Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ПОЯСНЮВАЛЬНА ЗАПИСКА

Дипломної роботи
магістра
(назва освітньо-кваліфікаційного рівня)

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

спеціальність *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*
(назва освітньої програми)

освітньо-наукова програма *кібербезпека*

на тему: Удосконалений метод захисту персональних даних від атак соціальної інженерії

Виконавець: студентка ІІ курсу, групи КБм-21

(підпис)	**Прокопенко Аліна Миколаївна** (прізвище ім'я по-батькові)

	Прізвище, ініціали	**Оцінка**	**Підпис**
Науковий керівник	Лукова-Чуйко Н. В.		
Рецензент	Гнатюк С. О.		
Нормоконтроль	Фесенко А. О.		

Київ 2022

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри кібербезпеки
та захисту інформації
_____ Н.В. Лукова-Чуйко
«__» _____ 2021 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

студентці КБм-21 (група) Прокопенко Аліні Миколаївні (прізвище ім'я по-батькові)

Тема дипломної роботи Удосконалений метод захисту персональних даних від атак соціальної інженерії

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 5 від 29.10.2021

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень Процес захисту персональних даних.

Предмет досліджень Методи протидії соціальної інженерії

Мета Удосконалити вже існуючий метод захисту персональних даних від атак соціальної інженерії.

Вихідні дані для проведення роботи Методи виявлення фішингових атак.

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна Удосконалення методу захисту персональних даних від атак соціальної інженерії шляхом розробки тренінгу з вирішення проблеми реальними випадками.

Практична цінність Запропонований метод може використовуватися організаціями для виявлення фішингових атак.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота виконана у повному обсязі відповідно до теми.

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Розробка плану для досягнення мети роботи	29.10.2021 – 30.11.2021
Аналіз літературних джерел	01.01.2022 – 14.02.2022
Вдосконалення методу виявлення фішингових атак та розробка рішення відповідно до даного методу	15.02.2022 – 24.04.2022
Оформлення і друк пояснювальної записки	25.04.2022 – 19.05.2022

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект Зниження збитків через викрадення даних

Соціальний ефект Підвищення знань користувачів щодо виявлення фішингових атак.

7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ Лукова-Чуйко Н. В.
(підпис) (прізвище, ініціали)

Завдання прийняв до виконання _____ Прокопенко А. М.
(підпис) (прізвище, ініціали)

Дата видачі завдання: _____
Термін подання дипломної роботи до ЕК _____

УДК 316.776

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Удосконалений метод захисту персональних даних від атак соціальної інженерії»: 56 сторінок, 16 рисунків, 2 таблиці, 2 додатки, 45 джерел.

Об’єкт дослідження – процес захисту персональних даних.

Мета роботи – удосконалити вже існуючий метод захисту персональних даних від атак соціальної інженерії.

Предмет дослідження – методи протидії соціальної інженерії.

Методи дослідження – аналіз, мозковий штурм, вивчення реальний випадків.

У спеціальній частині дана характеристика типам атак та механізму атаки соціальної інженерії, проведено аналіз існуючих методів виявлення фішингу. Запропоновано удосконалений метод виявлення фішингу та розроблене рішення відповідно до даного методу.

Наукова новизна роботи полягає в удосконаленні методу захисту персональних даних від атак соціальної інженерії шляхом доповнення вже існуючого методу навчання користувачів шляхом тренінгу з вирішення проблеми реальними випадками.

Практична цінність отриманих результатів полягає в тому, що запропонований метод може використовуватися організаціями для виявлення фішингових атак.

В подальшому запропонований метод може використовуватися організаціями та експертами з соціальної інженерії для створення нових тренінгів з метою навчання користувачів відповідно до поставлених перед ними задач.

Напрямки подальших досліджень полягають в удосконаленні наявних методів виявлення фішингу, адаптуючи їх до сучасного світу, оскільки технології

розвиваються, атаки вдосконалюються, зловмисники отримують більше практичного досвіду.

Ключові слова: соціальна інженерія, захист інформації, методи та засоби соціальної інженерії, протидія атакам, атаки соціальної інженерії, захист персональних даних.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ЄДРПОУ - Єдиний державний реєстр підприємств та організацій України
ЄС - Європейський Союз
ЗУ - Закон України
ІКС - Інформаційно-комунікаційна система
ІС - Інформаційна система
ІТС - Інформаційно-телекомунікаційна система
ПД - Персональні дані
ПЗ - Програмне забезпечення
ПК - Персональний комп’ютер
СІ - Соціальна інженерія
DNS - Domain Name System
DOM - Document Object Model
HTML - HyperText Markup Language

ВСТУП

Соціальна інженерія – це такий нетехнічний тип стратегії кібератак, який базується на взаємодії між людьми та маніпуляціях таким чином, щоб людина порушила стандартні правила кібербезпеки. Автором даного поняття вважається Кевін Митник. Для таких атак не потрібно бути хакером і знати купу технічної інформації, тому зловмисники активно використовують дану тактику. Легше обманом отримати бажане, ніж зламувати програмне забезпечення, наприклад, людина за власним бажанням передасть вам свій пароль, аніж ви спробуєте зламати його. Проте соціальна інженерія вимагає від зловмисника гарної підготовки, що зазвичай має на меті збір інформації про жертву, аби точно знати, як саме можна отримати бажану інформацію.

У сучасному світі найвразливішою ланкою серед усіх кібератак залишається людина. Пандемія тільки підтвердила цей факт, оскільки кількість фішингових атак протягом 2020-2021 років збільшилась. Фішинг використовується для крадіжки особистих даних та встановлення шкідливих програм.

Соціальна інженерія – одна з тих галузей, які розвиваються дуже стрімко. Технології не стоять на місці, психологія розвивається, проводяться нові дослідження, публікуються результати. Усім цим активно користуються зловмисники.

Час також грає проти вас, оскільки атаки зазвичай відбуваються доволі швидко, ще до того, як людина зрозуміє, що трапилося щось не те. За цей час може відбутися кілька атак одночасно за тією ж схемою. Звісно, опісля схема атаки викриється, додасться необхідна інформація в усі алгоритми, але певна кількість людей вже стануть жертвами зловмисників за цей час.

Людська цікавість також грає проти людей. Цікавість перейти за посиланням і подивитись «що там» або перетелефонувати особі з СМС. Таким чином людина сама віддає себе в руки зловмисників. І цим вони теж активно користуються.

Людина – істота соціальна, їй схильно мати друзів і ворогів. Цим теж користуються зловмисники, маскуючись під перших чи других. Наприклад, пишуть від імені вашого хорошого друга, що йому потрібні кошти вже тут і зараз, питання життя і смерті. І тут також варто не втрачати пильності і перетелефонувати другові спитатися, чи це справді він вам написав.

Списки таких прогалин і недоліків можна довго продовжувати, проте висновок один: методи протидії та виявлення атак соціальної інженерії потребують регулярних переглядів та вдосконалень.

Отже, актуальність даної теми зумовлена потребою удосконалення методів захисту від атак соціальної інженерії.

РОЗДІЛ 1
ПЕРСОНАЛЬНІ ДАНІ У СОЦІАЛЬНІЙ ІНЖЕНЕРІЇ

1.1 Класифікація інформації

Інформація, яка зберігається та обробляється підлягає класифікації. Інформація, що обробляється у ІКС, поділяється на відкриту та на інформацію з обмеженим доступом. До відкритої інформації, наприклад, можемо віднести нормативно-довідкову інформацію, медіаресурси, файли зображень, файли оновлень ПЗ тощо. До інформації з обмеженим доступом належить конфіденційна інформація, службова та таємна. Також до інформації з обмеженим доступом належить технологічна інформація – налаштування апаратних та програмних засобів ІТС, атрибути та права доступу користувачів, облікові записи користувачів, правила розмежування доступу, журнали реєстрації подій компонентів ІТС, ключові дані, необхідні для шифрування та електронного цифрового підпису даних тощо.

Закон України “Про інформацію” [1] окреслює конфіденційну інформацію як інформацію про фізичну особу, а також інформацію, доступ до якої обмежено фізичною або юридичною особою. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом

Комерційною таємницею є інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію. [2]

У той же час Кабінет Міністрів України визначає Постановою від 9 серпня 1993 р. N 611 “Про перелік відомостей, що не становлять комерційної таємниці” чіткий перелік інформації, яка не належить до комерційної таємниці [3]:

- установчі документи, документи, що дозволяють займатися підприємницькою чи господарською діяльністю та її окремими видами;
- інформація за всіма встановленими формами державної звітності;
- дані, необхідні для перевірки обчислення і сплати податків та інших обов'язкових платежів;
- відомості про чисельність і склад співробітників, їхню заробітну плату в цілому та за професіями й посадами, а також наявність вільних робочих місць;
- документи про сплату податків і обов'язкових платежів;
- документи про платоспроможність;
- відомості про участь посадових осіб підприємства в кооперативах, малих підприємствах, спілках, об'єднаннях та інших організаціях, які займаються підприємницькою діяльністю;
- відомості, що відповідно до чинного законодавства підлягають оголошенню.

Право інтелектуальної власності на комерційну таємницю належить особі, яка на законних підставах визначила інформацію комерційною таємницею, оскільки комерційна таємниця є об'єктом інтелектуальної власності. До майнових прав власника комерційної таємниці належать виключне право перешкоджати неправомірному розголошенню, збиранню або використанню комерційної таємниці.

1.2 Поняття персональних даних

Закон України "Про захист персональних даних" [4] визначає персональні дані як відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Це найуживаніше визначення даного поняття - і воно є найбільш узагальненим. Перелік відомостей, які належать до персональних даних, змінюється від однієї держави до іншої. Наприклад, інформація про IP-адресу в країнах Європейського Союзу належить до персональних даних, а у Сполучених Штатах Америки ні, проте відноситься до інформації, що пов'язана з персональними даними.

Також вищезгаданий ЗУ визначає ще кілька важливих термінів.

Суб’єкт персональних даних - фізична особа, персональні дані якої обробляються.

Розпорядник персональних даних - фізична чи юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця.

База персональних даних - іменована сукупність упорядкованих персональних даних в електронній формі та/або у формі картотек персональних даних;

Володілець персональних даних - фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом;

Згода суб’єкта персональних даних - добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди.

Знеособлення персональних даних - вилучення відомостей, які дають змогу прямо чи опосередковано ідентифікувати особу;

Обробка персональних даних - будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем;

Третя особа - будь-яка особа, за винятком суб’єкта персональних даних, володільця чи розпорядника персональних даних та Уповноваженого Верховної Ради України з прав людини, якій володільцем чи розпорядником персональних даних здійснюється передача персональних даних.

Регламент (ЄС) 2016/679 Європейського Парламенту та Ради [5] надає більш розширене визначення персональним даним.

“Персональні дані” означає будь-яку інформацію, що стосується ідентифікованої або потенційно можливо ідентифікованої фізичної особи - суб’єкта даних.

Потенційно можлива ідентифікована фізична особа - це така особа, яку можна ідентифікувати, прямо чи опосередковано, зокрема, шляхом посилання на такий ідентифікатор, як ім'я, ідентифікаційний номер, дані про місцезнаходження, онлайн ідентифікатор, один або кілька факторів, характерних для фізичної, фізіологічної, генетичної, психічної, економічної, культурної або соціальної ідентичності цієї фізичної особи.

Приклади персональних даних:

- прізвище, ім’я, по-батькові;
- домашня адреса;
- дата народження, дата весілля;
- дівоче прізвище мами, бабусі;
- електронна адреса, яка містить ім’я і прізвище;
- дані про місцезнаходження;
- ідентифікаційний номер;
- номер внутрішнього, закордонного паспорта або будь-якого аналогічного документу;
- медичні дані.

Приклади інформації, яка не є персональними даними:

- реєстраційний номер підприємства, в Україні - код ЄДРПОУ;
- знеособлена інформація;
- електронні адреси такі, як info@example.com, support@example.com.

Персональні дані можуть бути як конфіденційною інформацією, так і відкритою. Пункт 2 статті 11 ЗУ “Про інформацію” [1] встановлює, що конфіденційними є зокрема дані про національність, освіту, сімейний стан, релігійні переконання, стан здоров’я, місце проживання і/або реєстрації, дата і місце народження.

1.3 Загрози персональним даним

Згідно з українським законодавством [6] не допускаються збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини. А отже, загрози персональним даним можна описати наступним чином - це загрози несанкціонованого зберігання, використання та поширення конфіденційних даних.

За згодою суб’єкта персональних даних конфіденційна інформація може оброблятися і зберігатися розпорядником, мету в цей час визначає володілець даних. Таким чином, володілець і розпорядник несуть відповідальність за дотримання конфіденційності довіреної їм інформації. Будь-які дані зберігаються в інформаційних системах, а отже, мова йтиме про загрози персональним даним, які зберігаються та обробляються в ІС.

Усі загрози можна умовно поділити на такі, які можуть бути реалізовані внаслідок атак, та такі, які не залежать від атак.

Загрози, які не пов’язані з цілеспрямованими атаками, можуть як призвести до втрати, спотворення або компрометації персональних даних суб’єкта, так і створити умови для їх використання зловмисниками.

Такими загрозами можуть бути:

- такі, що не пов'язані з діяльністю людини: стихійні лиха та природні явища (землетруси, повені, урагани тощо);
- загрози соціально-політичного характеру: страйки, диверсії, локальні конфлікти, війна, що супроводжуються нападом на об'єкт, що містить ресурси інформаційної системи, тощо;
- помилкові дії та/або порушення персоналом та користувачами інформаційної системи вимог до відповідної експлуатаційної, організаційної, технічної чи іншої документації;

- загрози антропогенного характеру, наприклад: аварії та різного роду несправності та перешкоди, що призводять до порушень і збоїв у роботі апаратних компонентів інформаційної системи.

Захист від загроз, які не залежать від атак, регулюється інструкціями, розробленими та затвердженими уповноваженими службами розпорядника персональних даних, з урахуванням специфічних умов функціонування інформаційної системи, а також чинних нормативних документів.

Захист від загроз, які можуть бути реалізовані внаслідок атаки, повинен забезпечуватися за допомогою захисних заходів і засобів, які використовуються інформаційною системою і призначені переважно для протидії атакам.

Склад і зміст загроз безпеки ПД визначається сукупністю умов і факторів, що створюють загрозу несанкціонованого, у тому числі випадкового, доступу до ПД.

Сукупність таких умов і факторів формується з урахуванням особливостей ІС, властивостей середовища розповсюдження інформаційних сигналів, що містять захищену інформацію, та можливостей джерел загроз.

Наступні характеристики ІС можуть викликати загрози для ПД:

• структура, категорія та обсяг персональних даних, що обробляються в ІС;

• наявність підключень ІС до мереж зв'язку загального користування та/або Інтернету;

• характеристики підсистеми безпеки та режими обробки персональних даних;

• режими диференціації прав доступу користувачів ІС;

• розташування та умови розміщення технічного обладнання ІС.

Основними елементами ІС, в якій обробляються персональні дані, є:

• персональні дані, що містяться в базах даних, як сукупність інформації та її джерел, що використовуються в інформаційній системі;

• інформаційні технології, як сукупність методів і методів використання комп’ютерних технологій при обробці персональних даних;

• програмне та апаратне забезпечення, що обробляє персональні дані;

• засоби захисту інформації;

• додаткове обладнання та системи.

Загрози можна умовно класифікувати наступним чином:

• за видами можливих джерел загрози безпеці персональних даних, спричинених навмисними чи ненавмисними діями користувачів ІС: з доступом до неї чи без; джерела загроз щодо ІС можуть бути як зовнішніми, так і внутрішніми;

• за видами несанкціонованих дій з персональними даними:

- загрози конфіденційності даних;
- загрози цілісності даних;
- загрози доступності даних;

• за методами реалізації ризику безпеки персональних даних:

- загрози, реалізовані в ІС при їх підключенні до локальних мереж;
- загрози, реалізовані в ІС при їх підключенні до глобальних мереж;
- загрози, реалізовані в ІС, які не мають підключення до будь-яких мереж.

• за типом каналів реалізації ризику безпеки персональних даних:

- загрози, що реалізуються через технічні канали витоку інформації;
- загрози, що реалізуються програмними методами (за допомогою стандартного ПЗ або спеціально розробленого або прикладного ПЗ.

Висновки за розділом 1

Отже, у першому розділі було розглянуто базові поняття, які необхідні для розуміння проблематики роботи, а саме класифікація інформації; поняття персональних даних згідно українського та міжнародного законодавства та приклади; які існують загрози персональним даним, їх класифікація.

РОЗДІЛ 2
АТАКИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

2.1 Механізм атаки соціальної інженерії

Атака соціальної інженерії має спільну структуру. Вони відбуваються в один або кілька кроків [7].

На рис. 2.1 зображений життєвий цикл атаки СІ.

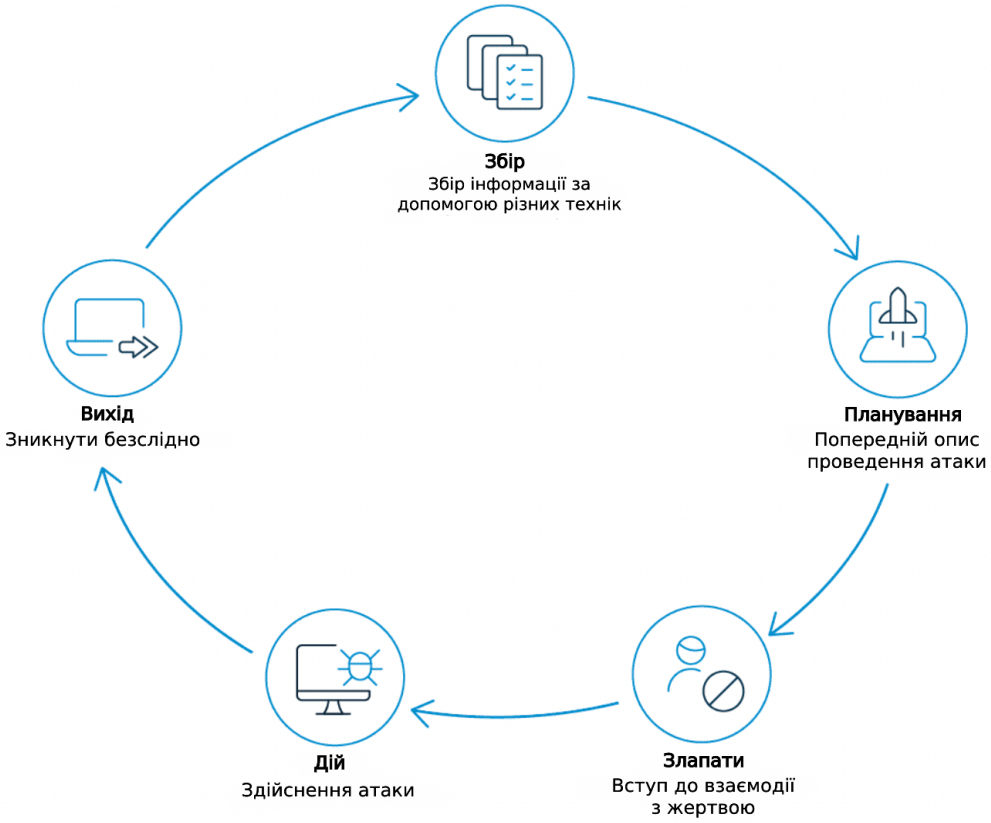

Рисунок 2.1 - Життєвий цикл атаки

1. Збір інформації та планування

Імовірність успіху більшості атак залежить саме від цієї фази, тому є логічним, що зловмисники приділяють цьому етапу більшу частину свого часу та уваги. Інформація може збиратися різними методами. Маючи правильну інформацію, зловмисник може визначити вектор атаки, можливі паролі, ймовірні

відповіді окремих осіб й уточнити цілі. На цьому етапі зловмисник дуже добре ознайомлюється з жертвою та формулює конкретний план атаки під дану особу.

2. Встановлення контакту з жертвою та взаємодія

На цьому етапі зловмисник встановлює контакт з жертвою та вибудовує довірливі стосунки. Це критична точка, оскільки якість встановленого контакту визначає рівень співпраці та міру, з якою жертва буде допомагати зловмисникові досягти мети. Наприклад, це може бути доволі короткотривалий контакт, як поспішати до дверей з широкою посмішкою та зоровим контактом, щоб жертва притримала двері відкритими для зловмисника. Це може бути особисте спілкування по телефону або смол-ток з секретарем у фойє. Водночас цей етап може бути більш масштабним - таким, як побудова онлайн-знайомство та встановлення стосунків із жертвою за допомогою фальшивого профілю на сайті знайомств або в соціальних мережах.

Після цього зловмисник використовує як зібрану інформацію, так і встановлений контакт, не викликаючи підозр. Далі відбувається взаємодія зловмисника і жертви, наприклад, це може бути реалізовано шляхом розголошення, здавалося б, неважливої інформації або доступу, наданого/переданого зловмиснику. Приклади успішної фази взаємодії включають:

- утримання дверей відкритими або введення зловмисника всередину приміщення;
- розкриття пароля та імені користувача по телефону;
- вставлення флеш-накопичувача USB із шкідливим ПЗ до комп’ютера компанії;
- відкриття зараженого вкладення електронної пошти
- розкриття комерційної таємниці під час обговорення з нібито «знайомим».

3. Виконання атаки

Ця фаза — це коли зловмисник досягає своєї кінцевої мети. Як правило, атака закінчується ще до того, як жертва починає розуміти, що відбувається. Натомість зловмисник має на меті закінчити атаку таким чином, щоб жертва почувалася так,

ніби вона зробив щось корисне для “знайомого”, тим самим забезпечуючи можливу подальшу взаємодію.

4. Вихід

Зловмисник стирає цифрові відбитки будь-якого свого перебування. В результаті нападник досягає двох важливих цілей. По-перше, жертва не знає, що напад відбувся. По-друге, зловмисник приховує свою особу. Добре спланована і плавна стратегія виходу є метою нападника і останнім актом в атаці.

2.2 Сфера застосування СІ

Сфера застосування СІ достатньо широка, однак Кевін Митник визначив наступні сфери, як основні [8].

- збір відкритої інформації про жертву, а саме з’ясування інтересів та особливостей поведінки потенційної жертви, соцмереж, якими вона користується, а також імен, під якими вона з’являється у мережі Інтернет, через ведення діалогу з нею або з її оточенням у службах обміну миттєвими повідомленнями;
- отримання конфіденційної інформації про об’єкт атаки або інформації, що становить для зловмисника певний інтерес, наприклад номери телефонів потенційної жертви, адресу її реєстрації, проживання, реальне ім’я та прізвище тощо, через встановлення контакту з нею або шляхом оману;
- отримання інформації про об’єкт атаки, необхідної для забезпечення НСД до системи, а саме пароля, яким користується потенційна жертва, серії та номеру паспорта та інших відомостей про неї шляхом входження в довіру до обраної жертви;
- примушення жертви до дій, необхідних порушникові, через нав’язування такому об’єкту нової моделі поведінки.

Наприклад. Проникнення в мережу організації для дестабілізації з певною метою роботи її основних вузлів.

Загальна дестабілізація роботи в організації з метою зниження її впливу, а згодом і повного її знищення.

Фінансові махінації в організації.

Фішинг та інші способи викрадення паролів із метою доступу до ПД тощо.

Розвідка ІТС. Викрадення клієнтських баз. Інформація про маркетингові плани організації. Загальна інформація про організацію, її сильні і слабкі ланки з метою подальшого знищення. Часто застосовується для рейдерських атак. Інформація про найбільш перспективних співробітників із метою їх подальшого переманювання до своєї організації.

2.3 Типи атак соціальної інженерії

Атаки соціальної інженерії не втрачають своєї популярності, з часом з'являються нові типи маніпулювання людьми, а отже і типи атак. На рисунку 2.2 зображені основні типи атак СІ.

Рисунок 2.2 – Атаки соціальної інженерії

Фішинг — це такий тип атак СІ, за якого зловмисник обманним шляхом заволодіває конфіденційною інформацією. В основному зловмисники використовують даний тип атак використовуючи електронну пошту (рис.2.3).

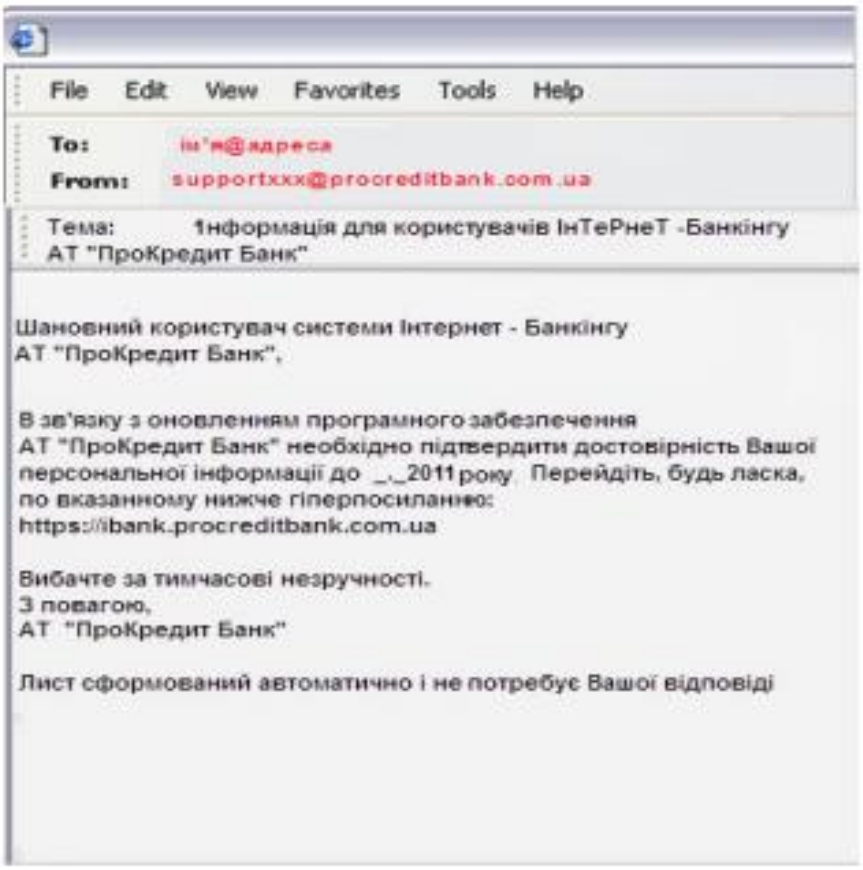

Рисунок 2.3 – Приклад фішингового електронного листа

Відтак існують найпопулярніші сценарії. Коли зловмисник надсилає фішинговий лист, він має на меті – змусити користувача виконати певні дії, щоб отримати певні дані для подальшої атаки, або ж встановити шкідливе ПЗ як частину більш широкомасштабної спроби проникнення. Фішингова атака матиме більше шансів бути успішною, якщо атака персоналізована під конкретного користувач. Таким чином зловмисник створює ілюзію того, що електронний лист отриманого з надійного джерела, а отже, це підвищує ймовірність того, що користувач прочитає цей лист або навіть виконає дії згідно з рекомендаціями зловмисника. Усі фішинг

атаки можуть бути поділені на 5 груп (рис 2.4): спрямований фішинг, полювання на корпоративних китів, телефонний фішинг, інтерактивний фішинг голосової відповіді та компромісний фішинг для ділової електронної пошти.

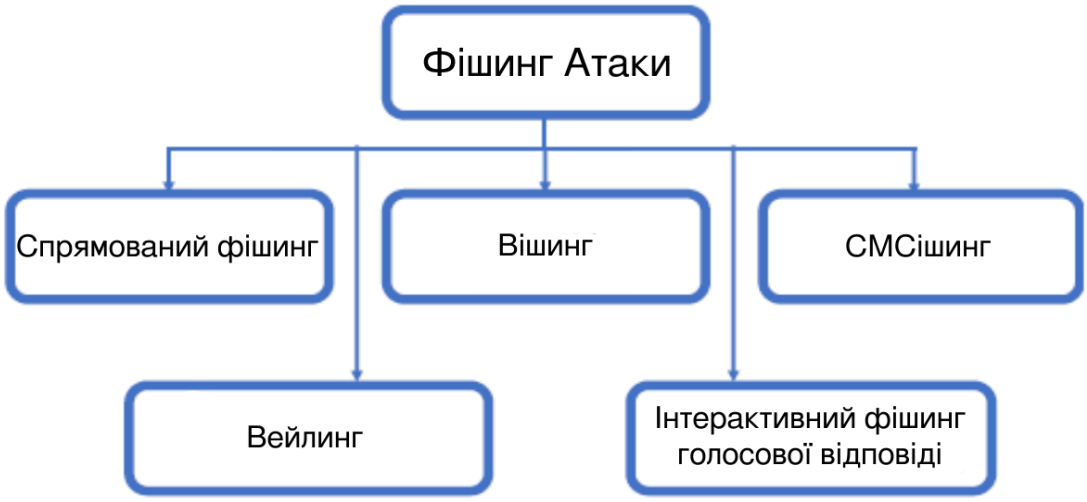

Рисунок 2.4 – Різновиди фішинг атак

Спрямований фішинг (spear phishing) – це цілеспрямована фішингова атака. Як звичайний, так і спрямований фішинг використовують електронну пошту, щоб досягнути мети. Але у випадку спрямованого фішингу персоналізовані електронні листи надсилають конкретній особі. Перед відправленням такого електронного листа зловмисник вивчає інтереси потенційної жертви. Найчастіше жертвами спрямованого фішингу є високі посадові особи, які мають доступ до більшої конфіденційної інформації, аніж пересічний робітник.

Телефонний або голосовий фішинг або вішинг (англ. vishing від поєднання Voice та Fishing) – це такий тип атаки, коли кіберзлочинець дзвонить за номером телефону й за допомогою створення відчуття невідкладності ситуації змушує людину вчиняти проти своїх інтересів. Такі дзвінки зазвичай відбуваються в стресовий час, наприклад, посеред ночі, коли людина раптово прокидається і має зрозуміти, що відбувається. Ці атаки є популярними, оскільки телефонні дзвінки знеособлені, оскільки жертва не бачить співрозмовника. А це надає неабиякі

переваги зловмиснику, оскільки завжди можна покласти слухавку і, наприклад, викинути сім-карту. У більшості країн вже існує обов'язкова реєстрація номеру з прив'язкою до паспортних даних особи, але навіть за такого сценарію, користувач має на це певний проміжок часу до блокування сім-карти, а це дає можливість бути знеособленим деякий період.

СМС фішинг (Smishing) – це вид фішингу, який використовує текстові повідомлення на мобільних телефонах. Злочинці видають себе за офіційне джерело, щоб завоювати довіру жертви (рис. 2.5). Наприклад, під час СМС фішингу зловмисник може надіслати жертві посилання на веб-сайт. Коли жертва відвідає цей веб-сайт, на мобільний телефон буде встановлене зловмисне ПЗ. Також популярний сценарій смс-фішингу, це смс-повідомлення з довільного або прихованого номеру ніби-то від банку з текстом «*Vasha karta bude zablokovana bankom. Terminovo proidit avtorizaciu, abo zatelefonuite…*».

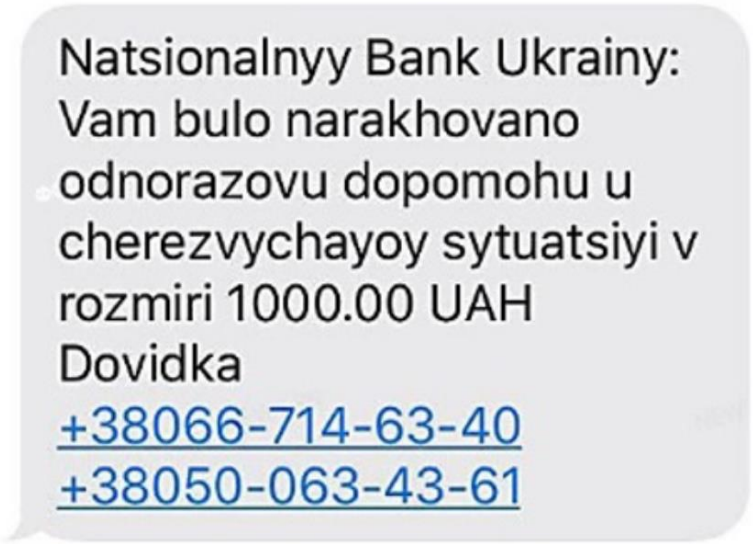

Рисунок 2.5 – Приклад СМСішингу

Whaling (полювання на корпоративних китів) – це фішингова атака, що спрямована на осіб, які мають повний доступ до інформації у межах організації, наприклад, її вище керівництво. Також цілями можуть бути політики або знаменитості. Термін вейлінг походить від розміру атак, а китів вибирають відповідно до їхніх повноважень у компанії. Через чітко спрямований характер

вейлінг-атаки часто важче виявити, ніж стандартні фішинг-атаки. На підприємстві адміністратори безпеки можуть допомогти знизити ефективність вейлінг-атак, залучаючи співробітників корпоративного управління пройти навчання з інформаційної безпеки.

Інтерактивний фішинг голосової відповіді виконується за допомогою інтерактивної системи голосового реагування, щоб жертва вводила приватну інформацію так, ніби вона отримала дзвінок від знайомого бізнесу або банку.

Компромісний фішинг для ділової електронної пошти імітує полювання на корпоративних китів, орієнтуючись на великих «риб» у корпоративних компаніях, щоб отримати доступ до їхніх ділових електронних листів, календаря, платежів, бухгалтерського обліку чи іншої приватної інформації. Соціальний інженер використовує ці дані для надсилання електронної пошти, змінюючи попередні електронні листи, для зміни графіку зустрічей, читання професійної інформації про підприємство та контакту з клієнтами чи постачальниками послуг. Зловмисник починає з дослідження високопосадових працівників через соціальні мережі, щоб знати та розуміти їхню професійну інформацію, таку як можлива кількість грошей, яку жертва може отримати від банку. Отримавши бажану інформацію, зловмисник надсилає дуже переконливий діловий електронний лист, щоб звичайний працівник натиснув на посилання або завантажив вкладення для компрометації мережі компанії. Зловмисник вибирає конкретний час відповідно до графіку жертва та створює в листі середовище екстреності дії, щоб працівник точно зробив те, що від нього очікують.

Фармінг (pharming) – це такий метод соціальної інженерії, коли зловмисник створює фальшивий веб-сайт, який імітує офіційний, щоб змусити користувачів вводити свої облікові та інші персональні дані, вважаючи, що вони підключені до легітимного сайту. Однією з технік, яка використовується при фармінг-атаці, є отруєння кешу DNS.

Диверсійні крадіжки полягають у неправильному направленні транспортної компанії для доставки кур’єра або посилки в потрібне місце.

Оманливе ПЗ (scareware) – це шкідливе ПЗ, яке переконує користувача здійснити конкретну дію, використовуючи його страх. Оманливе ПЗ створює спливаючі вікна, схожі на вікна діалогу операційної системи. Ці вікна містять підроблені повідомлення про те, що система знаходиться під загрозою, й інструкцію, що вам треба зробити, аби прибрати загрозу. Насправді жодних проблем немає і, виконуючи ті кроки, користувач самостійно дозволяє виконати зазначену програму, а вона, у свою чергу, встановить на його комп'ютер зловмисний код.

Поширений приклад оманливих програм – законні спливаючі вікна, що з’являються у веб-браузері під час серфінгу в Інтернеті, відображаючи такий текст, як: "Ваш комп'ютер може бути заражений шкідливими програмами". Він або пропонує встановити певний інструмент (часто заражений зловмисними програмами), або містить посилання на шкідливий сайт.

Також подібне програмне забезпечення може поширюватись за допомогою спам-електронної пошти, які містять неправдиві попередження або пропонує користувачам купувати непотрібні/шкідливі послуги.

Програми-вимагачі (Ransomware). Такі програми обмежують та блокують доступ до даних та файлів жертви, шифруючи їх. За першим сценарієм цього типу атак для розшифрування потрібно заплатити викуп, інакше – файли буде знищено. Інший варіант мети програм-вимагачів, шантаж розкриття даних, якщо не заплатити. Наслідки такої атаки можуть бути дорожчими, ніж сам викуп.

Бейтинг (приманка) або «Дорожнє яблуко» (road apple) – це коли зловмисник залишає заражений шкідливим програмним засобом фізичний пристрій, наприклад, флеш-диск USB, у місці, в якому його обов'язково знайдуть. Носій має виглядати як офіційний, мати логотип чи надпис, що зацікавить співробітника. Жертви підбирають наживку з цікавості і вставляють її на робочий або домашній комп’ютер, що призводить до автоматичного встановлення зловмисного програмного забезпечення в системі. Якщо співробітник вставить такий носій до комп'ютеру, що має зв'язок з корпоративною мережею підприємства, запускається шкідливий код і зловмисник отримує доступ до одного комп'ютера чи до усієї мережі.

Також існує онлайн-бейтинг. Це можуть бути привабливі оголошення, які призводять до шкідливих сайтів або спонукають користувачів завантажувати програми, заражені шкідливим програмним забезпеченням [9].

QUID PRO QUO (послуга за послугу) — несанкціоноване надання додаткових прав і можливостей зареєстрованим користувачам системи. Цей вид атаки передбачає дзвінок соціального інженера в організацію по корпоративному телефону. Здебільшого соціальний інженер представляється співробітником технічної підтримки, який здійснює опитування щодо виникнення технічних проблем. Під час «розв'язання» технічних проблем соціальний інженер «спонукає» користувача до введення команд, які дадуть змогу соціальному інженерові запустити або встановити шкідливе ПЗ на його комп'ютер [8].

Претекстинг полягає у створенні кіберзлочинцем такої вразливої для жертви ситуації, яка б спонукала її до розголошення конфіденційної інформації, яку б людина в інших умовах не надала би добровільно. Даній атаці передує збір інформації про жертву, аби атака була успішною.

Конкретним прикладом претекстинту є зворотна соціальна інженерія.[10].

Зворотна соціальна інженерія. Суть такої атаки полягає в тому, щоб змусити жертву самостійно звернутися до кіберзлочинця за послугою. Схема такої атаки зображена на рис. 2.6. Атаку можна поділити на 6 етапів. Перший етап, як завжди, - планування атаки. Зазвичай самій атаці передує невелика диверсія, наприклад, ініціація збою в роботі ПК, що підключений до мережі – це другий етап. На третьому етапі в жертви виникають певні труднощі, далі зловмисник чекає, поки жертва самостійно звернеться до нього за допомогою. Атака розрахована на те, щоб створити такий масштаб непрацездатності, аби жертва не звернулася до колег або керівництва і в той же час самостійно усунути збій не могла.

Рисунок 2.6 – Метод зворотної СІ

Троянський кінь. Ця техніка базується на цікавості або жадібності мети. Зловмисник відправляє e-mail, що містить у вкладенні важливе оновлення антивіруса, або навіть свіжий компромат на співробітника. Така техніка залишається ефективною, поки користувачі будуть сліпо клікати по будь-яким посиланням і вкладенням.

Пошук інформації в смітті – це ще один сценарій СІ, який навіть не вважається правопорушенням з правової точки зору. Тож персонал компанії має усвідомити неприпустимість безконтрольного поводження зі сміттям. Отже, вкрай важливим є знищення як паперових відходів, так і електронних носіїв. Це має бути налагоджений процес, а отже:

1) мають бути розроблені процедури знищення сміття;

2) ємності під сміття мають бути розміщені таким чином, аби вони знаходилися поза межами доступу сторонніх осіб;

3) потрібно управляти внутрішніми відходами;

4) визначити категорії інформації, а також спосіб, в який персонал має з нею поводитись.

Несанкціоноване проникнення на територію (Piggybacking або Tailgating) відбувається тоді, коли зловмисник проникає до зони з обмеженим доступом слідом за уповноваженою особою. Для цього зловмисники використовують декілька способів:

- Вдають ніби супроводжують уповноважену особу.
- Приєднуються до великої групи співробітників, вдаючи що також працюють в організації.
- Вибирають жертву, яка легковажно ставиться до правил безпеки на об'єкті.
- Несанкціоноване проникнення слідом за зареєстрованим користувачем.

Запобігти несанкціонованому проникненню можна використовуючи тамбур-шлюзи з двома дверима. Після того, як співробітники входять у зовнішні двері, ці двері необхідно закрити перед тим як увійти у внутрішні двері.

Індивідуальні підходи. До індивідуальних підходів можна віднести як негативні стратегії, так і позитивні. Існують чотири різновиди такого підходу [8]:

1) залякування (зловмисники, які обрали цю стратегію, примушують жертву виконати запит за допомогою шантажу або видачі себе за іншу особу);

2) переконання (найбільш звичні форми переконання передбачають застосування лестощів);

3) використання довірливих стосунків (потребує підготовчого періоду, протягом якого мають встановитися відповідні стосунки);

4) допомога (хакер пропонує допомогу потенційній жертві, аби змусити її оприлюднити особисту інформацію).

Щоб запобігти атакам, побудованим на особистісному підході, необхідно:

- визначити в політиці безпеки компанії, що служба підтримки — єдина інстанція, куди потрібно звернутися із проблемами;
- гарантувати, що служба підтримки має ефективний механізм реагування на звернення в межах встановленого рівня обслуговування;

- регулярно перевіряти виконання сервісних робіт, аби мати певність, що користувачі на належному рівні отримують відповіді на свої запити.

2.4 Соціальна інженерія під час пандемії

Пандемія COVID-19 стала однією з найбільших проблем сучасності. Хвороба має здебільшого тяжкий перебіг, важкі наслідки, найгірший з яких – смерть. Саме це є причиною того, що COVID-19 використовується в різноманітних шкідливих кампаніях, включаючи фішингові листи, СМС, дзвінки, шкідливе програмне забезпечення, програми-вимагачі і підроблені домени. Страх – це те, чим найбільше користуються зловмисники в даній ситуації. Страх посилюється стресовою ситуацією через посилення карантинних заходів, страхом за життя та здоров'я (як власного, так і близьких), недовірою до статистичних даних про кількість хворих та смертей від хвороби, різних штамів COVID-19, дезінформація щодо якості, доступності та наявних побічних ефектів вакцинації тощо. Люди готові вірити у все, щоб захистити себе від реальної чи потенційної загрози. І цим одразу ж користуються злочинці [11].

Станом на жовтень 2021 року кількість вакцинованих стрімко почала зростати, а кількість смертей почала зменшуватися [12]. Однак кількість атак соціальної інженерії не зменшилася, а лише змінила вектор. Головна темою для злочинців стала вакцинація.

Group-IB [13] — це глобальна компанія з пошуку загроз і кіберрозвідки, яка спеціалізується на розслідуванні та запобіганні високотехнологічних кіберзлочинів. Вони опублікували всебічний аналіз схем шахрайства в глобальному масштабі. Загалом на шахрайство припадає 73% усіх онлайн-атак: 56% — це шахрайство (обман, внаслідок якого жертва добровільно розкриває конфіденційні дані) і 17% — фішингові атаки (викрадення даних банківської картки). Використовуючи запатентовану технологію Digital Risk Protection (DRP), експерти Group-IB виявили понад 70 груп шахраїв, які використовували лише одну з шахрайських схем

Classiscam, 36 з яких були спрямовані на Європу. Було встановлено, що лише за рік за цією схемою зловмисники обдурили користувачів на 7 750 000 євро.

Згідно з аналізом Group-IB, кількість фішингових атак під час пандемії зросла більш, ніж вдвічі. Фішинг використовується для крадіжки особистих даних та встановлення шкідливих програм. Хакери маскують свої розсилки під адреси авторитетних організацій: наприклад, ВООЗ, податкових служб, Центру контролю та профілактики захворювань чи МОЗ України.

Фішингові атаки від фейкового МОЗ на тему вакцинації зафіксував Національний координаційний центр кібербезпеки при РНБО України [14]. Ця фішингова атака була спрямована на українських інтернет-користувачів, основною темою якої став початок вакцинації проти COVID-19 в Україні. Загальна схема атаки зображена на рис. 2.7.

Під час атаки на популярній хостинг-платформі була створена фейкова веб-сторінка, яка імітувала сайт МОЗ України. Для розміщення сторінки зловмисники зареєстрували кілька доменів, які нагадували офіційний домен МОЗ України – moz.gov.ua. На цій фейковій сторінці міститься інформація про початок обов’язкової вакцинації від COVID-19 з 25 січня 2021 з пропозицією завантажити файл (документ Word) з деталями. Цей документ має вбудований шкідливий код, який завантажує та виконує інший шкідливий сценарій, що забезпечує віддалений контроль над зараженим комп’ютером. Таким чином зловмисники отримували повний доступ до комп’ютера жертви.

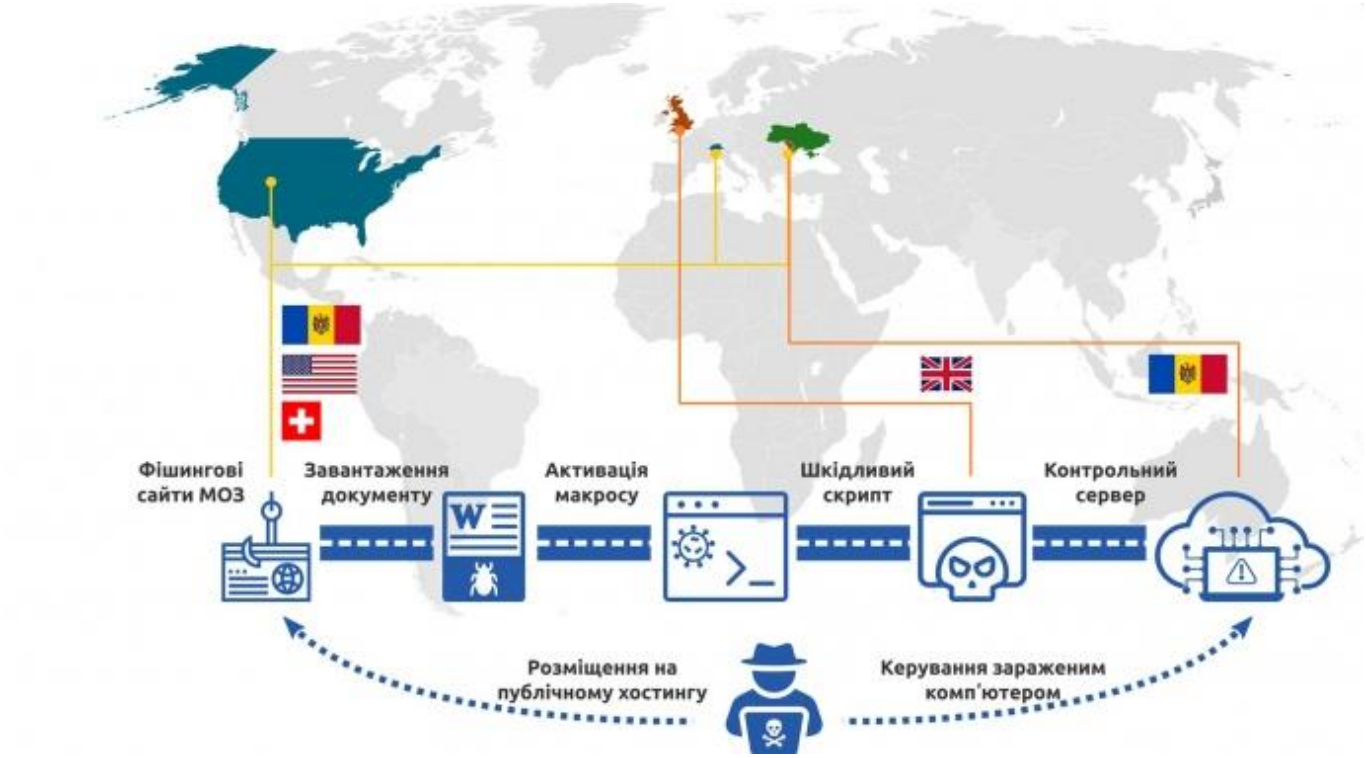

Рисунок 2.7 – Схема атаки

Звіт ENISA Threat Landscape (ETL) 2020 [15], опублікований Агентством кібербезпеки Європейського Союзу (ENISA), висвітлює ключові аспекти та тенденції, пов’язані з множиною загроз:

- зросла кількість фейкових веб-сайтів для онлайн-покупок і продавців-шахраїв;
- зросла кількість випадків кібербулінгу та вимагання;
- зловмисники використовують платформи соціальних мереж для підвищення ефективності цілеспрямованих атак;
- фінансова винагорода все ще є основною мотивацією для більшості кібератак;
- кількість жертв фішингу на темі COVID-19 в ЄС продовжує зростати;
- тематичні атаки COVID-19 включають повідомлення, які містять шкідливі вкладені файли, і повідомлення, які містять шкідливі посилання, які перенаправляють користувачів на фішингові сайти або зловмисне програмне забезпечення;

- багато випадків кібербезпеки залишаються непоміченими або виявляються через тривалий час;
- кількість потенційних загроз у віртуальному або фізичному середовищі продовжує збільшуватися, оскільки з’являється новий етап цифрової трансформації.

Ми бачимо, що пандемія негативно впливає на людей. Це викликано різними причинами, але наслідки однакові – зросла кількість нападів.

2.5 Виявлення фішингових атак

Можна виокремити два основних підходи до виявлення фішингу: навчання користувачів і за допомогою програмних засобів [16].

1) *Навчання користувачів*: користувачів можна навчити краще розуміти природу фішингових атак, що в результаті допоможе коректно розрізняти фішингові і справжні повідомлення. Це суперечить категоризації в роботі [17], де навчання користувачів розглядається як превентивний захід. Однак навчання має на меті розпізнавання користувачами фішингових атак, тому розглядається як підхід до виявлення фішингу.

2) *За допомогою програмних засобів*: цей підхід має на меті заповнити прогалину, яка виникає через помилку користувача або незнання, та розрізняти програмним способом фішингові та легітимні повідомлення. Цей недолік вимагає вирішення, оскільки навчання користувачів є дорожчим, ніж автоматична класифікація, та не завжди є можливим, наприклад, коли бази користувачів є завеликими (PayPal, eBay, Amazon тощо).

Розпізнавання фішингової атаки – це початкова точка протидії фішинговим атакам. На рисунку 2.8 показана схема підходів до розпізнавання фішингових атак.

Рисунок 2.8 - Підходи до розпізнавання фішингових атак

Ефективність виявлення може бути покращена за рахунок навчання класифікатора (як людини, так і ПЗ). У випадку з навчанням користувачів якість виявлення може бути покращена за рахунок їхнього індивідуального досвіду або за допомогою зовнішніх навчальних програм. У випадку програмної класифікації ефективність може бути підвищена в процесі в процесі “навчання” класифікатора, побудованого на алгоритмах машинного навчання, або вдосконаленням правил виявлення в системі на основі правил.

Методи виявлення базуються на методах контрзаходів, які можна умовно поділити як такі, які орієнтовані на людину, та ті, які орієнтовані на комп’ютер. У таблиці 2.1 порівнюються ці методи.

Таблиця 2.1

Порівняння методів

Метод	**Опис**	**Переваги**	**Недоліки**
Людина	Освіта	Легко піддаються навчанню	Можливість емоційного впливу
	Навчання		Відносність людських рішень

продовження таблиці 2.1

Людина	Інформованість	Невелика кількість жертв	Довірливість
			Жадібність
Комп'ютер	Програмне забезпечення	Ефективні	Дорога продукція
	Системи та інструменти	Точні	Обмежені людською необізнаністю
			Конкретне спрямування

Організація може мати один або кілька механізмів захисту. Проте організації варто застосовувати комбінації з людиноцентричних та комп'ютероцентричних методів захисту від атак. Чим більше методів застосовується, тим вищий рівень захисту від атак CI.

2.6 Програмний підхід до виявлення

Чорні списки. Це постійно оновлювані списки, що містять раніше виявлені фішингові URL-адреси. Недоліком даної методології є затримка в оновленні списків. Для того, щоб щойно створений фішинговий сайт потрапив у список, необхідний час. Цієї затримки між відправленням даних і додаванням сайту до списку може бути достатньо для досягнення зловмисниками своїх цілей.

Білі списки. Ці списки є чимось протилежним до чорних. Якщо є певна URL-адреса, її порівнюють з легітимною адресою зі базою даних "білого списку". База даних «білого списку» здебільшого містить список популярних справжніх URL-адрес та їхні важливі дані. Як і у випадку з чорним списком, для завантаження нової відомої URL-адреси може знадобитися певний час, через який. зловмисник, безсумнівно, може досягти своїх цілей. [18]

Евристичні методи виділяють певні характеристики веб-сторінки для того, щоб визначити легітимність веб-сайту, а не залежати від будь-яких попередньо

скомпільованих списків. Це перевага евристичних методів, над “списками”. Більшість цих характеристик витягуються з URL-адреси та дерево DOM даної веб-сторінки. Вилучені характеристики порівнюються з вже відомими, що були зібрані з фішингових та справжніх сторінок, щоб визначити їх легітимність. Деякі з цих підходів використовують евристики для обчислення оцінки підробки даної веб-сторінки, щоб перевірити її справжність. [19]

Сучасні веб-браузери та поштові клієнти побудовані з механізмами захисту від фішингу, такими як евристичні тести з метою виявлення фішингових атак. Так само евристичні тести виявлення фішингу можуть бути включені в антивіруси.

Методи візуальної схожості. Це методи розрізнення фішингових сайтів та легітимних сайтів за зовнішнім виглядом сайтів. Зазвичай фішингові сайти є майже точними копіями справжніх, щоб у користувача не виникали сумніви щодо легітимності ресурсу. З метою не бути виявленими зловмисники, як правило, вставляють зображення, Flash, ActiveX і Java-аплет замість HTML-тексту. Методи виявлення на основі візуальної схожості можуть швидко розпізнавати перераховані об’єкти на веб-сторінках фішингових сайтів. Методи, засновані на візуальній схожості, використовують підпис, щоб розрізняти фішингові сторінки. Щоб зробити підпис потрібно вибирати спільні компоненти з усього сайту, а не з окремої сторінки веб-сайту. Таким чином, одного підпису достатньо, щоб ідентифікувати різні цільові веб-сторінки окремого веб-сайту або унікальні форми веб-сайту. Даний метод використовує для порівняння дерево об’єктної моделі документа HTML (DOM), схожість каскадної таблиці стилів (CSS), візуальне сприйняття, візуальні особливості, піксельні та гібридні підходи [20].

Машинне навчання [17] забезпечує спрощені та ефективні методи аналізу даних, останнім часом демонструючи багатообіцяючі результати у проблемах класифікації в реальному часі. Ключовою перевагою машинного навчання є можливість створювати гнучкі моделі для конкретних завдань, таких як виявлення фішингу. Оскільки фішинг є проблемою класифікації, моделі машинного навчання можна використовувати як потужний інструмент. Моделі машинного навчання

можуть швидко адаптуватися до змін, щоб визначити моделі шахрайських операцій, які допомагають розробити систему ідентифікації на основі навчання.

Висновки за розділом 2

Отже, у другому розділі було розглянуто та описано механізм атаки та сферу застосування соціальної інженерії, основні типи атак соціальної інженерії. Зокрема було зосереджено увагу саме на фішингових атаках. Було проаналізовано та описано стан справ у сфері соціальної інженерії після початку пандемії COVID-19 2020. Після проведеного аналізу можна зробити висновок про те, що пандемія збільшила кількість атак з кількох причин: локдаун, збільшення кількості онлайн-замовлень та доставок різного типу, переживання за життя і здоров’я власне та близьких. Було описано підходи до виявлення фішингових атак: підхід навчання користувачів та програмний підхід до виявлення, який у свою чергу поділяється на способів виявлення фішингу таких, як чорні та білі списки, евристичні методи, методи візуальної схожості та методи машинного навчання.

РОЗДІЛ 3
МЕТОД ВИЯВЛЕННЯ ФІШИНГУ: НАВЧАННЯ КОРИСТУВАЧІВ

3.1 Огляд відкритих ресурсів навчання користувачів

У другому розділі даної роботи наведені два підходи до виявлення фішингових атак: навчання користувачів та програмний підхід. Для цієї роботи було обрано більш детально розглядати підхід навчання користувачів.

Не всі ресурси з навчання користувачів матимуть однаковий ефект на користувача, який з ними ознайомлюється.

Можна перелічити найпопулярніші наразі онлайн-ресурси по навчанню користувачів.

Матеріал від *Microsoft "Захист від фішингу"*, він доступний кількома мовами, в тому числі - українською. Також у таблиці 3.1 наведені інші онлайн-ресурси, які користуються популярністю серед користувачів.

Це веб-сайт UC Berkeley, який містить цілий розділ Education and Awareness (Освіта та Обізнаність). Тут висвітлені різні теми, зокрема й тема фішингу. Фішинг становить окрему тематику. На сайті можна ознайомитись з прикладами фішингових кампаній у різних соціальних мережах та на електронних скриньках.

National Cyber Security Center містить гайд для організацій "Фішингові атаки: захист вашої організації", що містить також відео-реалізацію.

Norton має гарну статтю "Що таке фішинг? Як розпізнати і уникнути фішингових афер". Стаття містить інформацію про те, що таке фішинг, як він працює та гарні інфографіки на тему.

Освітня платформа Udemy також пропонує низку онлайн-курсів, що мають на меті підвищити обізнаність користувачів. Наприклад, такі курси, як "Email фішинг" та "Практична оцінка фішингу".

Таблиця 3.1

Онлайн-матеріали з фішингу

Джерело	Назва	Посилання
Microsoft	Захист від фішингу	https://support.microsoft.com/uk-ua/windows/захист-від-фішингу-0c7ea947-ba98-3bd9-7184-430e1f860a44
UC Berkeley	Fight the Fish	https://security.berkeley.edu/education-awareness/fight-phish
National Cyber Security Center	Phishing attacks: defending your organization	https://www.ncsc.gov.uk/guidance/phishing
Norton	What is phishing? How to recognize and avoid phishing scams	https://us.norton.com/internetsecurity-online-scams-what-is-phishing.html
Udemy course	Practical Phishing Assessments	https://www.udemy.com/course/practical-phishing-assessments/
Udemy course	Email Phishing	https://www.udemy.com/course/introduction-to-real-time-phising-emailsanalyze-and-tools/

Окрім ресурсів, зазначених в таблиці 3.1, варто окремо виділити наступні два, які мають певну візуалізацію, за рахунок чого є більш привабливими для користувача, порівняно просто з текстом.

Anti-Phishing Phil — навчальна інтерактивна гра, створена Університетом Карнегі-Меллона (CMU) і належить компанії Wombat, у яку можна грати за допомогою веб-браузерів [21].

PhishGuru Cartoon — PhishGuru - це навчальна система, вбудована в поштові системи, яка намагається навчати користувачів у «найбільш придатний для навчання момент», коли користувач стає жертвою фішингової атаки, натиснувши, наприклад, посилання в тестовому фішинговому електронному листі. Після того, як користувач став жертвою атаки, дана система надає йому замальовану під мультфільми антифішингову інформацію (рис. 3.1).

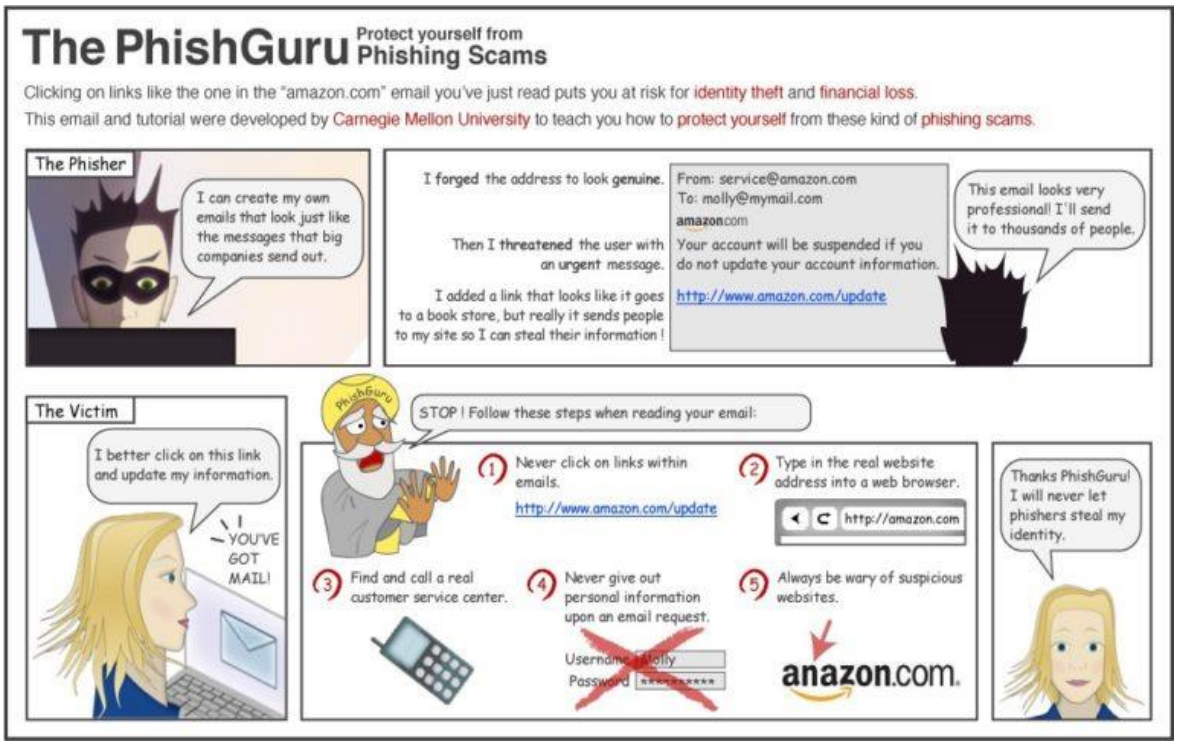

Рисунок 3.1 - Приклад відповіді системи PhishGuru Cartoon

Передбачається, що таким чином користувачі краще запам’ятовують потрібну інформацію та отримують конкретний досвід.

3.2 Методи навчання користувачів

Незалежно від наявних навичок чи здібностей, усі люди в організації мають пройти навчання з антифішингу. Для боротьби з фішингом існує багато методів до навчання користувачів. На рисунку 3.2 зображені деякі з основних [22].

Лекції. Це один з найстаріших методів і він досі лишається одним із найпоширеніших, незважаючи на свої недоліки. Залучення користувачів до лекцій

обмежується слуханням, конспектуванням, синтезом та упорядкуванням знань. Даний метод не вимагає будь-якого обладнання, окрім як наявність лектора та охоплення великої кількості матеріалу на одну лекцію. Матеріал також має бути логічним та структурованим для усного сприйняття, що полегшує навчання персоналу без додаткових друкованих або онлайн матеріалів.

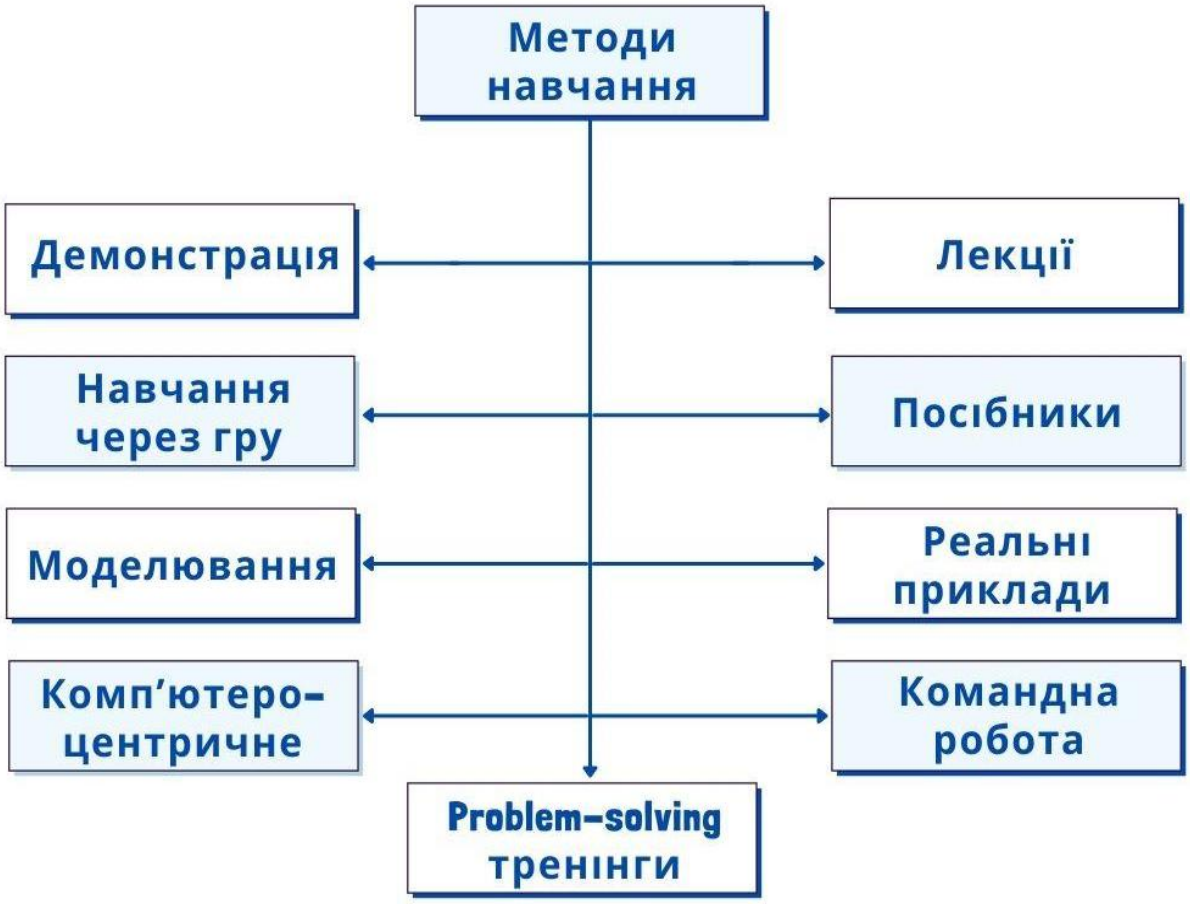

Рисунок 3.2 - Методи навчання користувачів

Попри те, що цей метод досі користується популярністю для навчання користувачів, він має недоліки, зокрема наступні:

- для лекцій потрібні ефектні доповідачі;
- потрібен інтерактив і гарна взаємодія лектора з аудиторією, інакше користувачі, як правило, швидко втрачають концентрацію та інтерес;
- від співробітників очікується, що вони навчатимуться в однаковому темпі та з однаковим розумінням, а це не так;

- виявленню фішингових атак у реальному часі не можна навчити лише на лекціях, для успіху потрібно залучати інші ресурси.

Навчальні посібники, гайди та мануали. У навчанні користувачів навчальний посібник є необхідним для поглиблення знань з теми. За допомогою посібників вони можуть дізнатися, як можна практикувати вдома або у вільний час. Існує багато різновидів навчальних посібників, наприклад:

- робочі зошити зазвичай використовуються на навчальних курсах, де конспектуються основні поняття, схеми та приклади фішингу;
- інструкції для самостійної роботи, які учні можуть виконувати у вільний час;
- довідкові посібники часто використовуються, щоб дізнатися більше про процеси та процедури;
- роздатковий матеріал містить загальну інформацію, яка доповнює матеріал, який викладає тренер на сесії.

Водночас одним із недоліків посібників є те, що користувачі можуть не зрозуміти деякі важливі поняття, просто читаючи матеріал.

Навчання на реальних прикладах. Це ретельне дослідження конкретного випадку або ситуації в реальному часі. Такий метод має можливість зробити процес навчання набагато більш реалістичним. Метою вивчення конкретного випадку є краще зрозуміти проблему. Таким чином, тренери надають детальні описи ситуації, дають можливі пояснення та оцінюють вирішення проблеми. Цей метод може використовувати різноманітні прийоми для збору інформації, включаючи інтерв'ю, спостереження, експерименти, опитувальники тощо. У контексті фішингу проводиться велика кількість тематичних досліджень, щоб оцінити труднощі та можливі рішення.

Групове навчання. Користувачі можуть поглибити свої знання під час командної роботи. Спільне навчання може допомогти слухачам покращити свою продуктивність. Очікується, що команди отримають нові навички та інформацію, а також допоможуть іншим членам опанувати нові навички та інформацію. Наприклад, різні антифішингові команди в кіберпросторі співпрацюють, щоб знайти

відповідні рішення для боротьби з фішингом. Недоліком цього методу навчання є те, що всі залежать один від одного.

Тренінг із вирішення проблем – це тип навчання, під час якого людина вчиться знаходити найкраще ефективне рішення проблеми, наприклад, фішингу. Навчання з вирішення проблем полягає в тому, щоб користувачі проходили три кроки. Визначення різних типів фішингових атак є першим кроком до їх подолання. Для цього користувачі повинні зібрати інформацію про фішингові атаки. Наступним кроком є висування слухачами ідеї щодо боротьби з фішинг-атакою. Після цього слухачі мають проголосувати або оцінити рішення для зменшення можливості фішингової атаки. На останньому етапі від слухачів вимагається втілити рішення, яке було обрано на попередньому етапі.

Демонстрація. Демонстрації, як правило, включають покрокове навчання. Наприклад, дуже важливо, щоб учні збирали фішингові дані в реальному часі та практикували те, чому їх навчили тренери. Багато експертів проводять живі демонстрації того, як зловмисник створює та здійснює фішингову атаку. Демонстрація може бути невдалою, якщо тренери не планують її належним чином. Це вимагає великої підготовки.

Навчання через гру. Існує кілька способів практикувати фішинг, але один з найпоширеніших – це гра. Навчання через гру є більш приємним, покращує засвоєння інформації та стимулює запам’ятати більше і краще. Таким чином, фішингові атаки краще розуміються через гру. Наприклад, гравці повинні ідентифікувати фішингові веб-сайти, надані тренером, щоб отримати очки.

Навчання на основі моделювання є високоефективним і економічно вигідним методом навчання слухачів у реальному часі в контрольованому середовищі. Це дає тренерам найкращий шанс побачити, наскільки добре слухачі реалізують свої таланти на практиці та приймають рішення щодо виявлення фішингу в імітованих реальних обставинах. Слухачі натомість отримують чудовий практичний досвід. Недоліком цієї стратегії є те, що зловмисники модифікують набору інструментів, що робить користувачів вразливими до атак.

Комп'ютерне навчання – це такий метод навчання, який покладається на використання цифрових технологій, таких як ноутбуки та планшети, щоб замінити традиційне навчання в класі. Зазвичай це робиться онлайн за допомогою системи управління навчанням (LMS) і може бути виконано з будь-якої точки світу. У комп'ютерному навчанні використовується багато основних методів, і одним з них є онлайн-вікторина. Вміння користуватися комп'ютером є ключовим моментом цього навчання.

3.3 Опис запропонованого методу

Аналізуючи інформацію, викладену в попередньому підрозділі, робимо висновки про те, що кожен з описаних методів має певні недоліки. Таким чином, автором пропонується поєднати два з вже існуючих методів з метою підвищення ефективності навчання користувачів. Пропонується поєднати наступні методи: навчання на реальних прикладах, та тренінг із вирішення проблем. В результаті матимемо тренінг із вирішення проблем, що базується на реальних прикладах.

Суть даного тренінгу заключається в тому, аби пройти вікторину, що базується на реальних прикладах, які можуть зустрітися пересічному українцю. Суть розробленого тренінгу заключається в тому, аби пройти опитування, що базується на реальних прикладах, які можуть зустрітися пересічному українцю. Приклади змодельовані відповідно до реальних випадків. Приклади засновані на оголошенні з продажу мобільного телефону на онлайн-платформі оголошень OLX.

Змодельоване оголошення можна побачити на рисунку 3.3. Звичайне оголошення, нічого особливого.

В оголошенні пропонується на продаж телефон компанії Apple iPhone 11 128GB. В моделюванні оголошення було обрано було саме цей телефон, оскільки зловмисники користуються певними вразливостями системи iOS, що безпосередньо розглядається в запропонованому рішенні.

Не зважаючи на те, що вже навіть сама платформа випустила гайд [23] про те, як не віддати свої кошти зловмиснику, люди досі стають жертвами кіберзловмисників, а отже, приклад є актуальним.

Рисунок 3.3 - Оголошення з продажу телефону

Схема тренінгу. Знайомство і загальні питання. Приклад 1. Висновки з прикладу 1. Приклад 2. Висновки з прикладу 2.

Знайомство включає наступні питання.

1. Стать
2. Вік
3. Чи знаєте ви що таке фішинг?
4. Чи стикалися ви з фішингом?
5. Чи були ви ціллю зловмисника?
6. Чи здатні ви відрізнити фішингове повідомлення?
7. Чи вивчали ви раніше тему фішингу?

Вхідні дані для прикладу 1 і 2. Ви - продавець на онлайн-платформі оголошень OLX. Ви виставили на продаж певний дороговартісний товар, наприклад, мобільний телефон вартістю 10 000 грн. Вам дуже хочеться продати свій товар і отримати кошти.

Приклад 1. Слухачеві пропонується ознайомитися з повідомленнями (рис. 3.4).

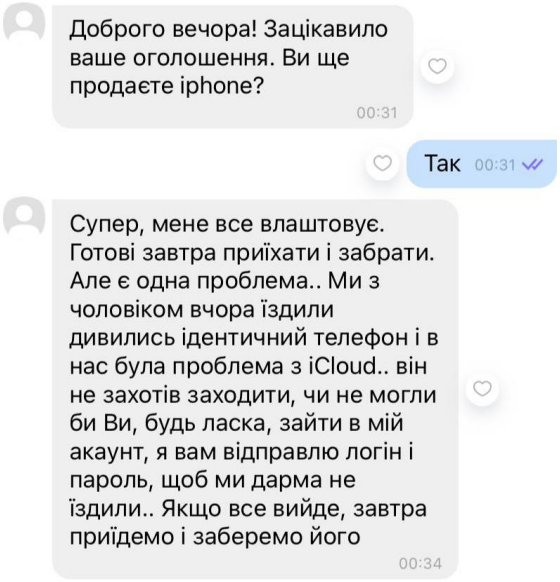

Рисунок 3.4 - Змодельовані повідомлення з прикладу 1

Далі слухач має зробити висновки і відповісти на питання.

1. Допоможете людині чи ні? І чому?
2. Як ви думаєте, яке буде продовження в цієї історії, якщо ви відповіли так і якщо ні?

Після цього наступним кроком слухачеві пояснюється даний приклад, суть та схема атаки та наводяться висновки.

Висновки з прикладу 1. Отже, приклад 1 - це типова схема вимагання грошей. По-перше, зловмисники використовують сторонній майданчик. Продавцеві з покупцем цілком можна обійтися платформою OLX для уточнюючих запитань. По-друге, зловмисники втираються до вас в довіру "щоб ми дарма не їздили.. " - таким чином намагаючись нав’язати вам відчуття провини, тобто чинять тиск на те, аби ви погодились. За успішного сценарію даної атаки - ви вводите в свій iPhone авторизаційні дані зовсім незнайомої вам особи. Відписуєте в месенджері "все ок,

все вийшло". Далі ви, органічно, хочете вийти з акаунту цієї особи, але не можете. Оскільки пароль невірний. Компанія Apple вимагає підтвердження виходу з iCloud за допомогою пароля. Таким чином зловмисник має контроль над вашим телефоном. Зазвичай за новий пароль зловмисники просять викуп в розмірі 50% вартості телефону. Звісно, ви можете писати скарги в Apple, доводити їм, що телефон і справді ваш, а це велика прикрість, але цей шлях обере меншість. Більшість просто заплатить гроші, аби їм розблокували їхній же пристрій. Будьте обізнані та не ловіться!

Якщо ви знаєте про такого типу атаки, ви молодець! Якщо ви засумнівалися і почали шукати в інтернеті інформацію щодо такого типу атак, ви молодець! Що ви можете зробити, аби таких ситуацій траплялося менше? Поділитися із знайомими. Таким чином більше людей будуть готові та не повірять шахраю.

Що робити, якщо вас таким чином таки вдалося спіймати на гачок і ви відправили гроші? Написати заяву в кіберполіцію, оскільки вимагач надсилатиме вам номер картки, також ви матимете його номер телефону.

Приклад 2. Слухачеві пропонується ознайомитися з наступними повідомленнями (рис. 3.5).

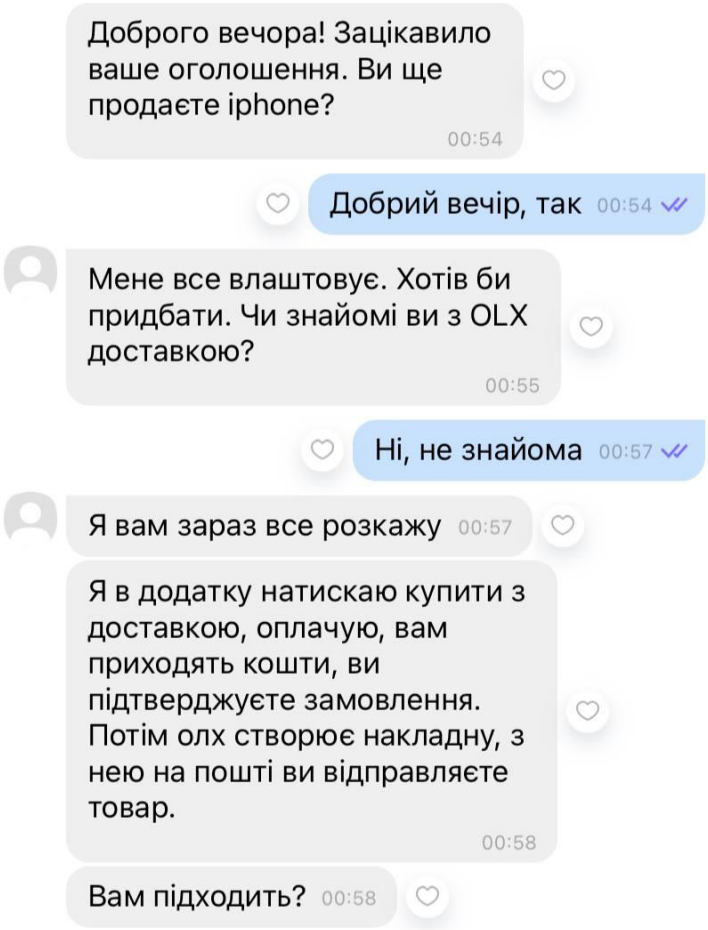

Рисунок 3.5 - Змодельовані повідомлення для прикладу 2

Далі слухач має зробити висновки і відповісти на питання.

1. Погоджуєтесь? Чому так або ні?
2. Як ви думаєте, яке буде продовження в цієї історії, якщо ви відповіли так і ні?

У випадку, якщо користувач погоджується, змодельований подальший розвиток подій. Пропонується наступний діалог до ознайомлення (рис. 3.6), та запитання, спрямовані на те, чи здатний слухач визначити фішингове посилання.

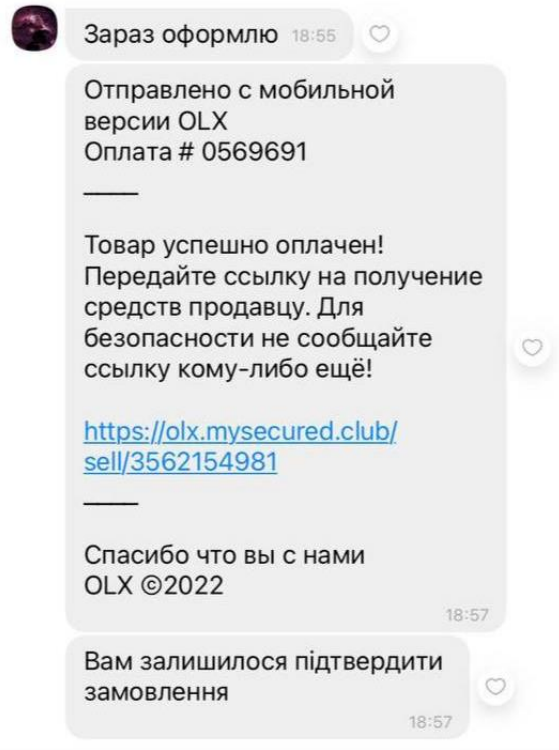

Рисунок 3.6 - Змодельовані повідомлення для прикладу 2

Сучасні веб-браузери вже здатні вирізняти фішингові посилання (рис. 3.7), та можуть показувати попередження, коли користувач хоче перейти за зазначеним посиланням.

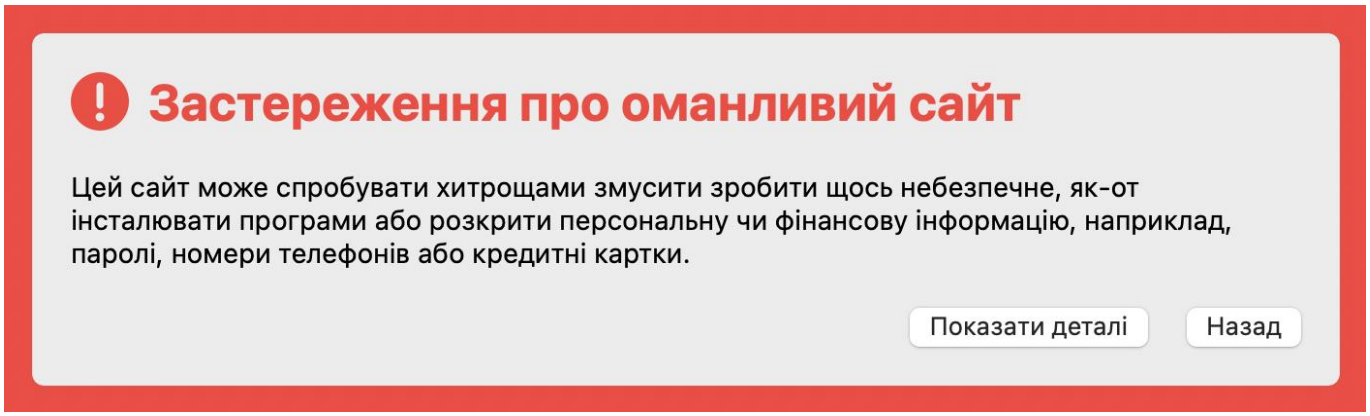

Рисунок 3.7 - Попередження про перехід на фішингову сторінку

Однак це відбувається не завжди. У випадку, якщо посилання відкривається, користувач побачить форму оплати (рис. 3.8), яка візуально майже ідентична до легітимного сайту.

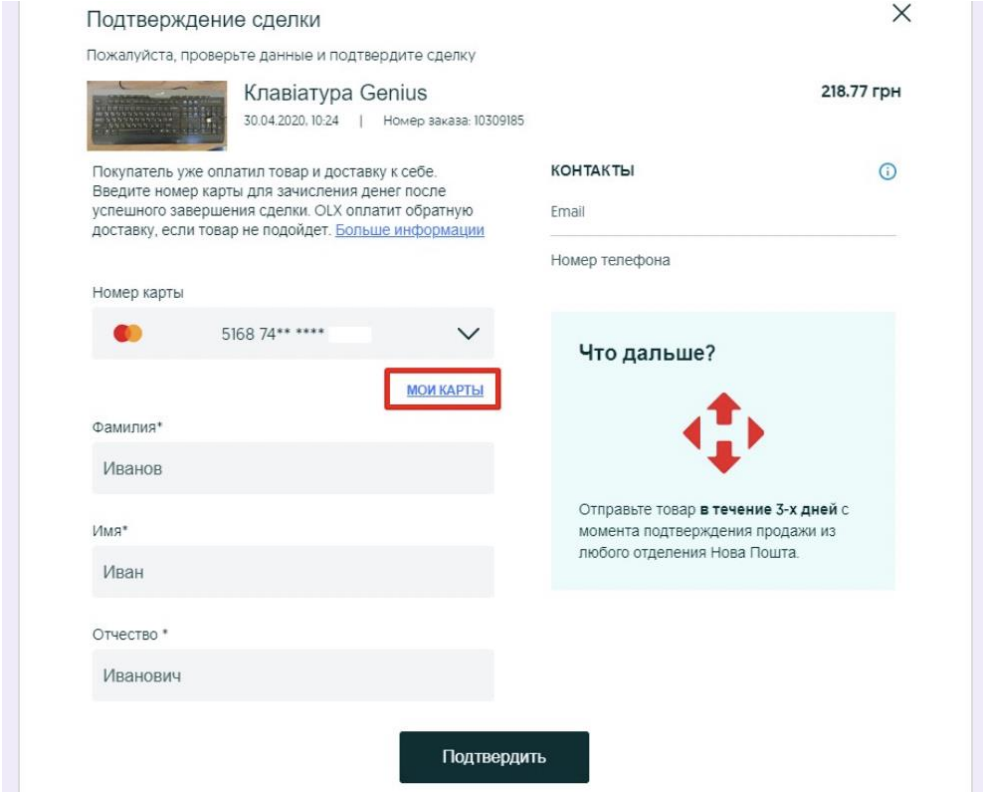

Рисунок 3.8 - Фішингова форма оплати

Після цього наступним кроком слухачеві пояснюється даний приклад, суть та схема атаки та наводяться висновки.

Висновки з прикладу 2. Не переходьте за посиланнями, які вам відправляють в особистих повідомленнях. Запам’ятайте це правило. Пам’ятайте, що в роботі послуги OLX Доставка відсутні будь-які індивідуальні форми і посилання для здійснення угоди / отримання коштів по угоді. Всю актуальну інформацію щодо купівлі-продажу ви можете побачити лише у своєму профілі в додатку або на веб-сайті.

Якщо ви відмовилися від такої OLX-доставки ще на початку, ви молодець! Поділіться з друзями. Найперше такі зловмисники пишуть також на сторонній ресурс - найчастіше Viber. Також варто звернути увагу на те, що фішингові повідомлення часто пишуться іншою мовою. Тобто ви спілкуєтесь українською, домовляєтесь українською, повідомлення з посиланням приходить російською. Це відбувається, наприклад, тому що серівс для генерації фішингових посилань працює тільки російською. Наступним "дзвіночком" є те, що у зловмисника майже завжди

немає уточнюючих питань, вони не намагаються збити ціну. Також зловмисники часто кваплять жертв, щоб у тої не було часу аналізувати те, що відбувається, тому зазвичай їхні легенди містять щось дуже термінове. Гарною вудочкою тут також є те, як саме шахраї пояснюють принцип роботи сервісу OLX-доставка. Воно майже відповідає дійсності, окрім моменту про те, що продавець отримує кошти до відправки. Згідно з даним сервісом, продавець отримує кошти лиш після того, як покупець забрав свою посилку з пошти і йому все підійшло. До того моменту, кошти вже списано з покупця, але вони знаходяться на рахунках OLX, і у випадку, коли покупцеві щось не підходить, він може відправити товар назад продавцеві і отримати свої кошти назад, відповідно, теж тільки після отримання продавцем товару, що не підійшов.

Висновки за розділом 3

У даному розділі були зібрані та проаналізовані існуючі методи виявлення фішингу щодо навчання користувачів. Кожен з них має свої переваги та недоліки. Було запропоноване рішення з удосконалення методу та розроблений опитувальник згідно даного методу.

ВИСНОВКИ

Персональні дані – це те, що є в кожної особи. На жаль, не всі люди вміють правильно користуватися своїми персональними даними, не уважно читають згоди на обробку персональних даних та в цілому є неуважними щодо інформації про себе, яку вони залишають по собі. Усім цим користуються зловмисники, вдало користуються зі своєю метою – зазвичай отримати прибуток різними шляхами. Вимагання грошей, шантаж за повернення певних даних, викрадення даних кредитних карток з метою збагачення шляхом крадіжки коштів з картки, витік інформації для погіршення репутації організації тощо. Висновок один: персональні дані потребують захисту.

Компанії інвестують великі суми грошей і ресурсів для створення ефективних стратегій проти атак соціальної інженерії [24, 25]. Однак існуючі методи виявлення мають обмеження, а контрзаходи неефективні для боротьби з постійно зростаючою кількістю атак соціальної інженерії.

У роботі проаналізовано методи протидії фішинговим атакам – це методи навчання користувачів та програмні методи. Усі методи мають певні недоліки, якими вдало користуються зловмисники.

Методи навчання користувачів обмежені суб’єктивними рішеннями людей. Технологічні методи є обмеженими, оскільки можуть бути використані технологічні вразливості. Ці атаки розвиваються день за днем, а зловмисники вдосконалюються.

Таким чином, існує велика потреба в більш ефективних методах виявлення та протидії для виявлення та мінімізації впливу цих атак.

У даній кваліфікаційній роботі було удосконалено метод захисту персональних даних від атак соціальної інженерії шляхом поєднання двох існуючих методів.

Відповідно до поставлених задач в роботі виконано:

- збір та аналіз літератури з питання персональних даних;
- збір та аналіз літератури типових атак соціальної інженерії;

- проаналізовано та описано механізм типової атаки;
- збір та аналіз існуючих методів виявлення фішингу;
- удосконалено метод виявлення фішингу;
- розроблено рішення згідно з удосконаленим методом.

У подальшому запропонований метод може використовуватися організаціями та експертами з соціальної інженерії для створення нових тренінгів з метою навчання користувачів відповідно до поставлених перед ними задач.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України "Про інформацію" [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2657-12#Text.
2. Цивільний кодекс України. Стаття 505 [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/go/435-15.
3. КАБІНЕТ МІНІСТРІВ УКРАЇНИ П О С Т А Н О В А від 9 серпня 1993 р. N 611 Про перелік відомостей, що не становлять комерційної таємниці [Електронний ресурс]. – 1993. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/611-93-п#Text .
4. Закон України "Про захист персональних даних" [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2297-17#Text.
5. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1374-1-1.
6. Конституція України. Стаття 32 [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.
7. Nyirak A. The Attack Cycle [Електронний ресурс] / Amade Nyirak – Режим доступу до ресурсу: https://www.social-engineer.org/framework/attack-vectors/attack-cycle/.
8. Інформаційна та Кібербезпека: Соціотехнічний Аспект / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа. – Київ: ДУТ, 2015.
9. Social Engineering [Електронний ресурс] – Режим доступу до ресурсу: https://www.imperva.com/learn/application-security/social-engineering-attack/.
10. Pretexting [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Pretexting.

11. Shramko S. Criminal-legal and criminological threats in the Internet space during the pandemic / S. Shramko, A. Kalinin. // Bulletin of the Association of Criminal Law of Ukraine. – 2021. – pp. 226–240.
12. Developing Story: COVID-19 Used in Malicious Campaigns // Trend Micro. – 2020. – URL: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains.
13. Global Scamdemic: Scams Become Number One Online Crime // Group-IB. – 2021. – URL: https://en.prnasia.com/releases/apac/global-scamdemic-scams-become-number-one-online-crime-321938.shtml.
14. Phishing attacks from the fake Ministry of Health on the topic of vaccination were recorded in Ukraine // Ukrainian Pravda. – 2021. – URL: https://www.pravda.com.ua/news/2021/02/12/7283229/.
15. The threat of cyberattacks is growing due to the pandemic: EU report // Juridical Newspaper. – 2020. – URL: https://yur-gazeta.com/golovna/zagroza-kiberatak-zrostae-cherez-pandemiyu-zvit-es.html.
16. Khonji M. Phishing Detection: A Literature Survey [Електронний ресурс] / M. Khonji, Y. Iraqi, A. Jones. – 2015. – Режим доступу до ресурсу: https://www.researchgate.net/publication/256841808_Phishing_Detection_A_Literature_Survey.
17. Abu-Nimeh S. A Comparison of Machine Learning Techniques for Phishing Detection [Електронний ресурс] / S. Abu-Nimeh, D. Nappa, X. Wang, S. Nair. – 2017. – Режим доступу до ресурсу: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.114.1242&rep=rep1&type=pdf .
18. Alanezi M. Phishing Detection Methods: A Review [Електронний ресурс] / Mafaz Alanezi. – 2021. – Режим доступу до ресурсу: https://www.researchgate.net/publication/355896081_Phishing_Detection_Methods_A_Review.

19. Bhattacharyya S. Detecting Phishing Websites, a Heuristic Approach [Електронний ресурс] / S. Bhattacharyya, C. Pal, P. Pandey. – 2017. – Режим доступу до ресурсу: http://www.ijlera.com/papers/v2-i3/20.201703073.pdf.
20. Jain A. Phishing Detection: Analysis of Visual Similarity Based Approaches [Електронний ресурс] / A. Jain, B. B. Gupta. – 2017. – Режим доступу до ресурсу: https://www.researchgate.net/publication/312205924_Phishing_Detection_Analysis_of_Visual_Similarity_Based_Approaches.
21. Anti-Phishing Phil [Електронний ресурс] – Режим доступу до ресурсу: https://www.cmu.edu/iso/aware/phil/index.html.
22. Sonowal G. Phishing and Communication Channels. A Guide to Identifying and Mitigating Phishing Attacks [Електронний ресурс] / Gunikhan Sonowal. – 2022. – Режим доступу до ресурсу: https://www.researchgate.net/publication/356908322_Training_Methods_for_Phishing_Detection.
23. Фішинг в OLX Доставка [Електронний ресурс] – Режим доступу до ресурсу: https://help.olx.ua/hc/uk/articles/360014371320-Фішинг-в-OLX-Доставка.
24. Cullen A. The social engineering attack spiral. [Електронний ресурс] / A. Cullen, L. Armitage. – 2020. – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/7502347.
25. Conteh N.Y. Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks. [Електронний ресурс] / N.Y. Conteh, P.J. Schmick. – 2016. – Режим доступу до ресурсу: https://www.accentsjournals.org/PaperDirectory/Journal/IJACR/2016/3/1.pdf.
26. Mohsin M. S. Phishing Detection and Prevention [Електронний ресурс] / M. S. Mohsin, Z. Sarwar, M. Saad. – 2020. – Режим доступу до ресурсу: https://www.researchgate.net/publication/358210427_Phishing_Detection_and_Prevention.
27. Захист від фішингу [Електронний ресурс] // Microsoft – Режим доступу до ресурсу: https://support.microsoft.com/uk-ua/windows/захист-від-фішингу-0c7ea947-ba98-3bd9-7184-430e1f860a44.

28. Fight the Phish [Електронний ресурс] // UC Berkeley – Режим доступу до ресурсу: https://security.berkeley.edu/education-awareness/fight-phish.
29. Phishing attacks: defending your organisation [Електронний ресурс] // National Cyber Security Centre – Режим доступу до ресурсу: https://www.ncsc.gov.uk/guidance/phishing.
30. What is phishing? How to recognize and avoid phishing scams [Електронний ресурс] // Norton – Режим доступу до ресурсу: https://us.norton.com/internetsecurity-online-scams-what-is-phishing.html.
31. Nohlberg M. The Cycle of Deception - A Model of Social Engineering Attacks, Defences and Victims [Електронний ресурс] / M. Nohlberg, S. Kowalski. – 2008. – Режим доступу до ресурсу: https://www.semanticscholar.org/paper/The-cycle-of-deception-a-model-of-social-attacks%2C-Nohlberg-Kowalski/78bebe2dd349781b55819e677a917aa480b3b05e.
32. Salahdine F. Social Engineering Attacks: A Survey [Електронний ресурс] / F. Salahdine, N. Kaabouch. – 2019. – Режим доступу до ресурсу: https://www.researchgate.net/publication/332151597_Social_Engineering_Attacks_A_Survey.
33. Saleem J. Defense Methods Against Social Engineering Attacks [Електронний ресурс] / J. Saleem, M. Hammoudeh. – 2018. – Режим доступу до ресурсу: https://www.researchgate.net/publication/319097404_Defense_Methods_Against_Social_Engineering_Attacks.
34. Закон України "Про основні засади забезпечення кібербезпеки України" [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
35. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №96/2016 Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://www.president.gov.ua/documents/962016-19836.
36. Акерлоф Д. Фішинг: Хто і як маніпулює вашим вибором / Д. Акерлоф, Р. Шиллер. – Київ: Наш Формат, 2017. – 272 с.

37. Mishra S. SMS Phishing and Mitigation Approaches [Електронний ресурс] / S. Mishra, D. Soni – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/8844920.
38. How to Keep Your Personal Information Secure [Електронний ресурс]. – 2012. – Режим доступу до ресурсу: https://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure.
39. The risk of social engineering on information security: a survey of it professionals [Електронний ресурс].— Режим доступу: https://www.academia.edu/22527821/The_Risk_of_Social_Engineering_on_Information_Security_09.
40. Social Engineering Defined [Електронний ресурс] – Режим доступу до ресурсу: https://www.social-engineer.org/framework/general-discussion/social-engineering-defined/.
41. What To Know About Identity Theft [Електронний ресурс] – Режим доступу до ресурсу: https://consumer.ftc.gov/articles/what-know-about-identity-theft.
42. What is Social Engineering? Examples & Prevention Tips [Електронний ресурс] – Режим доступу до ресурсу: https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering.
43. Manoj P. Detection and classification of phishing websites [Електронний ресурс] / P. Manoj, Y. Bhuvan Kumar, D. Rakshitha, G. Megha – 2021. – Режим доступу до ресурсу: https://www.peertechzpublications.com/articles/TCSIT-6-140.php.
44. Dong X. User behaviour based phishing websites detection [Електронний ресурс] / X. Dong, J. A. Clark, J. L. Jacob. – 2008. – Режим доступу до ресурсу: https://www.researchgate.net/publication/224370621_User_behaviour_based_phishing_websites_detection.
45. Xiangyu L. Social engineering and Insider threats. [Електронний ресурс] / L. Xiangyu, L. Qiuyang, S. Chandel. – 2017. – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/8250331.

ДОДАТОК А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Тези наукових доповідей:

1. Natalia Lukova-Chuiko, Alina Prokopenko. Impact of the COVID-19 on social engineering in Ukraine. 8th International Conference Information Technology and Implementation” (IT&I-2021). Kyiv.
2. Володимир Наконечний, Аліна Прокопенко. Соціальна інженерія. Методи протидії. ІІ Міжнародна науково-практична конференція "Проблеми кібербезпеки інформаційно-телекомунікаційних систем" (PCSITS 2019). Київ – 95с.

ДОДАТОК Б

Посилання на розроблений опитувальник.

https://docs.google.com/forms/d/e/1FAIpQLSfeYiuXPiKSnj5_h8sqmSRwCQ8t4teS3f_hJtbYoBFTjN2VUg/viewform