повідомлення на вашу
картку", "необхідно активувати рахунок",
        "заблоковані платежі", "стягнення боргів", "підтвердження через
телефон", "зміна картки", "неправомірна транзакція"
    };

    for (const auto& phrase : suspiciousPhrases) {
        if (phoneCall.find(phrase) != string::npos) {
            reason = "Повідомлення містить фразу '" + phrase + "', що є типовим
для вішингових атак.";
            return true;
        }
    }
    return false;
}

bool checkMultiFactorAuth(string inputCode, string correctCode) {
    return inputCode == correctCode;
}

void phishingTraining() {
    string email;
    string reason;
    cout << "Введіть текст електронного листа для перевірки на фішинг
(наприклад, 'термінова перевірка облікового запису'): ";
    getline(cin, email);

    if (checkPhishingEmail(email, reason)) {
        cout << "Попередження: Цей лист виглядає як фішингова спроба!\n";
        cout << "Причина: " << reason << endl;
    }
    else {
        cout << "Лист здається безпечним.\n";
    }
}

void vishingTraining() {
    string phoneCall;
    string reason;
    cout << "Введіть текст повідомлення з дзвінка для перевірки на вішинг
(наприклад, 'термінова проблема з банківським рахунком'): ";
    getline(cin, phoneCall);
```

```
    if (checkVishingCall(phoneCall, reason)) {
        cout << "Попередження: Це повідомлення виглядає як вішингова
спроба!\n";
        cout << "Причина: " << reason << endl;
    }
    else {
        cout << "Дзвінок здається легітимним.\n";
    }
}

void multiFactorAuthTraining() {
    string correctCode = "123456";
    string inputCode;
    cout << "Введіть код автентифікації: ";
    getline(cin, inputCode);

    if (checkMultiFactorAuth(inputCode, correctCode)) {
        cout << "Автентифікація успішна!\n";
    }
    else {
        cout << "Не вдалося автентифікувати. Спробуйте ще раз.\n";
    }
}

int main() {
    int choice;

    cout << "Програма навчання по фішингу та вішингу\n";
    cout << "Оберіть опцію для навчання:\n";
    cout << "1. Навчання по фішинговим листам\n";
    cout << "2. Навчання по вішинговим дзвінкам\n";
    cout << "3. Навчання багатофакторної автентифікації\n";
    cout << "Введіть ваш вибір (1-3): ";
    cin >> choice;
    cin.ignore();

    switch (choice) {
    case 1:
        phishingTraining();
        break;
    case 2:
        vishingTraining();
        break;
```

```
    case 3:
        multiFactorAuthTraining();
        break;
    default:
        cout << "Невірний вибір. Вихід з програми.\n";
        break;
    }

    return 0;
}
```