Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідувач кафедри кібербезпеки
та захисту інформації
_____ Н.В. Лукова-Чуйко
«__» червня 2021р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

дипломної роботи

бакалавра
(назва освітнього рівня)

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

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітня програма Кібербезпека
(назва освітньої програми)

на тему: «Заходи та засоби для захисту від соціальної інженерії, зокрема фішингу»

Виконавець: студент IV курсу, групи КБ-42

_____ **Шутенко Дмитро Валентинович**
(підпис) (прізвище ім'я по-батькові)

	Прізвище, ініціали	**Підпис**
Керівник	Фесенко А.О.	

Нормоконтроль	Зюбіна Р.В.	

Київ 2021

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
«10» жовтня 2020 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студенту **КБ-42** (група) **Шутенку Дмитру Валентиновичу** (прізвище ім'я по-батькові)

Тема дипломної роботи Заходи та засоби для захисту від соціальної інженерії, зокрема фішингу

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №2 від 08.10.2020 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Методи соціальної інженерії, фішинг у електронних листах.

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Проаналізувати методи соціальної інженерії, зокрема фішинг, та способи протидії ним, проаналізувати методи виявлення фішингових елементів у електронних листах, розробити технічну реалізацію системи виявлення фішинг-листів.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність полягає у створенні системи виявлення фішингу в електронних листах у веб-середовищі.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання:12 жовтня 2020 року

Завдання видав _____ (підпис) А.О. Фесенко (ініціали, прізвище)

Завдання прийняв до виконання _____ (підпис) Д.В. Шутенко (ініціали, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	25.01.2021 – 29.01.2021	*виконано*
2	Аналіз літератури	29.01.2021 – 11.02.2021	*виконано*
3	Написання загального плану роботи	12.02.2021 – 15.02.2021	*виконано*
4	Дослідження методів соціальної інженерії та наявних методів захисту від атак що на нех покладаються	16.02.2021 – 04.03.2021	*виконано*
5	Розробка переліку рекомендацій для захисту від соціальної інженерії	05.03.2021 – 21.03.2021	*виконано*
6	Постановка задачі створення технічного рішення для виявлення ознак фішингу в електронних листах	22.03.2021 – 08.04.2021	*виконано*
7	Підбір середовища реалізації, побудова, опис, оцінка якості та дослідна експлуатація алгоритму	09.04.2021 – 10.05.2021	*виконано*
8	Оформлення пояснювальної записки	11.05.2021 – 08.06.2021	*виконано*
9	Підготовка до захисту дипломної роботи	09.06.2021 – 21.06.2021	*виконано*

Завдання видав _____ (підпис) А.О. Фесенко (ініціали, прізвище)

Завдання прийняв до виконання _____ (підпис) Д.В. Шутенко (ініціали, прізвище)

Термін подання дипломної роботи до ЕК 08 червня 2021 року

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків, має 62 сторінок основного тексту та 2 таблиці. Список використаних джерел містить 35 найменувань і займає 4 сторінки.

Метою даної роботи є розробка переліку рекомендацій для захисту від негативного інформаційно-психологічного впливу зловмисників на свідомість працівників та технічного рішення виявлення фішингових електронних листів шляхом аналізу, синтезу та агрегації наявних рекомендацій та технічних рішень із обґрунтуванням необхідності їх використання.

У роботі проаналізована існуюча література та теоритичні засади протидії соціальній інженерії, проведено узагальнення вітчизняної і зарубіжної практики з теми розробки технічних та організаційних методів захисту від атак з використанням соціальної інженерії.

Розроблені рекомендації що узагальнюють найкращі практики сучасних підходів до захисту від маніпулятивного інформаційно-психологічного впливу шахраїв на свідомість працівників.

Розроблена система виявлення фішингу в електронних листах в веб-середовищі, як одного із технічних підходів до протидії зловмисникам, що покладаються на соціальну інженерію.

Ключові слова: людський фактор, маніпулятивний вплив, соціальна інженерія, виявлення фішингових листів, безкоштовні поштові скриньки.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ПК	–	Персональний комп’ютер
API	–	Application Programming Interface
CI	–	Соціальна інженерія;
АРМ	–	Автоматизоване робоче місце
PDF	–	Portable document format
TXT	–	Text file
IT	–	Information Technology
VPN	–	Virtual Private Network
ПЗ	–	Програмне забезпечення
DKIM	–	DomainKeys Identified Mail
SPF	–	Sender Policy Framework
APWG	–	Anti-Phishing Working Group

ВСТУП

Сьогодення вимагає все більшої винахідливості від хакерів, що намагаються обійти старанно налаштовані інженерами з інформаційної безпеки антивірусні програми, міжмережеві екрани та інші системи захисту, покликані захистити дані з обмеженим доступом. Пошук вразливостей в корпоративних мережах значно ускладнився після введення гігантами IT-індустрії кращих практик захисту власних мереж. Широко використовувані рішення з кібербезпеки працюють досить непогано, незважаючи на велику кількість хибних спрацювань, проте хакерів менше не стає. Вони адаптуються під нові технології захисту та все частіше користуються давно всім відомими методами соціальної інженерії для неправомірного заволодіння інформаційними активами компаній, підприємств, та будь-кого, хто з якихось причин стане їх ціллю. За результатами численних досліджень мішенями соціальних інженерів в буквальному розумінні є всі люди починаючи від керівника компанії до учня навчальної школи, який має сторінку в соціальній мережі [1].

В даній роботі основна увага буде приділена саме витоку даних з обмеженим доступом, адже це є – одним з найгірших сценаріїв, який може трапитися в будь-якій компанії, на підприємствах різної форми власності та абсолютно в будь-якій державній установі кожної країни світу. Зазначу, що методи та принади, якими користуються хакери для досягнення своєї мети, бувають досить різноманітними, проте найчастіше їх об’єднує одна спільна деталь – ставка на людську помилку.

Так звані соціальні інженери вважають, що ввести незнайомих з ІБ користувачів в оману набагато легше від багатомісячного моделювання, підготовки та проведення таргетованої атаки. Одним із найважливіших факторів для кіберзлочинців є гроші, зважаючи на це ми вкотре можемо впевнитись чому вони вибирають хакінг людської свідомості, а не добре захищеного програмного забезпечення — це не тільки простіше а і дешевше. Фінансові витрати на проведення таргетованої атаки на майстерно захищений об’єкт інформаційної діяльності можуть досягати десятків тисяч доларів в той час як достатньо витончені

спроби отримання тієї самої інформації шляхом введення працівників підприємства в оману можуть вартувати декілька десятків доларів та певний час на розробку покрокового плану дій.

Ошуканий працівник в наш час визначає втрати асоційовані з активами, до яких його акаунт має доступ, вважаючи, що хакер отримав доступ лише до робочого місця, а не до всієї мережі. Головним завданням сучасного інженера з інформаційної безпеки є мінімізація ризиків, у тому числі і тих, що пов'язані із втратою даних через недбалість або необізнаність працівників компанії [2].

Проблемою розробки технічних та організаційних методів захисту від атак з використанням соціальної інженерії у своїх дослідженнях займалось чимало закордонних науковців та представників бізнесу. Визначу тих, чиї доробки особливо справили на мене враження: Hassan Chizari, Heidi Wilcox, Maumita Bhattacharya, Josh Fruhlinger, Enrico Frumento, Kevin Mitnick, Bernard Oosterloo, Dimitrios Stergiou, Katharina Krombholz, Heidelinde Hobel, Markus Huber, Edgar Weippl, Ankit Kumar Jain, B. B. Gupta, Ping Yi, Yuxiang Guan, Futai Zou, Yao Yao, Wei Wang та Ting Zhu. Вітчизняні науковці також проводили дослідження на схожу тематику, слід відмітити наступних: Мохор В.В. , Цуркан О.В., Цуркан В.В., Герасимов Р.П. , В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа.

Однак, більшість із наявних на сьогодні публікацій лише наголошують на необхідності проведення навчання для співробітників, і лише деякі намагаються розробляти технологічні методи захисту, моніторингу та раннього попередження, тощо.

Метою дипломної роботи "Заходи та засоби для захисту від соціальної інженерії, зокрема фішингу" є розробка переліку рекомендацій для захисту від негативного інформаційно-психологічного впливу зловмисників на свідомість працівників та технічного рішення виявлення фішингових електронних листів шляхом аналізу, синтезу та агрегації наявних рекомендацій та технічних рішень із обґрунтуванням необхідності їх використання.

Для досягнення даної мети необхідно вирішити наступні задачі:

1. провести аналіз та класифікацію методів соціальної інженерії;

2. визначити найбільш часто вживаний метод соціальної інженерії;

3. провести аналітичний огляд наявних методів захисту від атак, що базуються на методах соціальної інженерії;

4. розробити вичерпний перелік рекомендацій щодо захисту від атак, що покладаються на методи соціальної інженерії;

5. обґрунтувати необхідність створення системи детектування фішингових листів;

6. формалізувати задачу створення технічного рішення для виявлення ознак фішингу в електронних листах у термінах комп'ютерного моделювання;

7. обґрунтовано підібрати середовище реалізації; побудувати та описати роботу алгоритму для виявлення фішингу в електронних листах;

8. провести дослідну експлуатацію та оцінку якості системи виявлення фішингу в електронних листах.

Об'єктом дослідження є процес захисту від соціальної інженерії в цілому та виявлення фішингу в електронних листах безпосередньо.

Предметом дослідження є рекомендації щодо захисту від соціальної інженерії та система виявлення фішингу в електронних листах, створена в веб середовищі.

Для досягнення мети дипломної роботи були використані наступні *методи дослідження*:

1. у розділі 1 було проведено аналіз методів соціальної інженерії та проаналізовано відомі способи протидії ним шляхом застосування структурного аналізу, методу порівняння та системного підходу;

2. у розділі 2 було здійснено моделювання та аналіз підходів для виявлення фішингу в електронних листах; проведено порівняльну характеристику середовищ розробки, для отримання повних відомостей про алгоритмічну складову даної задачі для її формалізації та вирішення;

3. у розділі 3 для здійснення технічної реалізації системи виявлення фішингу в електронних листах та проведення її дослідної експлуатації було застосовано експериментальний метод дослідження.

Наукова новизна дипломної роботи полягає в створенні сучасного та вичерпного переліку рекомендацій щодо захисту від зловмисників, які використовують СІ та розробці технічного рішення виявлення фішингових електронних листів що вирішують дану проблему, шляхом аналізу електронного листа в веб-середовищі.

Практичне значення отриманих результатів забезпечується створенням системи виявлення фішингу в електронних листах в веб-середовищі, як одного із технічних підходів до протидії зловмисникам, що покладаються на соціальну інженерію.

Основні результати дипломної роботи доповідалися та обговорювалися на V Міжнародній студентській олімпіаді “Шляхи та механізми захисту інформаційного простору України від шкідливих інформаційно-психологічних впливів“ 2019 року, III міжнародній науково-практичній конференції “ПРОБЛЕМИ ТА ШЛЯХИ ЗАХИСТУ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОЇ І ДУХОВНОЇ БЕЗПЕКИ ОСОБИ, СУСПІЛЬСТВА, ДЕРЖАВИ” 2019 року, VII Міжнародній науково-практичній конференції “Information Technology and Interactions“ 2020 року, VI Міжнародній студентській олімпіаді “Шляхи та механізми захисту інформаційного простору України від шкідливих інформаційно-психологічних впливів“ 2020 року, VI Всеукраїнській науково-практичній конференції “ПЕРСПЕКТИВНІ НАПРЯМИ ЗАХИСТУ ІНФОРМАЦІЇ“ 2020 року, IV Міжнародній науково-практичній конференції “Проблеми кібербезпеки інформаційно-телекомунікаційних систем” (PCSITS) 2021 року та на VII Міжнародній студентській олімпіаді “Шляхи та механізми захисту інформаційного простору України від шкідливих інформаційно-психологічних впливів” 2021 року. Основні положення дипломної роботи викладені в 7 наукових працях, серед яких: 3 реферати на міжнародних студентських олімпіадах та 4 – у матеріалах наукових конференцій, 3 з яких – міжнародні.

РОЗДІЛ 1
АНАЛІЗ МІСЦЯ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ СЕРЕД УСІХ КІБЕРАТАК ТА ВІДОМІ СПОСОБИ ПРОТИДІЇ

1.1 Визначення соціальної інженерії та атак, що на неї спираються, у правовому полі України

У терміна “соціальна інженерія” існує декілька визначень, наприклад:

- Несанкціоноване отримання конфіденційної інформації або неналежних прав доступу потенційним джерелом загроз на основі побудови довірчих відносин довіри з легітимним користувачем інформаційної системи.
- Прикидаючись тим, чим ви не є, з метою обдурити когось, щоб він видав інформацію, яку зазвичай не повинні давати і до якої ви не повинні мати доступу.
- Змушувати людей робити те, що вони зазвичай не зробили б для незнайомця.
- Акт отримання чи спроби отримати захищені дані в іншому випадку шляхом обману особи для розкриття захищеної інформації.
- Практика отримання конфіденційної інформації шляхом маніпуляцій законними користувачами.
- Наука, що вивчає методи психологічної маніпуляції над людьми для того, щоб змусити їх добровільно надавати інформацію.

Соціальні інженери здатні передбачити поведінку людини, а відтак – маніпулювати її свідомістю для задоволення власних потреб [3]. У рамках соціоінженерного підходу вразливості персоналу тлумачяться як його слабкості, потреби, манії (пристрасті), захоплення. Маніпулювання ними дозволяє отримати несанкціонований доступ до інформації без руйнування та перекручування головних для нього системоутворюючих якостей. Як наслідок, це призводить до нової моделі поведінки персоналу, створення сприятливих умов реалізації загроз безпеці інформації і, як наслідок, зменшенню здатності системи захисту інформації

протидіяти їх впливові (див. рис. 1.1). Це відображається в таких формах як, наприклад, шахрайство, обман, афера, інтрига, містифікація, провокація. Використанню кожної з означених форм маніпулювання передує визначення її змісту шляхом ретельного планування, організування та контролювання [4].

Рисунок 1.1 – Використання соціоінженерного підходу [4]

З огляду на рис. 1.1, використання соціоінженерного підходу до оцінювання захищеності інформації в комп'ютерних системах передбачає цілеспрямований вплив на свідомість (підсвідомість) персоналу проти волі, але за його згодою. Такий вплив дозволяє управляти поведінкою керівництва, адміністратора, користувачів через слабкості, інтереси, потреби, схильності, переконання, звички, психічний та емоційний стан. Тому маніпулювання цими вразливостями і виражається в таких формах як шахрайство, обман, афера, інтрига, містифікація, провокація. Разом з тим, використанню кожної з означених форм маніпулювання передує визначення їх сутності шляхом ретельних планування, організації та контролювання. У рамках соціоінженерного підходу використання атак соціальної інженерії орієнтоване на отримання "несанкціонованого" доступу до інформації при оцінюванні її захищеності шляхом негативного інформаційно-психологічного впливу на свідомість або підсвідомість персоналу. Шахрай обманює людей для того, щоб отримати їх гроші. Соціальний інженер на противагу йому зазвичай вводить в оману, та запевняє жертву самовільно передати йому чутливу інформацію.[5]

Як можемо помітити на рис. 1.2 зі звіту компанії Positive Technologies за 1 квартал 2020 року, що представляє відсотки атак, що використовували різні методи для порушення властивостей інформації (цілісність, конфіденційність, доступність), приблизно ¾ усіх кібератак спиралися на методи соціальної інженерії, що неабияк демонструє, що в сучасному кіберпросторі в першу чергу треба боятися фішингових листів а вже потім вправних хакерів.

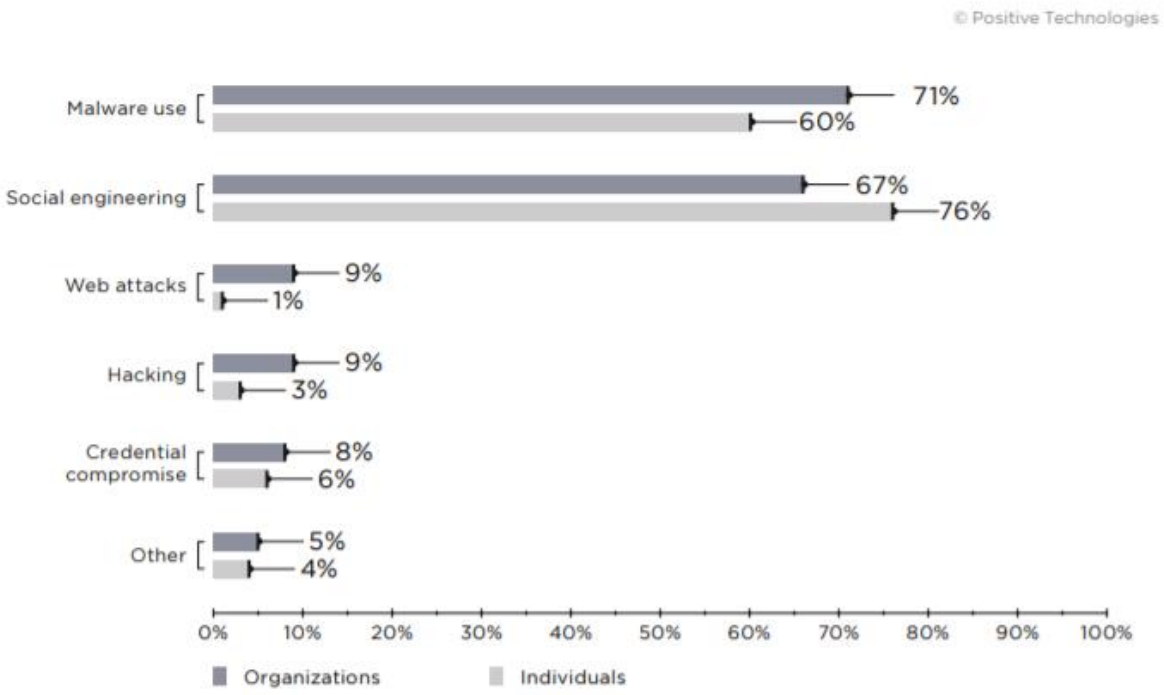

Рисунок 1.2 – Методи атак (відсоток атак, що використовували відповідний метод) [6]

Хоча соціальна інженерія є суттєвою загрозою, організації далеко не завжди звертають на неї увагу, і не визнають потенційні великі збитки, які можуть принести атаки соціальної інженерії. У цьому розділі буде проведено аналіз атак соціальної інженерії з тактиками, які використовує соціальний інженер, а потім класифікація найбільш популярних з них.

Атаку соціальної інженерії можна розглядати як цикл. Він складається з чотирьох фаз: збору інформації, розвитку відносин, експлуатації та виконання.

1. Збір інформації (дослідження) може виконуватися за допомогою різних технік і охоплює інформацію про організацію – наприклад телефонні списки, організаційні діаграми, – або про передбачувані цілі атаки – тобто особиста інформація.

2. Для розвитку відносин необхідна довіра. Людина за своєю природою заслуговує довіри, і відносини можуть бути легко побудовані за допомогою належних знань, отриманих на попередньому етапі. Відносини можуть бути використані для виконання атаки або надання зловмиснику додаткової інформації про ціль.

3. Під час експлуатації довірений зловмисник може впливати на ціль, щоб змусити розкрити інформацію або виконати якусь дію в інтересах зловмисника.

4. Фаза виконання може бути інтерпретована як виконання останнього кроку в атаці, якщо отриманий доступ або інформація не є кінцевою метою, і зловмиснику все ще потрібно виконати заключний акт, використовуючи отриману довіру та інформацію, наприклад, увійти в інформаційну систему для викрадення, зміни або видалення файлів [7].

1.2 Визначення актуальності теми дослідження

Сьогодні існує безліч рішень, що захищають апаратне та програмне забезпечення від вторгнення до інформаційної системи сторонніми особами та певною мірою внутрішніми агентами, але є лише обмежена кількість досліджень щодо людського фактору в інформаційній безпеці. Навіть якщо є найкращі технічні рішення для захисту інформації, все ж деякий персонал повинен мати доступ до системи і тим самим може скомпрометувати інформаційну безпеку на підприємстві; навмисно, не навмисно або шляхом маніпуляцій. Даний вид атак називають соціальною інженерією. Пом’якшення загроз, які несе ця маніпуляція, також зменшить навмисну та ненавмисну компрометацію систем та інформації. А отже, знизить загальний ризик.

Так само як мозок порушника виявляються безсилим перед спокусою скоєння злочину, мозок хакера прагне знайти більш витончений шлях досягнення власної мети оминаючи потужні технологічні засоби захисту. В більшості випадків це досягаються, коли таргетом зловнисника перестає бути система, а стає людина, що її використовує [5]. Історія знає численні приклади того, як навіть найдорожчі, найскладніші та найдосконаліші системи захисту інформації опиняються безсилими перед зловмисниками, що часом використовують низько технологічні рішення задля неправомірного заволодіння інформаційними активами підприємств. Загальною схемою у всіх подібних атаках було те, що на певному етапі атаки була задіяна взаємодія людини, взаємодія, якою маніпулювали та керували, щоб отримати бажані результати для зловмисника.

Хоча основними контрзаходами проти атак соціальної інженерії є обізнаність користувачів та поєднання технічних засобів контролю [2], очевидно, що сторона, що захищається, не в змозі захистити організацію від атак соціальної інженерії. Одна з ключових причин полягає в тому, що незалежно від того, скільки навчальних програм чи технічного контролю не розгорнуто, цього завжди буде недостатньо і люди залишаються найслабшим ланкою безпеки будь-якого підприємства. За словами всесвітньо відомого хакера Кевіна Митника:

“Найбільша загроза безпеці компанії – це не комп’ютерний вірус, не виправлена дірка в ключовій програмі або погано встановлений брандмауер. Насправді найбільшою загрозою можете бути ви. Я особисто переконався, що легше маніпулювати людьми, а не технологіями. Здебільшого організації не зважають на людський фактор".

Як вже було зазначено, людський фактор є найслабшою ланкою в ланцюжку інформаційної безпеки, і той, над яким потрібно працювати, щоб покращити загальний стан інформаційної безпеки в цілому. Атаки з використанням соціальної інженерії базуються на певних психологічних принципах і прийомах. Такі психологічні терміни, як нейролінгвістичне програмування, кадрування, закріплення, навіть гіпноз, часто пов’язані з методами соціальної інженерії [8]. Беручи до уваги той факт (на основі емпіричних даних та власного досвіду автора),

що більшість середньостатистичних компаній мають більший відсоток технічно здібних людей та набагато менший (або навіть не існує) відсоток працівників, здатних зрозуміти психологію, яка стоїть за атаками соціальної інженерії наскільки легко побудувати ефективну навчальну програму для зменшення ризику?

Ця проблема існує в урядових, бізнес та навчальних закладах по всьому світу. Не зважаючи на всі зусилля професіоналів сфери безпеки, інформація, захист якої є їх роботою все ще залишається вразливою та буде ціллю для порушників з навиками соціальної інженерії допоки не буде посилена найслабша ланка безпеки – людський фактор.[5]

Зараз, більше ніж будь-коли, ми маємо навчитися перестати бути самовпевненими і дізнатися більше про методи, які використовують ті, хто здійснює атаки спрямовані на порушення цілісності, конфіденційності та доступності наших комп'ютерних систем та інформаційних ресурсів.

Є багато статей, опитувань та книг, які присвячені людському фактору або суміжним темам. Але це все ще відносно невивчена галузь наукових досліджень. У більшості випадків статті та книги не мають наукового обґрунтування і не дають чіткого огляду, а лише обговорюють описи справ або дослідження. Однак ці дослідження показують, що людський фактор може завдати великої шкоди організаціям, не тільки фінансовим, але й іміджу організації, що, в свою чергу, впливає на цілі та безперервність організації в довгостроковій перспективі. Той, хто не думає як реагувати у випадку настання інциденту з безпеки заздалегідь неправий.[5]

В цілому, виникає необхідність надання послідовного загального огляду атак з використанням соціальної інженерії. Дипломна робота поєднує поточні дослідження соціальної інженерії з дослідженнями в інших областях та емпіричні дослідження, щоб зробити соціальну інженерію прозорою для організацій та допомогти їм управляти ризиками з точку зору атак, що покладаються на методи соціальної інженерії.

1.3 Класифікація та огляд методів соціальної інженерії

За останні століття мета викрадення інформації аж ніяк не змінилась, проте завдяки технічному прогресу зазнали чималих змін методи її здобуття. Як показує практика, до основних методів соціальної інженерії сьогодення слід включити :

- Претекстинг
- Фішинг
- Троянський кінь
- “Дорожнє яблуко”
- Кві про кво
- Зворотна соціальна інженерія

Кожна особа має свої слабкі сторони, які можуть бути використані при впливі на її свідомість; задача соціального інженера – запевнити жертву, що її дії є звичайною рутиною та не несуть в собі ані найменшої загрози [9]. Наприклад, працівник підприємства, що має відкриту платформу з різними рівнями доступу отримує e-mail від адресата, ім’я якого включає назву компанії, слово “support” та скопійовані з офіційних листів надписи фірмові елементи. В цьому листі звернення від керівника IT-відділу до всіх працівників відповідного підрозділу з інформаційним наповненням про запуск додаткової функції платформи у режимі тестування що включає дошку побажань, нововведення в компанії, соціальну ініціативу, тощо. Зробивши розсилку для всіх працівників підрозділу, шахрай зменшив шанси того, що в колективі працівників знайдеться скептик, що не повірить листу. Зробити сайт, схожий до офіційної платформи не видається дуже складним, а через те, що він працює у демо-режимі він не підв’язаний до усієї платформи (принаймні за даними з листа). Зайшовши на сайт, працівники бачать знайомий дизайн та оцінюють новий функціонал. Під кінець робочого дня приходить наступний лист, що пропонує пройти опитування з метою оцінки та покращення запущеного функціоналу. Працівники не вагаючись відповідають на ряд запитань та вже навіть не задумуються про власну безпеку, за що і отримують лист-подяку за участь у розробці. Згодом, працівники отримують черговий лист з повідомленням про успішну інтеграцію додаткової функції до звичного

функціоналу платформи та посилання для входу. Відкривши його, працівник бачить звичний для нього процес аутентифікації, і без зайвих вагань вводить омріяний для шахрая пароль. Сторінка починає завантажуватись та видає сповіщення, про проведення фінальних технічних робіт, що особливо не дивує працівника в зв'язку з новизною функції, хоча, це вже не так важливо адже зловмисник має доступ до його облікового запису.

Вище описаний метод соціальної інженерії називають претекстингом. Він базується на концепції довіри до суб'єкта, з яким встановлюється контакт через проведення ряду попередніх задач, які в свою чергу приводять до останнього сфабрикованого сценарію, під час якого шахрай, який вже отримав довіру особи, просить підтвердити особистість шляхом автентифікації, яка в свою чергу компрометує його дані [10].

Наступний метод соціальної інженерії – фішинг. Цей кіберзлочин полягає в тому, що шахрай пише своїм жертвам лист на електронну скриньку або СМС на мобільний телефон, видаючи себе за представника певної установи, організації чи веб-сайту та зобов'язує своїх жертв надати персональну інформацію (логіни та паролі від певних платформ, акаунтів в соціальних мережах, номера та секретні коди банківських карт, тощо), як один із етапів взаємодії з вищезгаданим суб'єктом, від якого приходить підроблене повідомлення [11]. Шляхи заманювання можуть бути різними, починаючи від пропозиції переглянути інформацію про кількість переглядів вашої сторінки в соціальній мережі (хоча не всі соцмережі надають подібного роду інформацію) до спеціальних пропозицій від інтернет магазинів чи банків, клієнтом яких є жертва [12]. Мета зловмисників – отримання будь-якої конфіденційної інформації, яку в майбутньому можна використати для просунутої атаки або банально поцупити гроші, цифрову особистість, тощо. Найбільш часто використовувані способи заманювання жертв включають:

- перевірку авторизації на сайті;
- підтвердження транзакції;
- необхідність відписки від розсилки чи спаму;
- сплата покупки з надзвичайно вигідною знижкою;

- необхідність встановлення нового програмного забезпечення;
- повідомлення про зміну умов надання послуг;
- підв’язка даних платіжних систем чи банківських карт при створенні акаунту з метою отримання певної (найчастіше фінансової) вигоди, тощо.

Слід зазначити, що характерними особливостями фішингу можна визначити схожість, проте не ідентичність імені відправника з відомим брендом, компанією, банком, тощо. Наприклад, шахраї можуть використовувати фейкову назву торгового майданчика “Alliexpress” замість реального “Aliexpress” або підкріпити фейкову адресу “www.oshadbank.ua” замість валідної “www.oschadbank.ua” [13]. Багато користувачів можуть не звернути увагу на ледве помітну помилку та запросто перейти за сфабрикованим посиланням чи сприйняти всерйоз повідомлення від штучно створеного банку чи платіжної системи які за зовнішнім виглядом можуть нагадувати офіційні ресурси. Надалі відбувається уже відомий нам сценарій – жертва довіряє ресурсу та проходить автентифікацію а шахраї отримують бажані конфіденційні дані.

Людям добре відома історія про Троянського коня. З плином часу та діджиталізацією нашого суспільства можна прослідкувати наступні зміни та перевтілення: хитромудрих греків тепер називають соціальними інженерами або шахраями, довірливих та необачних троянців – жертвами шахраїв, а концепт троянського коня перетворився на шкідливе програмне забезпечення, що інфікує комп’ютер та розповсюджується на інші девайси шляхом передачі портативними носіями чи посиланнями в інтернеті. Слід зазначити що в ідеології Троянського коня з XIII століття мало що змінилося. Тоді кінь був міфічною спорудою, що “допоміг” троянцям перемогти греків і спалив їх табори, тобто неначе став у нагоді, згодом ставши найбільшою помилкою славетного міста Трої. Зараз же Троянським конем називають програмне забезпечення, що декларується як корисне або ж нешкідливе і здатне вирішити особисті проблеми користувачів, пов’язані з кіберпростором. Після встановлення “трояна” комп’ютер перетворюється на осередок зарази. Ось тільки деякі можливості цього шкідливого програмного забезпечення:

- завада нормальній роботі користувача;
- використання обчислювальних потужностей та інших ресурсів комп'ютера для будь-якої (в тому числі незаконної) діяльності;
- шпигунство за користувачем;
- несанкціонований дистанційний доступ до файлів жертви, можливість модифікувати, видаляти та шифрування будь-які файли на жорсткому диску жертви;
- дезінформація з метою подальшого збагачення, тощо [14].

Слід також відмітити наявність різноманітних троянців створених під особливі задачі шахраїв, наприклад крадій паролів, що аналізує та пересилає шахраям всі дані для успішної автентифікації в облікових записах, до яких має доступ девайс; троянець, що може здійснювати дистанційне керування інфікованим девайсом; деструктивний троянець, який ставить перед собою мету знищення всіх даних з зараженого комп'ютера, телефона, планшета, тощо; та навіть троянець-вбивця антивірусу, який деактивує або видаляє антивірусну програму для полегшення доступу до файлів та операційної системи девайсу [15].

Достатньо високу популярність за кордоном має метод соціальної інженерії, похідний від троянського коня. Він називається "Дорожнє яблуко" та полягає в тому, що зловмисник навмисне підробляє фізичний носій, роблячи його максимально схожим на корпоративний. Потім підкидає інфікований диск, флешку або будь-який інший електронний носій, на якому зберігається вірус, у такі місця підприємства чи компанії, де працівники запросто його помітять (ліфт, вестибюль, туалет, парковка, тощо), та заберуть чи то для задоволення власної цікавості чи з метою повернути втрачений носій власнику [16]. Нерідко на такий носій може бути нанесена певна інформація, що може зацікавити пересічного працівника. Щось на кшталт "Премії 2021" чи "Зарплати 4 квартал". В будь-якому випадку рано чи пізно фізичний носій вірусу активують на корпоративному комп'ютері та відкриють широкі ворота для шахраїв в реалізації їх інформаційних потреб пов'язаних з інфікованим комп'ютером.

Наступний, не менш популярний метод соціальної інженерії – Кві про кво, що розшифровується як "послуга-за-послугу". Цей вид атаки перш за все

характеризується дзвінком зловмисника (або зв'язком корпоративною електронною поштою), який представляється працівником служби підтримки компанії, на яку працює жертва [17]. Маючи певний інсайт, вдавати з себе представника підтримки чи будь-якого іншого працівника для соціального інженера не виявляється проблемою. Він швидко переконує жертву в тому, що він покликаний допомогти у вирішенні певних технічних питань, що наче виникли на його комп'ютері, в корпоративній мережі чи на використовуваній платформі. Насправді ж ці проблеми сфабриковані зловмисником, або були попередньо завдані комп'ютеру жертви з метою безпроблемного переконання її в тому, що вона потребує технічної допомоги. Під час "вирішення технічних проблем" зловмисник рекомендує працівнику виконувати дії, що в майбутньому полегшують отримання доступу до цього комп'ютера. Нерідко такі "помічники" рекомендують встановити додаткове, замасковане під корисне програмне забезпечення, що насправді буде виконувати роль трояна чи будь-якого іншого шкідливого застосунку. Інший сценарій може включати дзвінок (чи e-mail) від представника підтримки з рекомендацією відкрити певний файл, який завідомо був некоректно зашифрований і не відкривається звичним способом. Жертва просить супорта про послугу: допомогти відкрити файл коректно і знову ж таки натикається на досить витончений метод соціальної інженерії. Крім того, під час виконання рекомендацій "колеги" жертва може надати конфіденційні дані штучно створеній для неї платформі чи діалоговому вікну, що неодмінно ретранслює введену інформацію зловмиснику (як у випадку з фішингом).

Досить популярним методом соціальної інженерії, що дуже нагадує кві про кво є Зворотна соціальна інженерія. Основна відмінність між цими методами полягає в тому, що, характеризуючи шляхи ведення зворотної соціальної інженерії, ми маємо розуміти, що жертва самостійно виходить на зв'язок із зловмисником для задоволення певних інформаційних або технічних потреб. Але, як змусити жертву самостійно ініціювати контакт з шахраями? Виділяють 2 найбільш популярні підходи:

1. Диверсія : зловмисник створює певну технічну проблему з використовуваним корпоративним ресурсом, для вирішення якої знань пересічного

працівника просто-на-просто недостатньо, тому єдиним виходом із ситуації для жертви є звернення до служби підтримки, інсайдером в якій і має бути зловмисник.

2. Реклама: якщо зловмисник певен, що працівник часом використовує комп'ютер в особистих цілях (що суперечить політиці компанії чи підприємства) можна спробувати використати небажання працівника звертатися до уповноважених працівників підтримки через можливе викриття його неправомірних дій як важіль впливу. І ось як: спочатку, зловмисник надсилає майбутній жертві листа на електронну пошту з рекламою комп'ютерного майстра. Згодом, використовуючи метод диверсії, описаної в 1 пункті, зловмисник реалізує несправність, що призводить до емуляції зараження системи вірусом. Жертва розуміє, що можливо, це саме її неправомірні дії викликали невиліковне зараження комп'ютера, і тут вона згадує про отриману декілька днів тому рекламу з пропозицією надання технічної допомоги. При цьому, один з можливих розвитків подій банально зобов'язує працівника звернутися до зловмисника "за допомогою"[18].

1.4 Визначення фішингу як набільш часто використовуваного методу соціальної інженерії

Одним із найбільш поширених та небезпечних видів атак соціальної інженерії є фішинг (англ. phishing, від fishing — риболовля) — вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів з переказу або обміну валюти, інтернет-магазинів. Шахраї намагаються змусити користувачів самостійно розкрити конфіденційні дані — наприклад, надсилаючи електронні листи із пропозиціями підтвердити реєстрацію облікового запису, що містять посилання на веб-сайт в інтернеті, зовнішній вигляд якого повністю копіює дизайн відомих ресурсів [19].

Фішинг заснований на незнанні користувачами основ мережевої безпеки. Зокрема, багато хто не знає простого факту: сервіси не розсилають листів з проханнями повідомити свої облікові дані, пароль та інше. Слід також визнати фішинг найпопулярнішим методом соціальної інженерії, адже відповідно до звіту

компанії Positive Technologies за 1 квартал 2020 року, більше половини випадків зараження комп'ютера шкідливим програмним забезпеченням відбулося саме через електронну пошту, це проілюстровано на рис. 1.3.

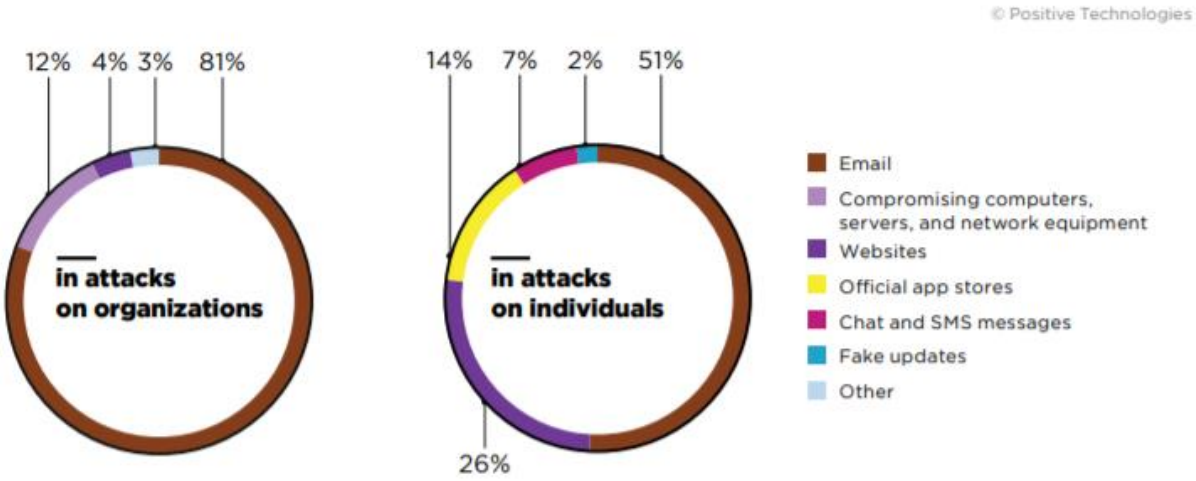

Рисунок 1.3 – Шляхи передачі шкідливого програмного забезпечення [6]

Для захисту від фішингу виробники основних інтернет-браузерів домовилися про застосування однакових способів інформування користувачів про те, що вони відкрили підозрілий сайт, який може належати шахраям. Нові версії браузерів вже володіють такою можливістю, яка відповідно іменується "антифішинг".

За даними компанії PhishMe, станом на березень 2016 року 93 % всіх фішингових листів намагались заразити комп'ютер жертви шкідливими програмами криптографічного здирництва (так зване англ. ransomware) [20] — вони шифрують дані на жорсткому диску та вимагають гроші від жертви за їхнє розшифрування. Також серед стійких тенденцій до підвищення ефективності фішингових атак було назване частіші випадки підлаштування вмісту листів під певну категорію жертв (за їхнім фахом) та із включенням певних елементів особистої інформації (зокрема, звернення до жертви за іменем). Принаймні кількість реалізованих атак є достатньою для розуміння необхідності в створенні системи детектування фішингових листів.

Починаючи з 2020 року спостерігалася досить серйозна “перекваліфікація” фішингових листів. Чимало винахідливих соціальних інженерів маскували електронні листи з шкідливим вкладенням під інформаційні брошури, документи зі зверненнями таких організацій як ООН, інформаційні листи з рекомендаціями, тощо. До прикладу, на рис. 1.4 зображений приклад PDF документу з вкладення до фішингового листа, що був замаскований під інформаційну кампанію ООН щодо національних свят та актуальної інформації щодо розповсюдження коронавірусної інфекції, розроблений групою хакерів іменованих “Higaisa”.

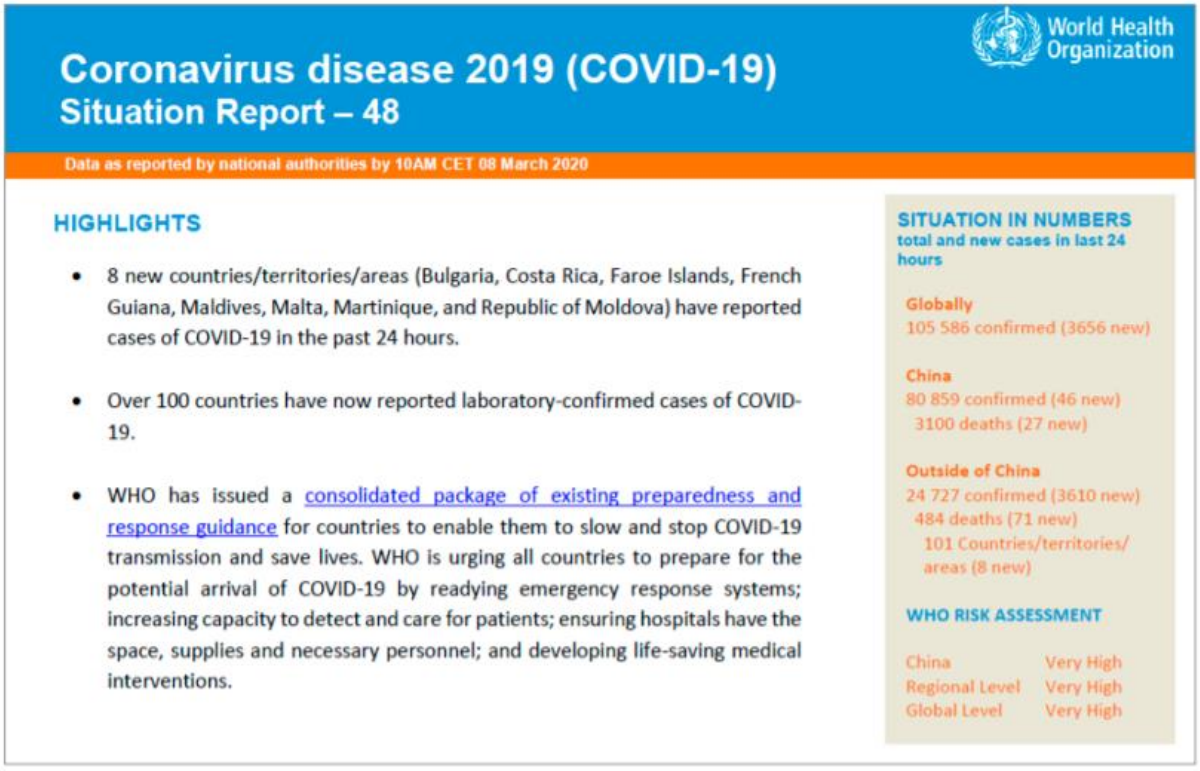

Рисунок 1.4 – Документ з шкідливим програмним забезпеченням, замаскований під інформаційну кампанію ООН щодо розповсюдження COVID-19 [21]

Одним з останніх масштабних ударів по державних інституціях України та Грузії були 14 атак хакерського угрупування “Gamaredon”, що спромоглося сховати шкідницький скрипт в документі, що зображено на рис. 1.5 за допомогою техніки “template injection” та провести обфускацію внесених макро кодів щоб унеможливити їх детектування антивірусним програмним забезпеченням. В

необхідний момент скрипти почали працювати на всіх інфікованих машинах, виводячи її з ладу таким чином, як того хотілося зловмисникам [22].

Рисунок 1.5 – Документ з вкладенням до фішингового електронного листа від хакерського угрупування “Gamaredon”

1.5 Фішинг у правовому полі України

Фішинг– шахрайські дії, спрямовані на виманювання певної інформації, наприклад реквізитів картки, у її власника. Зазвичай власник кредитної картки сам добровільно повідомляє шахраям потрібну інформацію.

Фішинг відноситься до кіберзлочинів. Суб’єктами кіберзлочинів можуть бути фізичні осудні особи, які до моменту їх вчинення досягли шістнадцятирічного віку. В той же час, спеціальний суб’єкт має місце у двох випадках:

● несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах, комп’ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362 Кримінального кодексу України), де суб’єктом виступає

особа, що має право доступу до інформації (ст. 362 Кримінального кодексу України);

● порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них обробляється (ст. 363 Кримінального кодексу України), де суб'єктом виступає особа, яка відповідає за експлуатацію електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Суб'єктивна сторона кіберзлочинів характеризується прямим умислом і, зазвичай, корисливим мотивом; діяння, передбачене ст. 363 Кримінального кодексу України, а саме, порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них обробляється, може вчинятися як умисно, так і через необережність, ставлення до порушення правил може бути умисним (хоч є позиція, що діяння може вчинятися лише у формі необережності).

Об'єктом злочину є суспільні відносини, на які посягають злочини, а предметом злочину слід вважати будь-які речі матеріального світу, з певними властивостями яких кримінальний закон пов'язує наявність у діях особи ознак конкретного складу злочину.

Кримінальна відповідальність:

● карається штрафом,

● обмеженням волі,

● позбавленням волі з позбавленням права обіймати певні посади чи займатися певною діяльністю [23].

1.6 Підходи до захисту від негативного інформаційно-психологічного впливу зловмисників на свідомість працівників

Поки розробники безперервно створюють все більш прогресивні методи захисту підвищуючи тим самим складність компрометації технічних вразливостей, атакуючі усе частіше використовують людський фактор. Зазвичай взлом людського фаервола коштує не більше затрат на декілька телефонних дзвінків чи надістанних електронних листів при тому що атакуючий не піддається майже жодним ризикам [5]. Як бачимо, принаймні з фінансової точки зору атаки, що покладаються на методи соціальної інженерії виявляються більш привабливими для хакерів у порівнянні з підготовкою до просунутих таргетованих атак, вартість проведення яких нерідко може сягати кількох тисяч доларів.

Комерційні продукти (рішення) по безпеці, що використовуються в більшості компаній, головним чином націлені на захист від непрофесійного компьютерного вторгнення, щось на кшталт тих, які влаштовують хакери-початківці також відомі як “script kiddies” [5]. Проте готовністю до захисту від просунутих атак, чи атак соціальних інженерів похвалитись може відносно невелика кількість українських компаній. З точки зору загального рівня безпеки – це є досить реальною проблемою, проте витрачаючи шалені кошти на безпеку бізнес банально не буде мати змогу розвиватись, що в перспективі ставить під сумнів необхідність захисту як такого. Корпоративна безпека може вважатися гарною коли зберігається певний баланс. Занадто низький рівень безпеки створює сприятливі умови для зловмисників експлуатувати вразливі місця систем, при цьому надмірна увага до безпеки призводить до уповільнення розвитку та процвітання компанії. Задача полягає в знаходженні балансу між захищеністю та ефективністю [5].

Складність полягає в тому, шо соціальний інженер вчиться звучати як безпосередній член команди, до якої відноситься жертва, яку намагаються ошукати. Основні інструменти, які використовуються: дружелюбність, використанні корпоративної лексики та можливо деякі психологічні маніпуляції, що є особливими та підбираються до конкретної жертви. Такими маніпуляціями може бути:

- Флірт
- Співчуття
- Залякування (Погрози)

- Відкритість
- Услужливість, тощо.

В більшості випадків, коли жертва вірить в те, що співрозмовник по той бік телефонної лінії чи екрану намагається їх допомогти, або зробити певну послугу для неї, вона більш охоче надасть конфіденційну інформацію яку в іншому випадку захищала б досить ретельно [5].

Впевнившись в тому, що хакери користуються методами соціальної інженерії для отримання будь-якої інформації в межах приватних компаній постає ряд наступних запитань: “А що як бажана інформація знаходиться у володінні національної поліції або національної гвардії? Чи не ризиковано телефонувати правоохоронним органам або військовослужбовцям?”. Всесвітньо відомий хакер Кевін Митник каже: “відповідь – НІ”, адже є дуже специфічне правило, яким користуються соціальні інженери. Вони знають, що службовці силових структур та військові з першого дня на службі привчаються до поваги рагу та/або звання. Таким чином, дзвінок лейтенанту від особи, що представилась майором може дати цій самій особі великий кредит довіри та розуміння того, що будь-яке його прохання буде виконане якнайшвидше. “Лейтенант буде керуватись тими принципами, які він вивчив та використовував роками тому вірогідність провалу цього дзвінка зазвичай менша ніж успіху”, – вважає Митник. Він також зазначає, що військові та правоохоронці – це не єдині категорії людей що мають чітке розуміння ранг, звання чи підпорядкованості, існує багато категорій людей чию природу професійної взаємодії можна експлуатувати подібним чином. Корпоративна ієрархія як на мене видається чи не найкращим прикладом.

В межах будь-якої компанії чи то підприємства мають бути розроблені політики інформаційної безпеки, що мають включати повний спектр того, яким чином інформація з різними рівнями доступу має оброблятися, передаватися, видалятися, тощо. Треба не лише радити працівникам захищати себе та організацію, а вводити ці рекомендації в політики безпеки та зобов’язати працівників слідувати їм. Регламентації потребують наступні пункти:

● Політика використання паролів, що мають складаються більш як з 8 символів та включати букви, цифри та спеціальні знаки (якщо потрібно – використання менеджерів паролів таким як 1Password, LastPass, тощо). Обов'язково змінювати паролі на всіх акаунтах, що мають схожий до скомпроментованого пароль;

● Правила роботи з корпоративною поштовою скринькою (перевіряти email-адресу відправника на предмет виявлення розбіжностей з офіційними назвами, те саме робити з інформаційним наповненням листа; оминати невідомі посилання та не завантажувати вкладення не впевнившись в їх безпечності; відкривши сайт з листа, звертати увагу на його URL, а саме на наявність помилок в назві або будь-яких відмінностей від офіційної, перевіряти домен 1 рівня). При необхідності та наявності досить серйозного бюджету – шифрувати пошту за допомогою програмного забезпечення побудованого на протоколі PGP та використовувати інструменти емуляції запуску вкладень в контрольованому середовищі (sandbox);

● Використовувати додаткові налаштування або розширення браузера і поштового агента для використання функції антиспаму та фільтрації листів;

● Оновлювати операційну систему, антивірус та додатки якими ви користуєтесь для отримання актуального фільтрування та баз даних шкідливого програмного забезпечення;

● Проводити регулярне сканування жорсткого диску антивірусним програмним забезпеченням;

● Використовувати багатофакторну автентифікацію для отримання доступу до будь-якого сервісу, що надає вхід в мережу організації ззовні (біометричний фактор вважається більш стійким);

● За необхідністю проводити шифрування даних на жорстких дисках та резервне копіювання даних та операційної системи;

● Використовувати VPN-сервіси для входу на акаунти та сервіси, що зберігають конфіденційні дані у випадку під'єднання до публічної Wi-Fi мережі;

● Проводити моніторинг останніх сесій користування обліковими засобами, перевіряти список надісланих повідомлень через поштового агента;

● Повідомляти працівників безпеки у випадку отримання листа, що схожий на фішинг, або після необачного відкриття його вмісту провести повне сканування автоматизованого робочого місця (за наявності більшого бюджету – створити та розгорнути сервіс, що буде надавати працівникам можливість в декілька клік ів сповіщати системи захисту та підрозділ безпеки про підозрілі email-и);

● Використовувати програми вилучення тимчасових файлів, якщо специфіка роботи не протирічить цьому;

● Має бути зазначено, що методи соціальної інженерії, зокрема фішинг, несуть серйозні фінансові ризики для організації.

Окрім цього, слід також виділити наступні кроки організації на шляху до покращення загального стану захищеності інформаційних систем та особистого складу з точки зору готовності до виявлення та протидії кібератакам:

● Заохочення керівників організації змінити налаштування безпеки своїх акаунтів в соцмережах та на інших платформах, зробивши їх приватними;

● Забезпечити проведення щорічних тренінгів з інформаційної та кібербезпеки;

● Надавати доступ працівникам тільки до тих ресурсів, сайтів та платформ, які вони мають використовувати для успішного виконання поставлених завдань, або обмежити доступ до інформаційних ресурсів, відімкнути від корпоративної мережі та мережі Інтернет, якщо в їх використанні працівниками немає необхідності;

● Провести конфігурацію брандмауера та фільтра агента електронної пошти на автоматизованих робочих місцях для додаткового захисту мережі від інфікованих файлів, вкладених в фішингові листи;

● Встановити модулі (розширення) для попередження використання сайтами незахищеного з’єднання або їх блокування [24];

● Впровадити системи захисту від кібератак: прикладом може бути SIEM-системи (програмний продукт, який об’єднує управління інформаційною безпекою та управління подіями безпеки) для менеджменту інцидентів з інформаційної безпеки чи SOAR-системи для автоматизації сценаріїв блокування атак.

● Здійснювати регулярний моніторинг, аналіз та поновлення методів, спрямованих на захист від соціальної інженерії та фішингу зокрема.

Кожен співробітник в організації повинен бути навчений проявляти відповідну ступінь підозри та обережності, коли до нього звертається хтось, кого він особисто не знає, особливо коли співрозмовник представляється особою з відповідними правами та просить надати доступ до комп'ютера співробітника чи мережі компанії, установи, тощо. Сама людська природа змушує нас довіряти іншим, але, як кажуть японці: "Бізнес – це війна". В контексті безпеки – це війна, потенційними втратами в якій може бути втрата геть усіх інформаційних активів підприємства та найбільш важливої як на мене складової подальшого існування компанії – її репутації. Як вже зазначалося, політики корпоративної та інформаційної безпеки повинні чітко визначати належну поведінку працівників з тими даними до яких їм надано доступ так само як і на війні солдати отримують засекречені повідомлення від командування на ряду з іншими наказами та рекомендаціями щодо захисту цього самого повідомлення. Це абсолютно реальне порівняння адже існують численні випадки коли занепад компаній починався з помилок працівників або їх недбалого ставлення до політик, що регламентували відповідне ведення їх професійної діяльності.

Кожна людина настільки вразлива до атак соціальної інженерії, що єдиним достатньо ефективним методом захисту, що його може використовувати компанія є навчання та організація тренінгів особистого складу, в яких їм будуть надані відповідні рекомендації необхідні для виявлення соціального інженера. Після цього етапу постійно нагадувати людям про те, що вони дізналися на тренінгу, адже ми схильні забувати про те, чим не користуємося на регулярних основах [25].

Практика показує, що навіть тимчасові токени та паролі або будь-які інші подібні форми аутентифікації не гарантують 100% захист від вправного соціального інженера. Єдиним реально надійним захистом можна вважати сумлінного працівника, який дотримується політики безпеки і розуміє, яким чином соціальні інженери можуть вплинути на його поведінку.

Проаналізувавши кращі підходи в компаніях, державних установах та підприємствах різної форми власності, можна стверджувати, що відділ інформаційної безпеки має проводити навчання співробітників, деталізуючи методи, використовувані соціальними інженерами. Особливу увагу треба приділити регламенту надання відомостей для службового користування особам, які називають себе співробітниками компанії, адже відомості які на перший погляд не є секретними і циркулюють між колегами в межах підрозділу або всієї компанії помилково вважаються нечутливими, хоча можуть бути успішно використаними соціальними інженерами для створення ілюзії того, що вони справді є “колегами з іншого підрозділу” [5].

Кожен працівник має знати, що навіть при наявності у “цифрового” співрозмовника знань процедур взаємодії в компанії, відповідних їм процедур, лексики та внутрішніх ідентифікаторів, він неодмінно має підтвердити особу співрозмовника та впевнитись, що особа має право на задоволення свого інформаційного запиту. Співрозмовник може бути звичайним працівником або підрядником з необхідними процедурними знаннями. Відповідно на кожній компанії лежить відповідальність за визначення відповідного методу для переконання в тому, що співрозмовник і справді є тим за кого себе видає в тих випадках, коли працівники взаємодіють з людьми, яких вони не можуть знати або впізнати по телефону або тим паче в електронному листуванні. Таким чином у випадку коли працівник не може впізнати особу, що видає себе за його колегу, слід зробити принаймні два кроки. Перший: впевнитись, що співрозмовник і справді працює у названій компанії. Друге: перевірити його дозвіл на отримання тих даних для отримання яких було зроблено запит. Якщо протягом спілкування виникають щонайменші сумніви – слід звернутися до відділу безпеки для перевірки і подальшого супроводження цього випадку [5].

При формуванні безпекових тренінгів або корпоративного навчання для співробітників компанії треба наголосити на наступному:

● Кожного разу коли незнайома людина робить запит на отримання певної інформації по телефону, слід ввічливо призупинити бесіду до моменту коли її особа та право на отримання інформації не буду перевірено.

● Надання (розголошення) інформації з обмеженим доступом має відбуватися виключно у відповідності до затверджених політик та процедур. Цей підхід може іти в розріз з природним бажанням працівників допомагати один одному, але саме цю властивість людини і експлуатують соціальні інженери, тому професіоналам не залишається нічого окрім залучення певної здорової параної, що кожен незнайомець потенційно може бути зловмисником.

Тренінги з інформаційної безпеки покликані захистити інформаційні активи компаній від витоку в публічний простір і створені не лише для тих IT-фахівців, що мають безпосередній контакт з вразливою інформацією, а для усіх співробітників компанії. Слід зазначити, що будь-які тренінги або навчальні програми з інформаційної безпеки мають проходити усі працівники підприємства, в свою чергу ті, хто для виконання своїх професійних обов'язків мають контакт з інформаційними активами компанії мають проходити більше спеціалізованих занять з кібербезпеки для розуміння джерел загроз, що без сумніву будуть робити спроби атакувати компанію для неправомірного отримання доступу до непублічних даних. В тренінгах з кібербезпеки обов'язково слід звернути увагу працівників на те, що особа, що знає інших добре відомих вам працівників, розуміється на професійному сленгу та різноманітних процедурах взаємодії працівників з різних підрозділів в рамках компанії чи з компаній-партнерів, все ще може бути не тим за кого себе видає. Під час навчання має бути наголошено: "У випадку сумніву – перевіряйте, звіряйте та робіть усе необхідне для того щоб впевнитись в тому, що інформаційний запит від конкретно цієї особи має бути задоволено" [5].

Розуміючи можливий шквал критики поясню своє бачення того, чому всі працівники компанії незалежно від займаної посади мають мати базові знання з інформаційної безпеки. Ми маємо розуміти, що не тільки боси та керівники компаній володіють цінною а тому і вразливою інформацією, яку намагаються поцупити порушники. В наш час працівники будь-якого рівня можуть стати

мішенями соціальних інженерів, які банально збирають певні дані для майбутніх більш масштабних атак. Це також стосується тих, хто навіть не використовує комп'ютер для виконання своїх професійних обов'язків. Навіть інформація якою володіє прибиральниця, що утилізує знищені шредером документи може бути корисною для соціального інженера, який намагається детально спланувати атаку на "більшого кита". Кевін Митник у своїх сучасних інтерв'ю нерідко і без аби якого сорому згадує про діяльність, що мала назву "dumpster diving" (пірнання у смітник) з метою знайти там важливі і недбало утилізовані компанією документи, папірці з паролями, нотатки про клієнтів тощо.

Що треба зробити аби таргетовані соціальними інженерами працівники не видавали дані з обмеженим доступом тим, кого вони вважають вищими за рангом виявляючи слабкість свого інстинкту? Як уже зазначалося, кожен працівник має пройти тренінг з інформаційної безпеки для розуміння необхідності захисту від промислового шпіонажу та крадіїв інформаційних активів. Слід також чітко роз'яснювати працівникам яка інформація про підприємство або установу де вони працюють є конфіденційною та критично важливою. Обов'язковим є також проведення аудиту всіх даних що циркулюють в межах підприємства або установи та серед персоналу для визначення критичної, важливої та чутливої інформації. Слід також визначити методи, що може використовувати потенційний порушник задля неправомірного заволодіння цією інформацією. В свою чергу тренінги з кібербезпеки мають будуватися навколо відповідей на ці питання, адже захищатися треба від тих методів соціальних інженерів які вони використовують найчастіше та з найбільшим успіхом. Кожен працівник, що має доступ до згаданих попередньо інформаційних активів компанії чи установи при отриманні запиту на отримання певних відомостей або доручення виконання певних дій на корпоративному ПК має задатися наступними питаннями:

1. "У випадку якщо я надам ці відомості найгіршому ворогу своєї організації, чи зможе він, використовуючи їх нанести організації абияку шкоду?";

2. "Чи я цілком розумію потенційний ефект від виконання тих доручень з корпоративним ПК які мені хтось надає?" [5].

Складність у тому, що це неабияк уповільнює процес виконання службових обов'язків і на перший погляд може здаватися що зайві перевірки особистості співрозмовника є зайвою тратою часу і проявом неабиякої параної, проте з іншого боку не перевіряючи та довіряючи усім ми тільки відкриваємо потенційні можливості для соціальних інженерів експлуатувати нашу довірливість та отримувати інформацію до якої вони не мають мати доступ за нормальних умов.

В межах великої організації чи інституції повинна бути створена єдина система реєстрації "подій безпеки" для працівників, які вважають, що вони, можливо, стали мішенню соціального інженера. Наявність єдиного місця для повідомлення про можливі випадки атак дасть можливість фахівцям з інформаційної безпеки відповідним чином їх проаналізувати та забезпечити ефективну систему раннього попередження, яка дасть зрозуміти, коли відбувається скоординована атака, завдяки чому можна уникнути будь-яких потенційних збитків негайно відредагувавши на загрозу.

Митник, який неодноразово збирав попередні дані шляхом телефонної розмови з пересічними працівниками для проведення детально спланованої атаки стверджує: "Якщо у вашій компанії використовуються будь-які види внутрішніх ідентифікаторів, таких як внутрішні номери телефонів, номери співробітників, команд, ідентифікатори рахунків відомств і навіть адреси електронної пошти, то вони повинні розглядатися як конфіденційна інформація, ретельно охоронятися і не надаватися особам, що не підтвердили свій доступ до них".

Під час проведення тренінгів слід звернути увагу всіх працівників на поширену практику прийняття невідомих людей за працівників на тій підставі, що вони звучать авторитетно чи знаються на професійній термінології. Те, що хтось знає процедури передачі даних в межах компанії або використовує внутрішню термінологію, не є підставою вважати, що його особу не потрібно перевіряти іншими способами.

Висновки за розділом 1

Головною задачею кожного співробітника є виконання своїх функціональних обов'язків, які зазвичай не включають контролювання безпекових аспектів. Часто, під тиском кінцевих термінів її виконання або будь-яким іншим тиском обережність та уважність до деталей відходять на другий план та зазвичай ігноруються. Соціальні інженери розраховують саме на такий підхід, коли займаються плануванням своїх атак. Відтак при прийомі співробітників на роботу слід наголошувати, що захист конфіденційних даних не закінчується одним лише підписом під угодою про нерозголошення. Слідування політикам інформаційної безпеки та відповідним політикам обробки, передачі, зберігання та видалення інформації має розцінюватися як обов'язковість, не виконання якої має приводити до дисциплінарних або інших наслідків.

"Безпека – це не продукт, а радше процес. Безпека – це не технологічна проблема, це проблема людей та управління ними", – твердить американский криптограф та фахівець в області комп'ютерної безпеки Брюс Шнайер. З ним важко не погодитись, адже не сьогодні не існує жодного технічного рішення, яке б гарантувало 100% захист обчислювальної мережі від широкого спектру кібератак, особливо від тих, які покладаються на соціальну інженерію.

Директорам та менеджерам із забезпечення інформаційної безпеки в компаніях слід звернути увагу на статистику, що приблизно кожен 5-й користувач інтернету отримував лист, що містив інструмент фішингу на поштову скриньку або стикався з фішингом в кіберпросторі [6]. На великих підприємствах слід проводити комплексний підхід до забезпечення інформаційної безпеки, збереження комерційної таємниці не тільки шляхом впровадження системи інформаційної безпеки, а і проведенням заходів спрямованих на навчання персоналу правильного поводження з інформаційними активами компанії для підтримки сталого розвитку.

Запропонована система захисту від маніпулятивного впливу методів соціальної інженерії на свідомість людей. Зокрема надані практичні рекомендації, методи, засоби та заходи, що мають проводитися для захисту від деструктивного впливу фішингу на особистостей та мінімізацію фінансових втрат спрямованих на відновлення скомпрометованих систем. На жаль, не існує таких інструментів, що

могли б 100% гарантувати захист від СІ, тому основною задачею офіцера з кібербезпеки в цьому контексті я вважаю проведення якісної роз'яснювальної роботи на ряду з відповідними тренінгами з ІБ, що дадуть змогу працівникам мати краще розуміння своїх вразливостей та методів захисту від маніпуляцій злочинців. Слід пам'ятати, що найбільш ефективним методом протидії фішингу є мобілізація усього персоналу компанії, підприємства, установи чи організації на спільну боротьбу з цією загрозою.

РОЗДІЛ 2
ПІДБІР ПІДХОДІВ ДЛЯ ВИЯВЛЕННЯ ФІШИНГОВИХ ЕЛЕМЕНТІВ В ЕЛЕКТРОННИХ ЛИСТАХ

2.1 Визначення можливих підходів для виявлення фішингу в електронних листах

Читання електронних листів стало досить небезпечним заняттям. Електронна пошта може стати пропуском для небезпечних вірусів, експлойтів, які можна запустити, просто відкривши електронну пошту або натиснувши на активне посилання або зображення в електронному листі. Ці фішингові атаки електронною поштою легко виконуються шляхом “email spoofing-у” (підробки листів). Два способи, відомі як “e-mail forging” (підробка електронної пошти) “mass emailing” (масове надсилання електронних листів) дуже полегшили зловмисникам завдання захопити більшу кількість жертв [26].

Одним із способів боротьби з шахрайством, що спирається на фішинг є блокування таких листів ще до того, як вони дістануться кінцевих користувачів. Таким чином задача полягає в створенні відповідної фільтрації на стороні поштового серверу домену чи поштового агента. В цьому розділі будуть визначені та проаналізовані підходи до виявлення фішингових елементів в електронних листах з метою створення прикладного програмного забезпечення яке буде прототипом для системи фільтрації електронних листів у майбутніх дослідженнях.

Проаналізувавши численні фішингові електронні листи було визначено їх наступні особливості:

1. Більша частина фішингових листів розсилається з безкоштовних поштових скриньок;

2. Частина фішингових листів не індивідуалізовані і можуть розсилатися великому списку адресатів;

3. Певні лінгвістичні кліше досить часто використовуються в фішингових листах;

4. Неспівпадіння домену, що підписав електронний листа з сервером електронної пошти до поштової скриньки якого буде надіслана відповідь.

В наступних підрозділах кожна особливість буде досліджена більш детально. Крім цього буде проведена оцінка можливості практичної реалізації фільтрування електронних листів за ідентифікованими особливостями в рамках дипломної роботи.

2.2 Аналіз електронної пошти відправника

Найпростішим та найефективнішим методом пошуку фішингових елементів в електронних листах можна вважати аналіз заголовків електронних листів. Вони містять досить багато інформації. Значна частина цієї інформації ніколи не відображається користувачеві при звичайному відкритті листа через поштового агента. Програма для читання електронних листів бачить лише декілька відомостей, таких як тема, дата, електронна пошта, інформація щодо відправника та адреса для відповіді. Дивно, що інформація, яка фактично відображається користувачеві, може бути легко підроблена!

У заголовках електронної пошти є кілька інших полів, які слід дослідити.

“Return Path”: адресат якому буде надіслана відповідь.

“From”: відправник, який надіслав електронний лист.

Помічено, що для більшості автоматично розісланих спамових чи рекламних розсилок ці записи не співпадають. Хоча, це може стати у нагоді при розробці антиспамові фільтрів, які не є об’єктом дослідження в даній дипломній роботі. Для пошуку саме фішингових елементів слід звернути увагу на наступне: відомі компанії, банки, державні установи або будь-які сервіси та платформи не користуються безкоштовними поштовими сервісами, а мають особистий домен, та використовують його для електронного листування. Таким чином у випадку коли отриманий лист надісланий з публічного домену (наприклад gmail.com), а представлення та інформаційне наповнення листа стверджує на приналежність

певному офіційному суб'єкту - можемо робити попередній висновок про те, що це фішинг. Інший досить часто використовуваний шахрайський трюк полягає в тому, що зловмисники можуть зареєструвати свій особистий домен, який буде виглядати дуже схожим чином на офіційний. Наприклад "oshadbank.ua" (не легітимний) зловмисники маскували під "oschadbank.ua" (легітимний), а "aliexpres.com" (не легітимний) - під "aliexpress.com" (легітимний). В контексті фішингових веб сайтів - їх блокуванням мають займатися інспектори кіберполіції, але в контексті захисту своєї організації інженери з інформаційної безпеки мають створити певні технічні рішення для фільтрації принаймні тих електронних листів інформаційне наповнення яких вказує на приналежність певному офіційному суб'єкту а відправник зареєстрував свою поштову скриньку в публічному домені.

2.3 Аналіз списку розсилки

Як уже зазначалося, в результаті дослідження багатьох фішингових електронних листів була виявлена наступна закономірність: більшість фішингових листів не індивідуалізовані і можуть розсилатися великому списку адресатів. З технічної точки зору це може бути реалізовано за допомогою існуючих сервісів або за допомогою самописних скриптів для розсилки повідомлень величезній кількості адресатів (точнісінько як спам).

Таким чином сервіси, що задумувалися з метою поширення рекламних пропозицій (такі як MassMailer , BulkMail , eMailer та багато інших) перетворюються на зброю у руках зловмисників, які заманюють жертв клікнути на посилання або завантажити вкладення, що в свою чергу призведе до виконання зловмисного коду ті інфікування їх девайсів. Таким чином для проведення масової розсилки за допомогою онлайн сервісу або власного скрипту зловмисники можуть навіть не залишатися в Інтернеті, поки масові розсилки надсилаються [27].

Більшість засобів масової розсилки стосуються клієнтської сторони і вимагають, щоб клієнтський комп'ютер знаходився в Інтернеті під час надсилання електронних листів. Таким чином, соціальні інженери використовують інструмент

масової розсилки найчастіше побудований на PHP, який виконується на стороні сервера, який використовує пропускну здатність скомпрометованого виділеного сервера. При цьому шлях електронного повідомлення після генерації виглядає так, як показано на рис. 2.1.

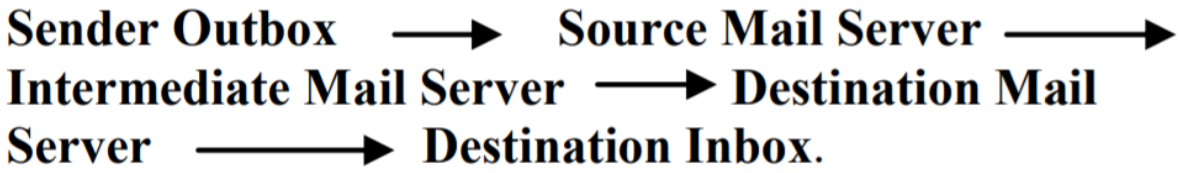

Рисунок 2.1 – Шлях електронного листа від поштової скриньки відправника до поштової скриньки одержувача [27]

Беручи до уваги той факт, що величезна кількість електронних листів, які є спамом чи фішингом розсилаються саме таким чином, інженерам з кібербезпеки було б доцільно створювати певну систему фільтрації вхідних та вихідних (у випадку якщо їх поштовий сервер буде скомпроментовано) електронних повідомлень з метою зупинення атаки на ранній стадії, ще до того, як лист побачить потенційна жертва.

2.4 Аналіз домену, що підписав email

Технології SPF, DKIM та DMARC надають набір інструментів, які можна використовувати для верифікації електронної пошти. Однак точний підхід до розгортання цих механізмів може відрізнятися залежно від конкретного механізму та середовища.

SPF і DKIM забезпечують механізми, що дозволяють одержувачу визначати, чи є електронний лист автентичним. Однак це досягається різними способами, і розуміння різниці методів допомагає з’ясувати, де кожен із них слід використовувати.

SPF ідентифікує електронний лист як автентичний, оскільки він надійшов від уповноваженого джерела. Цю оцінку може зробити лише перший поштовий сервер, який отримав електронне повідомлення після ретрансляції через Інтернет. На відміну від цього, DKIM визначає електронний лист як автентичний, оскільки сам електронний лист автентифікується цифровим підписом. Одержувач може покладатися на цифровий підпис у електронному листі, незалежно від того, звідки він отримав електронне повідомлення.

Вважається, що автентифікація DKIM є більш надійною, оскільки цей механізм автентифікації є:

● портативним і подорожує з електронною поштою незалежно від поштових серверів, через які вона проходить (отже, DKIM можна використовувати для більш складних процесів автентифікації електронної пошти)

● Стійкіший до зламу адже він заснований на криптографії з відкритим ключем (таким чином, стійкий до інших методів атаки, наприклад, "людина посередині").

Однак SPF простіший у впровадженні та має кращу підтримку (завдяки простоті та існуванню як стандарт більший проміжок часу).

Розглядаючи способи автентифікації потоків електронної пошти, організації можуть виявити, що для деяких обставин найкраще підходить DKIM, тоді як інші вимагають використання SPF.

Таким чином використання технологій SPF та DKIM з метою верифікації DNS домену поштового сервера з якого надійшов лист може допомогти ідентифікувати та відкидати фішингові листи ще на етапі їх надходження до SMTP організації. Таки чином працівники навіть ніколи з ними не зустрінуться [28].

2.5 Аналіз інформаційного наповнення email-у

Існує чимало досліджень, предметом проведення яких є методи пошуку фішингових елементів в електронних листах. Чандрашехаран Кришнан (Chandrashekharan Krishnan) напиклад проаналізував структурні властивості

електронних листів, щоб відокремити фішингові листи від автентичних. Основною метою підходу є класифікація фішингових електронних листів із використанням набору характеристик, які залишаються відносно незмінними щодо великої кількості електронних листів. Характеристики, що використовуються, - це мова, композиція, структура фішингового електронного листа, щоб можна було охопити всі різні контексти таких листів. Особливості, що стосуються мови, композиції та письма, такі як окремі синтаксичні та структурні риси, шаблони використання словникового запасу, незвичне вживання мови, стилістичні та суб стилістичні особливості залишаються відносно постійними. Виявлення та вивчення цих структурних особливостей з достатньо високою точністю є дуже складною задачею під час класифікації фішинг-листів [29].

Таким чином можна визначати лінгвістично-частотний аналіз одним із підходів у виявленні елементів спаму та фішингу в електронних листах. В свою чергу виникає складність в тому, що цей метод може використовуватися виключно у поєднанні з іншими адже використовуючи його наодинці може виникнути ситуація коли легітимний лист від певної організації буде розцінено як фішинг виключно тому, що він має схожу до фішингового листа стилістику (і це буде не дивно адже першочергово фішингові листи мали на меті повність скопіювати інформаційну складову автентичних листів додаючи заражені елементи).

2.6 Вибір підходу виявлення фішингових електронних листів

Провівши аналіз кожного із зазначених в розділах 2.2-2.5 методах виявлення елементів фішингу в електронних листах була зведена Таблиця 1 для порівняння їх ефективності, простоті технічної реалізації та необхідності проведення більш детального дослідження.

Таблиця 1

Порівняння методів виявлення фішингу у електронних листах

	Аналіз електронної пошти відправника	**Аналіз списку розсилки**	**Аналіз домену, що підписав email**	**Аналіз інформаційного наповнення email-у**
Ефективність	Висока при наявності бази даних публічних доменів, та доменів, що копіюють назви відомих організацій	Висока при виявленні фішингового листа з масової розсилки і дуже низька при спробі зловмисників індивідуалізовувати листи	Середня зважаючи на те, що деякі бізнеси використовують сервіси для автоматичного відправлення повідомлень (приклад: CRM може надсилати електронні листи використовуючи API іншого поштового серверу)	Середня при використанні як одного з методів виявлення елементів фішингу та досить низька при використанні наодинці
Простота технічної реалізації	Реалізується практично в будь-якому середовищі в форматі фільтру	Реалізується практично в будь-якому середовищі в форматі фільтру	Достатньо лего реалізується на поштовому сервері отримувача	Потребує достатьо клопіткого підходу до вннесення лінгвітичних паттернів або ж розробку систему машинного навчання для виявлення елементів фішингу
Необхідність проведення більш детального дослідження	Існує необхідність створення та пошуку механізмів регулярного оновлення бази даних публічних доменів, та доменів, що копіюють назви відомих організацій	Існує необхідність доопрацювання механізму фітрації адже як не дивно але з самого початку списки розсилки були розроблені для принесення користі та збільшення можливостей, а відтак ними все ще користуються легітимні відправники і не можна створювати	Існує необхідність доопрацювання механізму визначення підходів до зменшення кількості хибних спрацювань	Існує необхідність визначення повного та на жаль не вичерпного переліку лінгвістичних одиниць та патернів, що будуть вважатися підозрілими та розробка механізму машинного навчання аби програма була здатна виявляти

		фільтр який запросто віднесе їх листи в категорію спам\фішинг		закономірності. В іншому випадку - програмний код буде перевантажений кількістю перевірок і

Продовження Таблиці 1

				внаслідок цього швидкодія буде досить помітно знижена.
Загальна оцінка	Має високу ефективність та не має хибних спрацювань при легкості розробки в будь-якому середовищі. Єдиною складністю виявляється необхідність регулярного оновлення бази даних публічних доменів, та доменів, що копіюють назви відомих організацій.	Має загальну середню ефективність адже не захищає від індивідуалізованих фішингових листі. Проте не має хибних спрацювань та достатньо легко розгортається у будь-якому середовищі. Проблематика полягає з ідентифікацією не масового фішингу та потребує подальшого дослідження.	Має ефективність нижче середньої через високу кількість хибних спрацювань. Однак досить простий з точки зору імплементації на поштовому сервері.	Після проведення подальшого досить ретельного дослідження, виявлення лынгвыстичних патернів та розробки відповідного рішення на базі машинного навчання або штучного інтелекту в поєднанні з іншими методами може показати достатньо високий результат. Проте зазначена вище робота виходить за рамки дослідження і буде розглянута в наступних працях.

Висновки за розділом 2

Зважаючи на сучасні Інтернет-технології та їх регулювання, фішинг-атакам не можна повністю запобігти. Оскільки фішинг-листи все ще регулярно надходять багатьом користувачам, очевидно, що фільтри не є 100% ефективні [30]. Крім того, помилкові спрацьовування є серйозною проблемою фільтрів електронної пошти. Через міжнародні проблеми юрисдикції часто важко швидко закрити фішинг-сайти: за даними Робочої групи з боротьби з фішингом (APWG), фішингові сайти залишаються в мережі в середньому протягом 4/5 днів [31].

Щоб рішення із використанням доменних ключів було успішним, рівень прийняття в організаціях повинен бути високим [28]. Резюмуючи, наявні методи запобігання та виявлення фішингу не є 100% надійними проте в певному симбіозі можуть виявляти вже відомі фішингові елементи в електронних листах по заданим патернам, базу даних які слід напрацювати, проаналізувати та розробити алгоритми побудовані на машинному навчанні або на штучному інтелекті для більш вірогідного виявлення та блокування загроз на ранніх стадіях.

В рамках даної дипломної роботи було прийняте рішення розробити систему виявлення фішингових електронних листів побудовану на аналізі електронної пошти відправника адже вона має високу ефективність та не має хибних спрацювань при легкості розробки в будь-якому середовищі.

Складність в необхідності регулярного оновлення бази даних публічних доменів, та доменів, що копіюють назви відомих організацій не буде вирішуватися в конкретній праці з метою уникнення переускладнення на етапі комп'ютерного моделювання та технічної реалізації алгоритму.

РОЗДІЛ 3
ТЕХНІЧНА РЕАЛІЗАЦІЯ СИСТЕМИ ВИЯВЛЕННЯ ФІШИНГ-ЛИСТІВ

3.1 Технічна реалізація системи на основі вибраного підходу ідентифікації фішинг-листів

Як зазначалося в висновках до другого розділу дипломної роботи було прийняте рішення розробити систему виявлення фішингових електронних листів побудовану на аналізі електронної пошти відправника адже вона має високу ефективність та практично нульову кількість хибних спрацювань при легкості розробки в будь-якому середовищі. Складність створення бази даних публічних доменів, та доменів, що копіюють назви відомих організацій буде вирішуватися методом збору цих самих доменів з відкритих джерел та формування відповідної бази даних. Таким чином в рамках дипломної роботи, перевірка домену взятого з електронної адреси відправника буде відбуватися шляхом порівняння її з фіксованою кількістю доменів в базі даних. В майбутньому метод потребує покращення, а саме реалізацію процесу автоматичного оновлення вищезгаданої бази даних.

В свою чергу для тестування системи необхідно передбачити можливість вводу email-у для перевірки та відокремити домен з якого він був надісланий для порівняння з доменами, що складають базу даних використовуючи цикл в залежності від обраного середовища та мови програмування. Також буде передбачена можливість завантажити файл формату “txt” який буде змінювати базу даних за замовчуванням і в такому випадку отриманий з електронної адреси домен буду порівнюватися з наявними в файлі доменами. Слід наголосити, що використовуються домени першого + другого рівнів (наприклад “ukr.net”, “mail.ua” тощо). Слід також передбачити кнопку з приєднаною до неї синхронно виконуваною функцією аби перевірка домену не відбулася раніше ніж користувач

закінчить його набирати яка буде запускати сам алгоритм виокремлення домену та його порівняння з входженнями з обраної бази даних обо текстового файлу.

Обов'язковим також є графічний вивід результатів перевірки разом з поясненням того, чи виявлені елементи фішингу та можливість надати зворотній зв'язок у випадку виникнення помилки або не очікуваного результату.

3.2 Причини та переваги при виборі середовища виконання

Для реалізації системи виявлення фішингових електронних листів побудовану на аналізі електронної пошти відправника з можливістю легкого введення електронної адреси та вибору файлу з доменами середовищем виконання було обрано веб-середовище адже в ньому достатньо легко можна реалізувати введення користувацьких даних та обрання файлів. Крім того, використовуючи мову програмування JavaScript можна буде подавати результати перевірки за допомогою модальних вікон, що виявляється досить звичною для користувачів практикою.

Перевагами використання веб-середовища для реалізації сервісу та вибору мови програмування JavaScript зокрема є наступне:

● Розподіленість – користувач може працювати з системою з будь-якого місця, пов'язаного з WEB-сервером по мережі, перебуваючи в будь-якій точці земної кулі;

● Переносимість – Web-клієнти (браузери) існують для будь-яких платформ, від настільних комп'ютерів до стільникових телефонів. Web-сервера використовуються для більшості платформ, а Web-додатки зазвичай пишуться на кросплатформенних мовах програмування;

● Зручність інтерфейсу – майже кожен користувач комп'ютера хоча б раз запускав браузер і працював в ньому;

● Простота установки і обслуговування – нову версію web-додатки не треба встановлювати на всі комп'ютери - досить встановити на сервер [32] ;

● Швидкість - JavaScript має тенденцію бути дуже швидким, оскільки він часто запускається відразу в браузері клієнта. Поки він не вимагає зовнішніх

ресурсів, JavaScript не сповільнюється через виклики до серверного сервера. Крім того, всі основні браузери підтримують компіляцію JIT (вчасно) для JavaScript, що означає, що немає необхідності компілювати код перед його запуском.

● Простота - синтаксис JavaScript був натхненний Java і його порівняно легко вивчити порівняно з іншими популярними мовами, такими як C ++.

● Популярність - JavaScript є скрізь в Інтернеті, і з появою Node.js все частіше використовується на серверній основі. Існує незліченна кількість ресурсів для вивчення JavaScript. Як StackOverflow, так і GitHub демонструють дедалі більшу кількість проектів, які використовують JavaScript, і привабливість, яку вона здобула за останні роки, очікується лише збільшення.

● Сумісність - На відміну від PHP чи інших мов сценаріїв, JavaScript можна вставити на будь-яку веб-сторінку. JavaScript можна використовувати в багатьох різних видах програм завдяки підтримці інших мов, таких як Pearl та PHP.

● Навантаження сервера - JavaScript працює на стороні клієнта, тому загалом зменшує попит на сервери, а простим програмам сервер може взагалі не знадобитися.

● Розширені інтерфейси - JavaScript можна використовувати для створення таких функцій, як перетягування та компонентів, таких як повзунки, що все значно покращує користувальницький інтерфейс та досвід роботи на сайті.

● Розширена функціональність - Розробники можуть розширити функціональність веб-сторінок, написавши фрагменти JavaScript для сторонніх доповнень, таких як Greasemonkey.

● Універсальність - Є багато способів використовувати JavaScript через сервери Node.js. Якщо ви хотіли завантажити Node.js за допомогою Express, використовувати базу даних документів, як MongoDB, і використовувати JavaScript на інтерфейсі для клієнтів, можна розробити цілу програму JavaScript спереду назад, використовуючи лише JavaScript.

● Оновлення - З моменту появи ECMAScript 5 (специфікація сценаріїв, на яку покладається JavaScript), ECMA International займається оновленням JavaScript щорічно. [33]

3.3 Компоненти сервісу

З огляду на переваги веб-технологій для отримання користувацьких даних в форматі тексту так і файлів було побудовано технічну реалізацію системи виявлення елементів фішингу в електронних листах. Основні її компоненти були винесені на рис. 3.1, де зображено основні етапи алгоритму виявлення фішинг-листів.

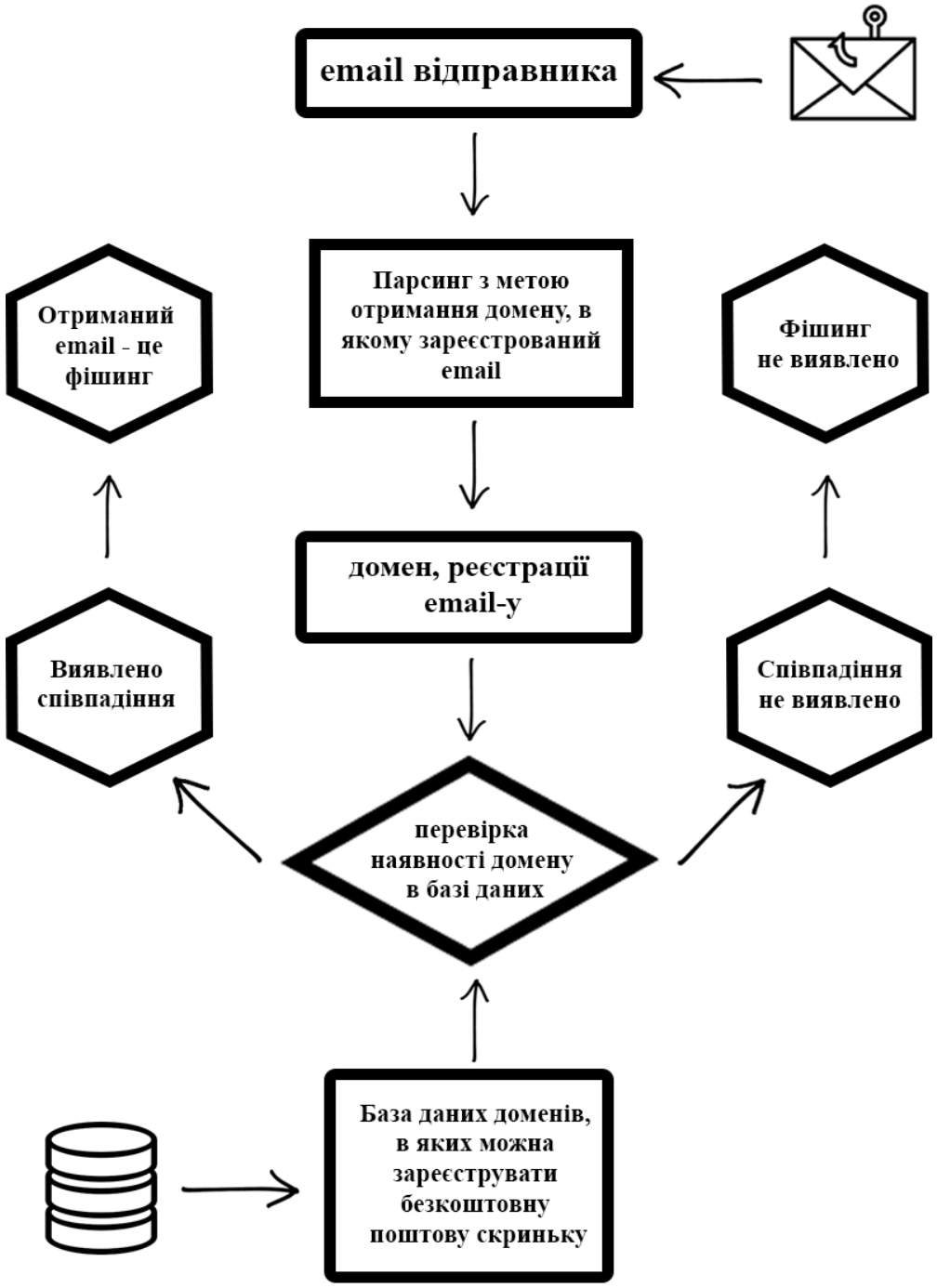

Рисунок 3.1 – Алгоритм ідентифікації фінинг-листів

3.4 Сервіс виявлення фішинг-листів

Для створення такого сервісу було використано каркас розроблений на HTML5 (Додаток А), який було стилізовано за допомогою CSS3 (Додаток В), алгоритмічну складову покладено на мову програмування JavaScript (стандарт ES6) (Додаток Б), крім цього для полегшення верстки було використано фреймворк

Bootstrap 4. Результуючу веб-сторінку можна побачити на рис. 3.2. В свою чергу на рис. 3.3 та рис. 3.4 наочно продемонстрована можливість вибору бази даних доменів за замовчуванням та можливість для юзера обрати текстовий файл з власного ПК.

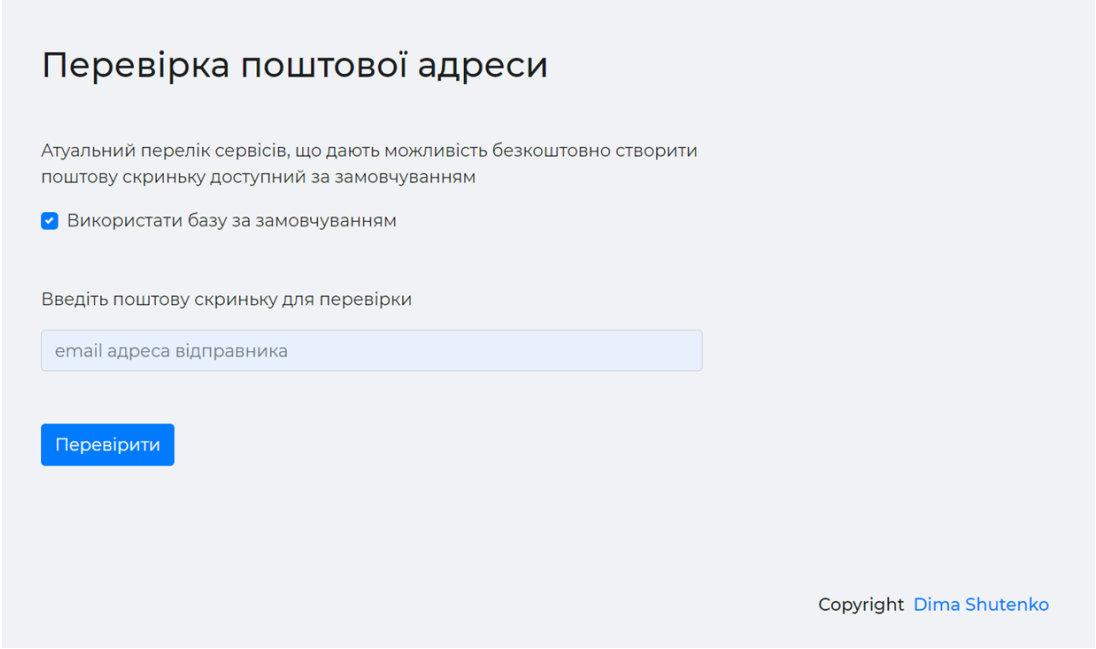

Рисунок 3.2 – Початкова веб-сторінка сервісу виявлення фішинг-листів

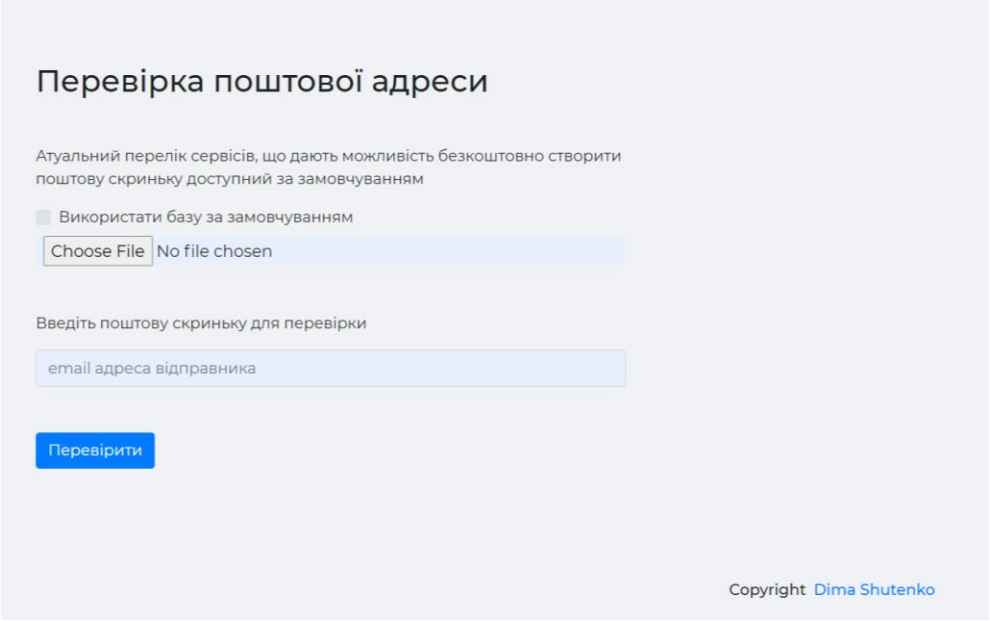

Рисунок 3.3 – Демонстрація можливості завантаження власної бази даних

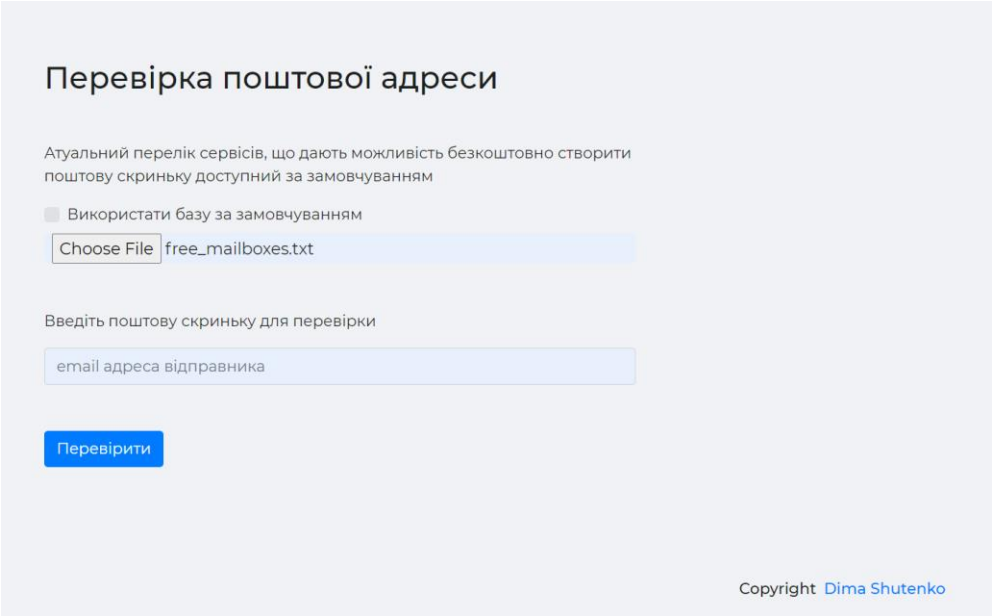

Рисунок 3.4 – Демонстрація можливості завантаження власної бази даних

В свою чергу на рис. 3.5 та рис. 3.6 продемонстровано роботу алгоритму при передачі різних електронних адресів на вході (один із них належить домену корпорації Microsoft, а інший намагається замаскуватися під центр підтримки клієнтів Monobank) відповідно. Таким чином можемо попередньо впевнитись в правильності роботи алгоритму визначення електронних адрес які відносяться до доменів які публічно надають можливість створення електронних поштових скриньок.

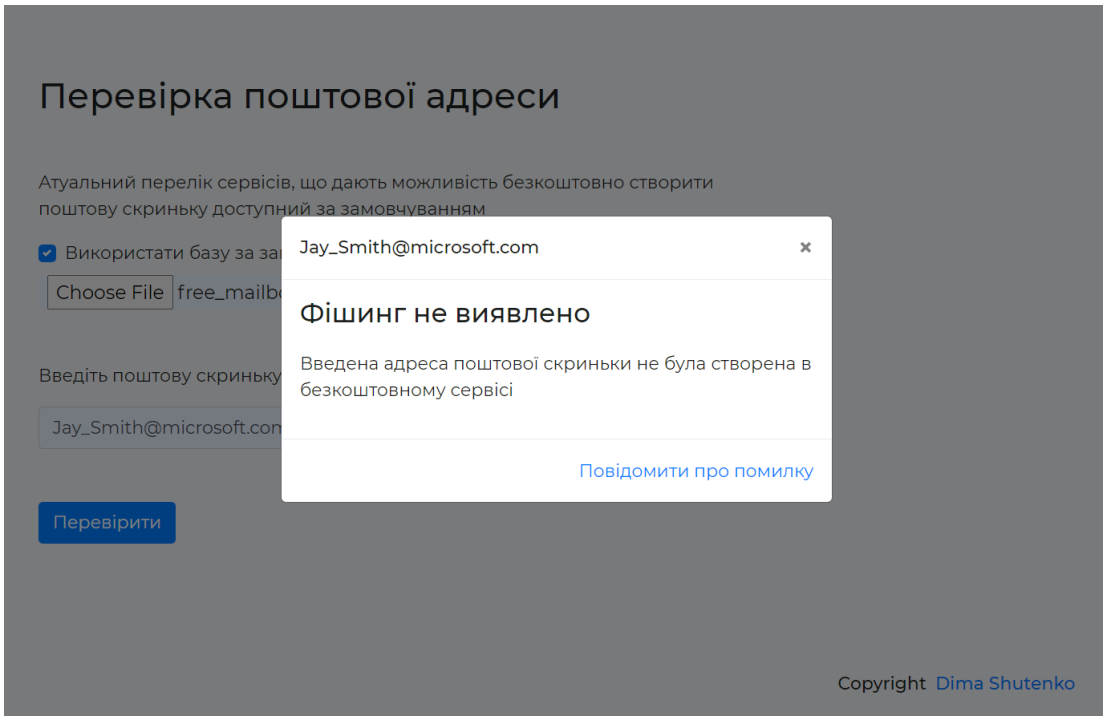

Рисунок 3.5 – Виконання алгоритму при введенні легітимної email адреси відправника

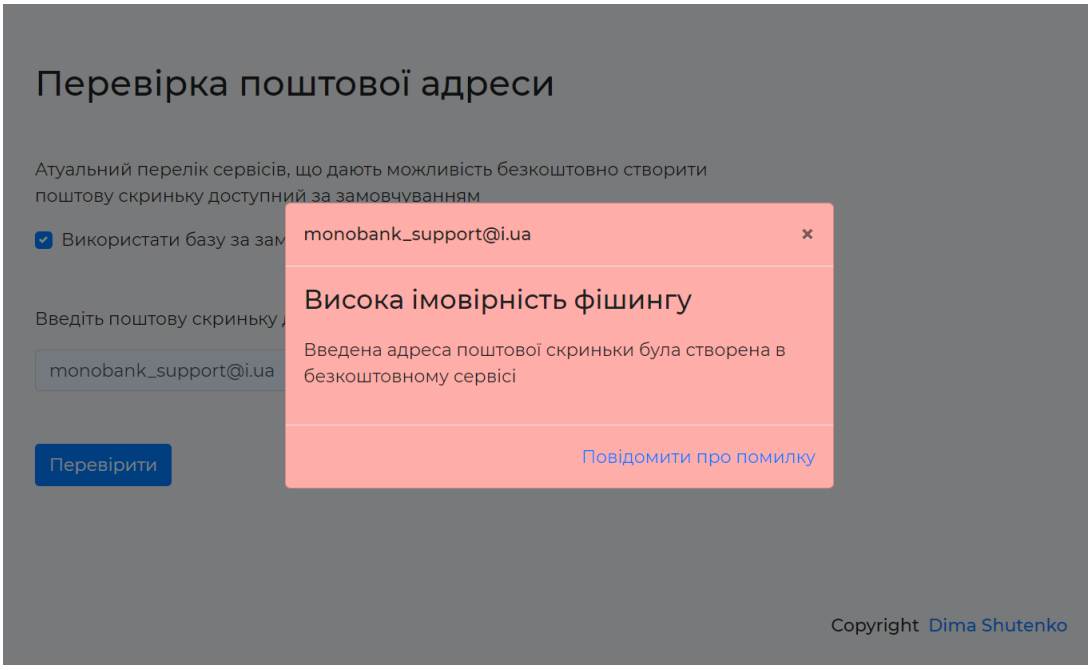

Рисунок 3.6 – Виконання алгоритму при введенні email адреси зловмисника

3.5 Дослідна експлуатація системи виявлення фішинг-листів

Дослідну експлуатацію запропонованої системи виявлення фішинг-листів було проведено на тестовій вибірці з 10 електронних скриньок. У досліджуваному наборі даних з вісьмома фішинговими адресами сервіс виявив 7 email адрес, не ідентифікувавши домен “oshadbank.ua” як фішинговий адже база доменів не включає варіації помилок в написанні усіх популярних сервісів (відповідний рядок позначений сірим кольором). Також слід констатувати відсутність хибних спрацювань.

Таблиця 2

Результати дослідної експлуатації системи виявлення фішингу

Досліджуваний email	Результат дослідження	Категорія email-у [34]
Mr_fisher@amazon.com	Фішинг не виявлено	Легітимний
privat_bank_support@i.ua	Фішинг виявлено	Фішинг
aliexpress@gmail.com	Фішинг виявлено	Фішинг
helpcenter@mvs.gov.ua	Фішинг не виявлено	Легітимний
contact_center@oshadbank.ua	Фішинг не виявлено	Фішинг
support@oschadbank.ua	Фішинг не виявлено	Легітимний
monobank_support@meta.ua	Фішинг виявлено	Фішинг
harvard@cs.com	Фішинг виявлено	Фішинг
helen_ginger@doctor.com	Фішинг виявлено	Фішинг
iphone_update@icloud.com	Фішинг виявлено	Фішинг
youtube-studio@gmx.com	Фішинг виявлено	Фішинг

Результатом проведення дослідної експлуатації системи виявленні фішингових електронних листів стала ефективність у ⅞ = 87%. Такий результат зумовлений недосконалістю щонайменше одного елемента — бази даних доменів

для перевірки, адже на етапі тестування вона не включала домени, які зловмисники можуть вміло замаскувати під відомі сервіси (приклад з Ощадбанком). Крім того, збільшуючи вибірку електронних адрес для тестування відсоток ефективності може знизитися завдяки тому, що внаслідок кібератак можуть бути скомпроментовані поштові сервери легітимних організацій і використовуватися для розсилання фішингових листів. Це неабияк підкреслює необхідність використання симбіозу методів виявлення елементів фішингу в майбутніх дослідженнях.

Висновки за розділом 3

У наш час шахраям доступні численні сервіси та технології для проведення фішинг-атак засобами електронної пошти. Оскільки масові фішингові розсилки надсилаються величезній кількості людей — кількість жертв збільшується пропорційно. Для боротьби з такого роду атаками було запропоновано інструмент для виявлення та запобігання фішинг-атакам, що надходять на електронну пошту у вигляді сфабрикованих листів [35].

Під час розгортання системи було передбачено можливість вводу електронної адреси відправника для перевірки, створено прототип бази даних з доменами, в яких є можливість створення безкоштовної поштової скриньки. Також була передбачена можливість завантажити файл формату “txt” який буде змінювати базу даних за замовчуванням і в такому випадку отриманий з електронної адреси домен порівнюється з наявними в файлі доменами. Крім цього була розроблена кнопка з приєднаною до неї синхронно виконуваною функцією, яка буде запускати сам алгоритм відокремлення домену та його порівняння з входженнями з обраної бази даних обо текстового файлу.

Результатом виконання перевірки є графічний вивід результатів разом з поясненням того, чи виявлені елементи фішингу та можливість надати зворотній зв’язок у випадку виникнення помилки. Після технічної реалізації системи виявлення фішингу в електронних листах була проведена її дослідна експлуатація

методом експериментального дослідження та виявлено, що ефективність розробленого підходу при перевірці з заданими умовами сягнула 87%.

ВИСНОВКИ

У дипломній роботі було висвітлено актуальність такої проблеми як поширення фішингових атак. Фішинг визначається як “атака соціальної інженерії, яка використовує електронну пошту, веб-сторінки соціальних мереж та інші засоби масової інформації для передачі повідомлень, спрямованих на переконання потенційних жертв виконати певні дії (наприклад, введення облікових даних для входу на клоновану веб-сторінку, завантаження вкладення, вбудованого в шкідливе програмне забезпечення, або відкриття інфекційного гіперпосилання) або розголошення конфіденційної інформації на користь зловмисника в контексті кібербезпеки”.

Фішинг може призвести до розкриття конфіденційної інформації, фінансових втрат та зменшення довіри до взламоного ресурсу будь-якої організації.

Зважаючи на це, у роботі було проаналізовано методи соціальної інженерії, зокрема фішинг, як найчастіше використовуваний метод. Було розглянуто фішинг у правовому полі України, а також можливі підходи до захисту від негативного інформаційно-психологічного впливу фішингових атак.

Також було визначено можливі підходи до виявлення фішингу в електронних листах, включаючи аналіз електронної пошти відправника, списку розсилки, домену, що підписав e-mail, інформаційного наповнення email-у тощо.

На основі аналізу було вирішено здійснити технічну реалізацію системи виявлення фішинг-листів, в якій передбачено можливість вводу електронної адреси відправника для перевірки, створено прототип бази даних з доменами, в яких є можливість створення безкоштовної поштової скриньки. Також була передбачена можливість завантажити файл формату “txt” який буде змінювати базу даних за замовчуванням.

Після технічної реалізації системи виявлення фішингу в електронних листах була проведена її дослідна експлуатація методом експериментального дослідження

та виявлено, що ефективність розробленого підходу при перевірці з заданими умовами сягнула 87%.

Таким чином, мету роботи досягнуто, поставлені задачі виконано.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Social engineering explained: How criminals exploit human behavior: веб-сайт. URL: https://www.csoonline.com/article/2124681/what-is-social-engineering.html (дата звернення: 8.06.2021).

2. Social Engineering: an IT Security problem doomed to get worse: веб-сайт. URL: https://medium.com/our-insights/social-engineering-an-it-security-problem-doomed-to-get-worst-c9429ccf3330 (дата звернення: 8.06.2021).

3. Whitepaper “Social Engineering: Exploiting the Weakest Links” by The European Network and Information Security Agency, October 08, веб-сайт. URL: https://www.enisa.europa.eu/publications/archive/social-engineering/at_download/fullReport (дата звернення: 8.06.2021).

4. Оцінювання захищеності інформації в комп’ютерних системах за соціоінженерним підходом / Мохор В.В., Цуркан О.В., Цуркан В.В., Герасимов Р.П.: веб-сайт. URL: http://ceur-ws.org/Vol-2067/paper13.pdf (дата звернення: 8.06.2021).

5. Kevin D. Mitnick / William L. Simon / Steve Wozniak // The Art of Deception: Controlling the Human Element of Security, 2002. 577 p.

6. July 15, 2020 Cybersecurity threatscape, Q1 2020: веб-сайт. URL: https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2020-q1/ (дата звернення: 8.06.2021).

7. ІСТОРІЯ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ПРОТИБОРСТВА: підручник / Я.М.Жарков, Л.Ф.Компанцева, В.В.Остроухов В.М.Петрик, М.М.Присяжнюк, Є.Д.Скулиш. Київ: Науково-видавничий відділ Нпціональної академії СБ України, 2012. 212 с.

8. Біленко А.А., Гайдур Г.І. // ДОСЛІДЖЕННЯ МЕТОДИКИ ПРОТИДІЇ СОЦІАЛЬНОМУ ІНЖИНІРИНГУ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ’ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ: веб-сайт. URL: http://www.dut.edu.ua/uploads/p_422_79548521.pdf (дата звернення: 8.06.2021).

9. Katharina Krombholz, Heidelinde Hobel, Markus Huber, Edgar Weippl // Advanced Social Engineering Attacks: веб-сайт. URL: https://publications.sba-research.org/publications/jisa_revised.pdf (дата звернення: 8.06.2021).

10. Pretexting | Social Engineering: веб-сайт. URL: https://blog.mailfence.com/pretexting/ (дата звернення: 8.06.2021).

11. How to keep your information secure: веб-сайт. URL: https://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure (дата звернення: 8.06.2021).

12. What is phishing? веб-сайт. URL: http://www.phishing.org/what-is-phishing (дата звернення: 8.06.2021).

13. Фишинговая атака: веб-сайт. URL: https://hostiq.ua/blog/internet-phishing/ (дата звернення: 8.06.2021).

14. What are Trojan horses? How do they work? веб-сайт. URL: https://www.enotes.com/homework-help/what-trojan-horses-how-they-work-how-social-789466 (дата звернення: 8.06.2021).

15. What is a Trojan horse? веб-сайт. URL: https://securingtomorrow.mcafee.com/consumer/family-safety/trojan-horse/ (дата звернення: 8.06.2021).

16. Социальная инженерия: метод «Дорожное яблоко»: веб-сайт. URL: http://www.spy-soft.net/socialnaya-inzheneriya-metod-dorozhnoe-yabloko/ (дата звернення: 8.06.2021).

17. Social Engineering: Quid Pro Quo attacks: веб-сайт. URL: https://blog.mailfence.com/quid-pro-quo-attacks/ (дата звернення: 8.06.2021).

18. How to protect insiders from social engineering threats | Reverse social engineering: веб-сайт. URL: https://docs.microsoft.com/en-us/previous-versions/tn-archive/cc875841(v=technet.10) (дата звернення: 8.06.2021).

19. Bernard Oosterloo, Peter Geurtsen, Theo Thiadens, Irene van Santen, Jeffrey Hicks, Peter Wemmenhove // Managing Social Engineering Risk - Making social engineering transparent: веб-сайт. URL: https://essay.utwente.nl/59233/1/scriptie_B_Oosterloo.pdf (дата звернення: 8.06.2021).

20. PhishMe: Q1 2016 Sees 93% of Phishing Emails Contain Ransomware: веб-сайт. URL: https://www.businesswire.com/news/home/20160606005677/en/PhishMe%C2%A0Q1-2016-Sees-93-of-Phishing-Emails-Contain-Ransomware (дата звернення: 8.06.2021).

21. COVID-19 and New Year greetings: an investigation into the tools and methods used by the Higaisa group: веб-сайт. URL: https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/covid-19-and-new-year-greetings-the-higaisa-group/ (дата звернення: 8.06.2021).

22. Gamaredon APT Targeting Ukraine with New Variants: веб-сайт. URL: https://cybleinc.com/2020/10/19/gamaredon-apt-targeting-ukraine-with-new-variants/ (дата звернення: 8.06.2021).

23. Про Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї: Стаття 362 в редакції Закону № 2289-IV від 23.12.2004; із змінами, внесеними згідно із Законами № 770-VIII від 10.11.2015, № 2617-VIII від 22.11.2018. URL: https://kku.com.ua/st-362 (дата звернення: 8.06.2021).

24. Phishing Detection: Analysis of Visual Similarity Based: веб-сайт. URL: https://www.hindawi.com/journals/scn/2017/5421046/ (дата звернення: 8.06.2021).

25. Dimitrios Stergiou // Social Engineering and Influence: веб-сайт. URL: http://www.diva-portal.org/smash/get/diva2:1016104/FULLTEXT02.pdf (дата звернення: 8.06.2021).

26. Ponnurangam Kumaraguru, Steve Sheng, Alessandro Acquisti, Lorrie Cranor / Teaching Johnny not to fall for phish: веб-сайт. URL: https://www.researchgate.net/publication/220169843_Teaching_Johnny_not_to_fall_for_phish (дата звернення: 8.06.2021).

27. Shamal Firake, Pravin Soni, Dr. B.B.Meshram // Phishing E-mail Analysis. – – 2011: веб-сайт. URL: http://www.ijcset.excelingtech.co.uk/vol2issue1/05-vol2issue1.pdf (дата звернення: 8.06.2021).

28. Cyber.gov.au // How to Combat Fake Emails: веб-сайт. URL: https://www.cyber.gov.au/acsc/view-all-content/publications/how-combat-fake-emails (дата звернення: 8.06.2021).

29. M. Chandrashekaran, K. Narayana, S. Upadhyaya, ― Phishing Email Detection Based on Structural Properties‖, symposium on Information Assurance: Intrusion Detection and Prevention, New York, 2006.

30. Ladislav Burita, Petr Matoulek, Kamil Halouzka, Pavel Kozak // Analysis of phishing emails. — 2021: веб-сайт. URL: https://www.aimspress.com/article/doi/10.3934/electreng.2021006?viewType=HTML (дата звернення: 8.06.2021).

31. Phishing Activity Trends Report 4 th Quarter 2020 by APWG: веб-сайт. URL: https://docs.apwg.org/reports/apwg_trends_report_q4_2020.pdf (дата звернення: 8.06.2021).

32. Основные преимущества WEB-технологий: веб-сайт. URL: https://ppt-online.org/507805 (дата звернення: 8.06.2021).

33. Переваги та недоліки JavaScript: веб-сайт. URL: https://hackit-ukraine.com/627-the-advantages-and-disadvantages-of-javascript (дата звернення: 8.06.2021).

34. URLVoid: Check if a Website is Malicious/Scam or Safe/Legit: веб-сайт. URL: https://www.urlvoid.com/ (дата звернення: 8.06.2021).

35. Web Phishing Detection Using a Deep Learning Framework: веб-сайт. URL: https://www.hindawi.com/journals/wcmc/2018/4678746/ (дата звернення: 8.06.2021).

ДОДАТОК А

```
<!DOCTYPE html>
<html lang="ua">
<head>
<meta charset="UTF-8">
<title>Checker</title>
<meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
<script src="https://kit.fontawesome.com/80a7e9f90a.js"></script>
<meta property="og:title" content="Email checker by Dima Shutenko">
<meta property="og:description" content="Phishing email address checker">
<meta property="og:type" content="article">
<meta property="og:image" content="img/image.jpg">
<meta property="og:site_name" content="Phishing email address checker">
<link rel="stylesheet" href="css/normalize.css">
<link href="https://fonts.googleapis.com/css2?family=Montserrat:ital,wght@0,100;0,200;0,300;0,400;0,500;0,600;0,700;0,800;0,900;1,100;1,200;1,300;1,400;1,500;1,600;1,700;1,800;1,900&display=swap" rel="stylesheet">
<link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css" integrity="sha384-Gn5384xqQ1aoWXA+058RXPxPg6fy4IWvTNh0E263XmFcJlSAwiGgFAW/dAiS6JXm" crossorigin="anonymous">
<link rel="stylesheet" href="css/main.css">
<link rel="stylesheet" href="css/media.css">
<link rel="icon" href="img/d.png" type="image/x-icon">
</head>
```

```
<body>
<div id="myModal_fraud" class="modal fade" role="dialog" tabindex="-1">
<div class="modal-dialog modal-dialog-centered" role="document">
<div class="modal-content">
<div class="modal-header">
<h6 class="modal-title">Повідомлення</h6>
<button type="button" class="close" data-dismiss="modal">&times;</button>
</div>
<div class="modal-body">
<h4 class="d-flex" style="margin-bottom: 20px">Велика імовірність фішингу</h4>
<p>Введена адреса поштової скриньки була створена в безкоштовному сервісі</p>
</div>
<div class="modal-footer">
<a href="https://www.linkedin.com/in/dima-shutenko/" class="ml-auto">Повідомити про помилку</a>
</div>
</div>
</div>
</div>
<div id="myModal_no_fraud" class="modal fade" role="dialog" tabindex="-1">
<div class="modal-dialog modal-dialog-centered" role="document">
<div class="modal-content">
<div class="modal-header">
<h6 class="modal-title">Повідомлення</h6>
<button type="button" class="close" data-dismiss="modal">&times;</button></div>
<div class="modal-body">
<h4 class="d-flex" style="margin-bottom: 20px">Фішинг не виявлено</h4>
```

```
<p>Введена адреса поштової скриньки не була створена в безкоштовному сервісі</p>
</div>
<div class="modal-footer">
<a href="https://www.linkedin.com/in/dima-shutenko/"  class="ml-auto">Повідомити про помилку</a>
</div>
</div>
</div>
</div>
<div class="container">
<div class="row">
<div class="col-lg-8">
<h2 class="mb-5">Перевірка поштової адреси</h2>
<div class="">
<div class="d-flex mb-3">Атуальний перелік сервісів, що дають можливість безкоштовно створити поштову скриньку доступний за замовчуванням</div>
<div class="custom-control custom-checkbox d-flex mb-2">
<input type="checkbox" class="custom-control-input" id="use_defaults">
<label class="custom-control-label" for="use_defaults" checked>Використати базу за замовчуванням</label>
</div>
<input type="file" id="file-selector">
<div class="d-flex mb-3 mt-5">Введіть поштову скриньку для перевірки</div>
        <input type="text" class="form-control" id="input-email"  name="user_email" placeholder="email адреса відправника">
<button type="submit" class="btn btn-primary mt-5" onclick="check()">Перевірити</button>
</div>
</div>
```

```
</div>
</div>
<div class="container mt-5">
<h6 class="d-flex ml-auto">Copyright <a href="https://www.linkedin.com/in/dima-shutenko/" class="d-flex ml-2"> Dima Shutenko</a></h6>
</div>
<script src="https://code.jquery.com/jquery-3.2.1.slim.min.js" integrity="sha384-KJ3o2DKtIkvYIK3UENzmM7KCkRr/rE9/Qpg6aAZGJwFDMVNA/GpGFF93hXpG5KkN" crossorigin="anonymous"></script>
<script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js" integrity="sha384-ApNbgh9B+Y1QKtv3Rn7W3mgPxhU9K/ScQsAP7hUibX39j7fakFPskvXusvfa0b4Q" crossorigin="anonymous"></script>
<script src="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js" integrity="sha384-JZR6Spejh4U02d8jOt6vLEHfe/JQGiRRSQQxSfFWpi1MquVdAyjUar5+76PVCmYl" crossorigin="anonymous"></script>
<script src="js/main.js"></script>
</body>
</html>
```

ДОДАТОК Б

```
$(document).ready(function () {
    document.querySelector("#use_defaults").checked = true;
    document.querySelector('#file-selector').style.display = "none";
    document.querySelector('#use_defaults').addEventListener('change', (event) => {
        if (event.currentTarget.checked) {
            document.querySelector('#file-selector').style.display = "none";
        } else {
            document.querySelector('#file-selector').style.display = "block";
        }
    })
    let input = document.querySelector('input[type ="file"]');
    let free_mailboxex_text, free_mailboxex_arr, arr_ = [];
    input.addEventListener('change', function (e) {
        const reader = new FileReader();
        reader.onload = function () {
            free_mailboxex_text = reader.result;
            free_mailboxex_arr = free_mailboxex_text.split("\n");
        }
        reader.readAsText(input.files[0]);
    }, false)
     let arr = [...];  // умисно пропущено через величезну кількість елементів
    check = () => {
        let entered_email = document.querySelector('#input-email').value;
```

```
    var first_split = entered_email.split("@")[1];
    let domain = first_split;
    var second_split = first_split.split(".");
    if (second_split.length == 2) {
    } else if (second_split.length > 2) {
        var str = first_split.substring(first_split.indexOf(".")  + 1);
    }
    document.querySelectorAll('.modal-title').forEach(function (element) {
        element.innerHTML  = entered_email;
    });
            if (document.querySelector("#use_defaults").checked = true) {
        arr.forEach(function (element) {
            arr_.push(element.slice(0,  -1));
        });
    } else {
        free_mailboxex_arr.forEach(function (element) {
            arr_.push(element.slice(0,  -1));
        });
    }
    if (arr_.includes(domain)) {
        $('#myModal_fraud').modal('show');
    } else {
        $('#myModal_no_fraud').modal('show');
    }
}
```

ДОДАТОК В

```
*{
box-sizing: border-box;
}
h1,h2,h3,h4,h5{
margin:0;
}
ul {
margin:  0;
padding: 0;
}
ul li{
margin:  0;
padding: 0;
display: block;
}
a, input, button, .button{
outline:  none;
}
a, input, button, .button:focus{
outline:  none;
}
a, input, button, .button:active{
```

```
outline: none;
}
a, input, button, .button:hover{
outline: none;
text-decoration: none;
}
.color-1{
color: #3664D8;
}
.color-2{
color: #212353;
}
body{
font-family: 'Montserrat', sans-serif;
background: #f0f2f5;
position: relative;
width: 100%;
color: #1c1e21;
}
.container{
max-width: 970px;
        margin: 0 auto;
display: flex;
-webkit-display: flex;
padding-top: 5%;
```

```
    justify-content: center;
}
input{
background-color: #e8f0fe!important;
    width: 100%;
    font-size: 17px;
    padding-left: 8px;
    border-radius: 6px;
}
#myModal_fraud .modal-content{
background: #ffada9;
}
.center_all_text *{
text-align: center;
}
```