МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “СОЦІАЛЬНА ІНЖЕНЕРІЯ В ЦИФРОВОМУ СЕРЕДОВИЩІ АНАЛІЗ НОВИХ МЕТОДІВ ТА ЇХ ВПЛИВУ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ ОРГАНІЗАЦІЇ”

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

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

_____ Ілля ПАЛАМАРЧУК
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41

Ілля ПАЛАМАРЧУК
Ім’я, ПРІЗВИЩЕ

Керівник: Сергій ГОЛОБОРОДЬКО
Ім’я, ПРІЗВИЩЕ

Рецензент: _____
_____
Ім’я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
“____”_____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Паламарчуку Іллі Вікторовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Соціальна інженерія в цифровому середовищі: аналіз нових методів та їх впливу на інформаційну безпеку організації”,
керівник кваліфікаційної роботи ГОЛОБОРОДЬКО Сергій
(ПРІЗВИЩЕ, Ім’я, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “___“ березня 2024 р. №___.

2. Строк подання кваліфікаційної роботи “20” травня 2024 р.

3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека організації, методи та засоби протидії соціоінженерним атакам, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
4.1. Дослідити життєвий цикл, різновиди та типові сценарії соціоінженерних атак.
4.2. Проаналізувати сценарії загроз з використанням нових методів соціальної інженерії в цифровому середовищі.
4.3. Розробити практичні рекомендації для протидії кібератакам з елементами соціальної інженерії.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “11“ березня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2024	
2.	Збір та аналіз літератури.	29.03.2024	
3.	Дослідження теоретичних основ соціальної інженерії та інформаційної безпеки	08.04.2024	
4.	Дослідження сценаріїв загроз з використанням нових методів соціальної інженерії в цифровому середовищі	22.04.2024	
5.	Вивчення інструментів та методів формування обізнаності й навчання персоналу для протидії кібератакам з елементами соціальної інженерії	08.05.2024	
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2024	
7.	Оформлення роботи.	22.05.2024	
8.	Оформлення презентації.	03.06.2024	
9.	Отримання рецензії на роботу.	03.06.2024	
10.	Захист в ДЕК.	__.06.2024	

Здобувачка вищої освіти _____ Ілля ПАЛАМАРЧУК

(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Сергій ГОЛОБОРОДЬКО

(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

Направляється здобувач Паламарчук І.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Соціальна інженерія в цифровому середовищі: аналіз нових методів та їх впливу на інформаційну безпеку організації"

Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач ПАЛАМАРЧУК Ілля у кваліфікаційній роботі дослідив життєвий цикл, різновиди та типові сценарії соціоінженерних атак, проаналізував сценарії загроз з використанням нових методів соціальної інженерії в цифровому середовищі, розробив практичні рекомендації для протидії кібератакам з елементами соціальної інженерії.

ПАЛАМАРЧУК Ілля показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на конференції.

Все це дозволяє оцінити кваліфікаційну роботу здобувача ПАЛАМАРЧУКА Іллі на оцінку "добре" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Сергій ГОЛОБОРОДЬКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Паламарчук І.В. допускається до захисту даної роботи в Державній екзаменаційній комісії.

Завідувач кафедри
управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти ПАЛАМАРЧУКА Іллі
на тему “Соціальна інженерія в цифровому середовищі: аналіз нових методів та їх впливу на інформаційну безпеку організації”

Актуальність. Усвідомлення ризиків соціальної інженерії в цифрову епоху має надзвичайно важливе значення, оскільки значна кількість успішних кібератак стають результатом експлуатації людських слабкостей, а не технічних вразливостей. З розвитком сучасних технік соціальної інженерії організації повинні бути на крок попереду, щоб захиститися від фінансових і репутаційних втрат. Це передбачає оновлення стратегій безпеки, навчання співробітників і дотримання нормативних вимог. З огляду на зазначене дослідження проблеми захисту від сучасних соціоінженерних атак є актуальним науковим завданням.

Позитивні сторони.

1. У роботі проведено детальний аналіз сучасних методів соціальної інженерії та стратегій захисту від подібних атак, що забезпечує всебічне розуміння предмета дослідження.
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків.
3. Автор опрацював значну джерельну базу: 45 публікацій, в тому числі англомовних.
4. За результатами дослідження запропоновано практичні рекомендації для організацій щодо пом'якшення ризиків, пов'язаних із соціальною інженерією.

Недоліки.

1. Доцільно було б приділити більше уваги аналізу сучасних сценаріїв реалізації кібератак з елементами соціальної інженерії і дослідженню програмних інструментів, які можуть бути використані кіберзлочинцями для їх реалізації.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

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

Рецензент: _____ _____
підпис Ім’я, ПРІЗВИЩЕ
_____

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню нових методів соціальної інженерії в цифровому середовищі. Робота складається зі вступу, трьох розділів, що містять 16 рисунків та 1 таблицю, висновків і списку використаних джерел із 45 найменувань. Загальний обсяг роботи становить 77 аркушів, з яких 5 аркушів займає список використаних джерел.

Метою роботи є дослідження нових методів соціальної інженерії та аналіз їх впливу на інформаційну безпеку організації.

Об'єктом дослідження є соціальна інженерія як загроза інформаційній безпеці організації.

Предмет дослідження – особливості реалізації сучасних загроз соціальної інженерії та застосування превентивних та коригувальних заходів.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи порівняння, класифікації, системного підходу до управління інформаційною безпекою.

Як результат у роботі досліджено життєвий цикл, різновиди та типові сценарії соціоінженерних атак; вивчено сценарії загроз з використанням нових методів соціальної інженерії в цифровому середовищі; розроблено практичні рекомендації для протидії кібератакам з елементами соціальної інженерії.

Галузь застосування. Розроблені підходи можуть бути використані для підвищення рівня інформаційної безпеки шляхом впровадження заходів із протидії кібератакам з використанням соціальної інженерії.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, СОЦІАЛЬНА ІНЖЕНЕРІЯ, ФІШИНГ, ШТУЧНИЙ ІНТЕЛЕКТ, СОЦІАЛЬНІ МЕРЕЖІ.

ABSTRACT

The qualification work is devoted to the study of new methods of social engineering in the digital environment. The work consists of an introduction, three chapters containing 16 figures and 1 table, conclusions and a list of 45 references. The total volume of the work is 77 pages, of which 5 pages are occupied by the list of references.

The purpose of the study is to provide a scientific substantiation of the essence of the concept of «social engineering», to study new methods of social engineering and to analyze their impact on the information security of an organization.

The object of the study is social engineering as a threat to the information security of an organization.

The subject of the study is the peculiarities of the implementation of modern threats of social engineering and the application of preventive and corrective measures.

Research methods. To solve the above scientific task, the paper uses methods of comparison, classification, and a systematic approach to information security management.

As a result, the life cycle, types and typical scenarios of social engineering attacks are investigated; threat scenarios using new methods of social engineering in the digital environment are studied; practical recommendations for countering cyberattacks with elements of social engineering are developed.

Field of application. The developed approaches can be used to increase the level of information security by implementing measures to counteract cyberattacks using social engineering.

Keywords: INFORMATION SECURITY, SOCIAL ENGINEERING, PHISHING, ARTIFICIAL INTELLIGENCE, SOCIAL NETWORKS.

ЗМІСТ

ВСТУП

Актуальність теми. Визначальною характеристикою сучасного суспільства є стрімкий розвиток комп'ютерних інформаційних технологій. Інтернет став невід'ємним елементом повсякденного життя, а загрози в кіберпросторі постійно розвиваються, що підкреслює зростаючу потребу в передових технологіях кібербезпеки. Простого усвідомлення цих загроз недостатньо для ефективного реагування на інциденти, тому питання кібербезпеки потребують постійної уваги. Наразі спостерігається помітний дефіцит медіаграмотності серед населення, що призводить до неадекватного сприйняття загроз та недостатнього впровадження необхідних заходів кібербезпеки. Нагальність вирішення цієї проблеми підкреслюється поточним та очікуваним зростанням кількості кібератак із застосуванням методів соціальної інженерії, що зумовлено широким впровадженням технологій електронної економіки та значними масштабами онлайн-комунікації.

Таким чином, соціальна інженерія у сфері інформаційної та кібербезпеки є надзвичайно актуальною в умовах стрімкого розвитку цифрових технологій та інформаційного суспільства. Соціальна інженерія, як метод маніпуляції людьми з метою отримання несанкціонованого доступу до інформації, стала одним із найсерйозніших викликів для сучасних організацій. Успішні атаки соціальних інженерів можуть призвести до значних фінансових втрат, порушення ділових процесів, втрати конфіденційної інформації та пошкодження репутації організацій. З огляду на зазначене дослідження нових методів проведення атак, основою яких є соціальна інженерія є актуальним науковим завданням.

Мета роботи полягає у дослідженні нових методів соціальної інженерії та аналізі їх впливу на інформаційну безпеку організації.

Об’єкт дослідження **–** соціальна інженерія як загроза інформаційній безпеці організації.

Предмет дослідження **–** особливості реалізації сучасних загроз соціальної інженерії та застосування превентивних та коригувальних заходів.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання:**

1. Дослідити життєвий цикл, різновиди та типові сценарії соціоінженерних атак.

2. Проаналізувати сценарії загроз з використанням нових методів соціальної інженерії в цифровому середовищі.

3. Розробити практичні рекомендації для протидії кібератакам з елементами соціальної інженерії.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи порівняння, класифікації, системного підходу до управління інформаційною безпекою.

Практичне значення одержаних результатів. Застосування напрацювань дасть змогу здійснити обґрунтований вибір методів і інструментів для протидії кібератакам, основою яких є соціальна інженерія.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 28 лютого 2024 року.

Розділ 1 ТЕОРЕТИЧНІ ОСНОВИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Перед початком дослідження теми кваліфікаційної роботи необхідно ознайомитися з основними визначеннями у галузі соціальної інженерії, типовими сценаріями та основними методами протидії кібератакам з використанням соціальної інженерії.

1.1 Поняття та сутність соціальної інженерії в контексті забезпечення інформаційної безпеки організації

Соціальна інженерія у галузі інформаційної безпеки – це метод несанкціонованого доступу до захищених інформаційних ресурсів, який базується на способах впливу на людську психологію. Даний метод поєднує в собі як глибокі знання у сфері інформаційних технологій, так і неабиякі навички та знання з соціології та психології [1].

Соціальний інженер – фахівець широкого профілю, який зазвичай володіє нестандартним способом мислення, гнучким розумом, використовує обман, психологічний вплив, переконання, хороші манери в спілкуванні, позитивні та негативні якості людини для того, щоб змусити об’єкт впливу здійснювати дії, які він не робив б зазвичай для незнайомої людини [2].

Загроза, яку становить соціальна інженерія для інформаційної безпеки, є значною, оскільки вона спрямована на маніпулювання людьми, які є найслабшою ланкою в системі захисту. Використовуючи психологічні методи впливу, зловмисники можуть змусити співробітників організацій розкрити конфіденційну інформацію, надати доступ до критично важливих систем або виконати дії, що ставлять під загрозу безпеку. Навіть найсучасніші технічні засоби захисту не завжди можуть протистояти соціальній інженерії, оскільки вона оминає технологічні бар'єри, зосереджуючись на людському факторі. Наслідки таких атак можуть бути серйозними, включаючи фінансові втрати,

шкоду репутації, крадіжку інтелектуальної власності та організаційні порушення.

Основна мета соціальних інженерів – отримати доступ до захищених систем з метою викрадення даних. Відмінною рисою цієї форми атаки є те, що мішенню є не сама машина, а її оператор. Тому очевидно, що всі методи та прийоми, які застосовують соціальні інженери, базуються на використанні притаманних людському фактору слабкостей, які можна вважати вкрай деструктивними. Це пов'язано з тим, що зловмисник може отримати інформацію, наприклад, через телефонну розмову або шляхом проникнення в організацію під виглядом співробітника. Щоб захиститися від такого типу атак, важливо знати про найпоширеніші види шахрайства, розуміти, чого насправді хочуть зловмисники, і вчасно організувати відповідну політику безпеки. Вся інформація в цьому світі захищена людьми, а її основними носіями є також люди, які мають свій звичний набір комплексів, слабкостей та упереджень, якими користуються соціальні інженери.

Соціальна інженерія поділяється на дві категорії: короткострокова і довгострокова. Короткострокова соціальна інженерія проводиться у відносно короткий проміжок часу. Її перевагою є те, що вона не потребує значних витрат часу та ресурсів, а недоліком – те, що соціальний інженер не може примусити людину до якихось значущих дій [3]. Довгострокова соціальна інженерія характеризується необхідністю інвестування значної кількості часу для того, щоб підкорити людину. Недоліком такого підходу є тривалість необхідної підготовки, а перевагою – те, що він дозволяє соціальному інженеру примусити людину до більш значущих дій.

Маніпуляція детально вивчалась і вивчається різними науковцями і Роберт Чалдіні сформулював 6 людських рис, які соціальні інженери можуть використовувати для соціоінженерних атак [4]:

- авторитет;
- здатність вселяти в інших відчуття легкості та впевненості;
- взаємність;

- відповідальність;
- соціальна приналежність;
- обмежена кількість.

Соціальні інженери використовують низку маніпулятивних технік, включаючи довіру, щоб отримати інформацію від об’єктів атак. Приналежність – це здатність формувати почуття спільності з об’єктом впливу через спільні інтереси. Взаємність використовується, коли зловмисник пропонує допомогу та очікує взаємної реакції. Відповідальність грає на бажанні людей виконувати свої обіцянки, змушуючи їх діяти відповідно до інструкцій нападника. Феномен соціальної приналежності експлуатує схильність людини дотримуватися норм своєї соціальної групи. Заклики до дефіциту експлуатують страх втратити вигідну можливість, що може бути використано для впливу на об’єкт атаки, щоб змусити її діяти необдумано і без належного обмірковування.

Організації та уряди зацікавлені в захисті конфіденційної інформації. Технології самі по собі не є достатньо захищеними від вищезгаданих атак [5].

Таким чином можна виділити декілька причин, що полегшують проведення соціоінженерних атак [6]:

- поведінка людини, взаємодія в соціальних мережах;
- сприйняття, надмірна самовпевненість;
- психологічні схильності;
- організаційні фактори;
- брак кваліфікованих людських ресурсів;
- відсутність захисту в системі;
- неефективні апаратні та програмні засоби захисту.

1.2 Огляд типових методів та технік соціальної інженерії

Модель дій соціального інженера поділяється на декілька основних напрямків, що дозволяє зрозуміти різні методи й тактики, які можуть

використовуватися для досягнення злочинних цілей. Ці дії можна розподілити на дві основні категорії: дії над системою та дії над інформацією (рис. 1.1).

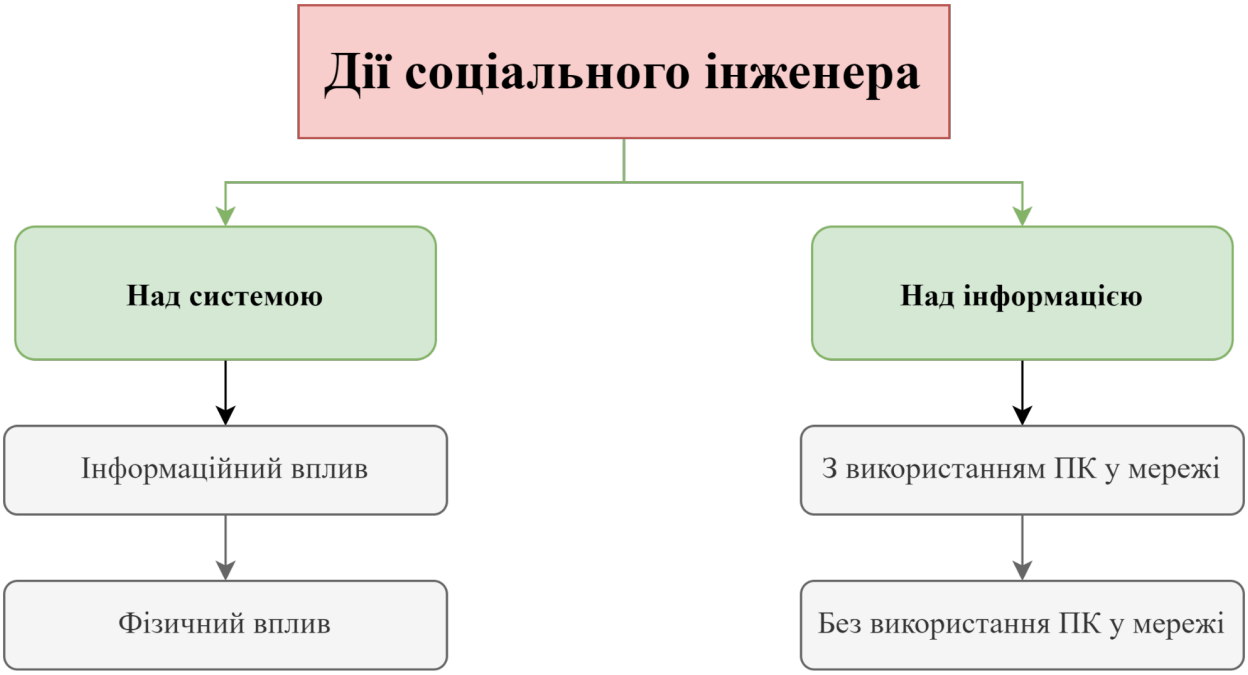

Рис. 1.1. Модель дій соціального інженера

Соціальний інженер може використовувати безліч шкідливих програм для зараження комп'ютерів у цільовій організації. Це можуть бути віруси, трояни, руткіти та інші види шкідливих програм, які можуть викрадати дані, пошкоджувати системи або надавати несанкціонований доступ до комп'ютерів.

У разі успішного проникнення соціальний інженер може видалити або несанкціоновано модифікувати важливі дані, необхідні для нормального функціонування організації. Це може призвести до значних системних збоїв і втрати важливої інформації.

Дестабілізація системних процесів може бути досягнута шляхом зміни або пошкодження критично важливих процесів. Це може спричинити збої в роботі організації, що ускладнює відновлення нормального функціонування системи.

Так, згідно з рис. 1.1. дії соціального інженера з інформацією можна розділити на дві категорії: ті, що проводяться з використанням персонального комп'ютера (ПК), і ті, що проводяться без використання ПК. Наприклад,

соціальний інженер може виконати наступні дії за допомогою ПК, підключеного до локальної мережі організації:

- можливість змінювати існуючі дані дозволяє соціальному інженеру вносити корективи, які можуть сприяти досягненню його цілей, наприклад, змінювати фінансові звіти або інші важливі документи;
- видалення інформації може бути виконано як локально, так і віддалено через мережу. Це може призвести до втрати важливих даних і перешкоджати відновленню нормальної роботи організації;
- інформація може бути скопійована без прямого підключення до мережі організації шляхом фізичного доступу до носіїв інформації, таких як зовнішні жорсткі диски або інші пристрої зберігання даних;
- дані можуть бути видалені без підключення до мережі через фізичний доступ до носіїв інформації, що дозволяє зловмиснику знищити або викрасти критично важливі дані.

Життєвий цикл соціальної інженерії (рис. 1.2) відображає порядок дій соціальних інженерів при реалізації атаки.

Початкова фаза атаки передбачає збір інформації та розвідувальних даних про осіб або організації, на які спрямована атака. Це робиться в рамках підготовки до самої атаки. Зловмисники вивчають потенційні об’єкти впливу, їхні ролі, поведінку та вразливості, які можна експлуатувати.

Друга фаза, «гачок», передбачає реалізацію атаки за допомогою соціальної інженерії. Це відбувається шляхом ініціювання контакту з об’єктами атак та залучення їх до взаємодії через обман. Зловмисники використовують різні приводи, такі як видавання себе за іншу особу, удавання або маніпуляції, щоб завоювати довіру об’єктів впливу і контролювати взаємодію.

На третій фазі зловмисники реалізують заплановану атаку шляхом отримання або несанкціонованого доступу до конфіденційної інформації протягом тривалого періоду часу, використовуючи довіру та зв'язок з об’єктом атаки.

На останній фазі, після отримання бажаної інформації або доступу зловмисники завершують взаємодію відповідно до початкового плану, видаляючи будь-які сліди або докази, які можуть викликати підозру в об’єктів впливу або служб безпеки. Вони замітають сліди й намагаються уникнути викриття.

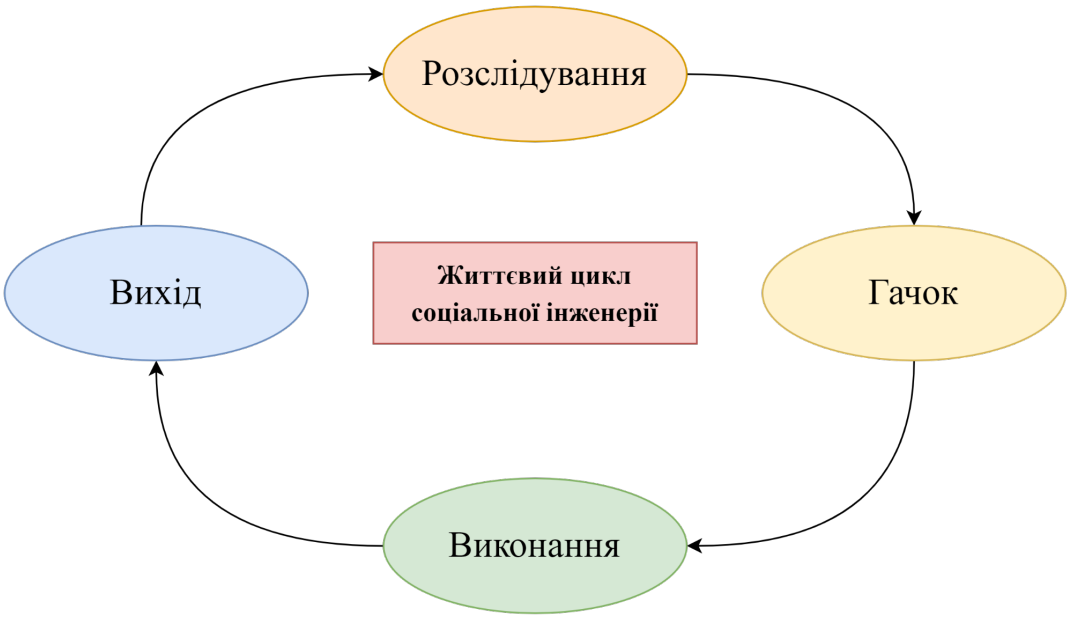

Рис. 1.2. Життєвий цикл соціальної інженерії [7]

Усі атаки соціальних інженерів вкладаються в одну практично незмінну схему, відображену на рис. 1.3:

Рис. 1.3 Схема атаки соціального інженера

Спочатку соціальним інженером формується мета впливу на об’єкт. Тобто обирається, якого результату має досягти атака. Наприклад, результатом атаки

може бути викрадення або видалення даних, вплив на репутацію та надійність організації та інше.

Наступним кроком атаки є збір інформації про об’єкт впливу. Передбачається використання публічних джерел розміщення інформації про організацію, залучення інсайдерів, недоброчесних працівників і т.д. Збір інформації – важливий етап проведення атаки, тому що від нього залежить весь результат, оскільки соціальні інженери не можуть працювати без достатньої кількості інформації. А якісний аналіз об'єкта атаки допомагає і пришвидшує результат.

Визначення найбільш зручних об’єктів впливу – третій крок соціоінженерної атаки. Він повністю базується на зібраній та проаналізованій раніше інформації. Цей етап передбачає вибір доцільних цілей, щоб не бути виявленим та швидше отримати бажаний результат.

Четвертий етап – атракція. Під поняттям атракція мається на увазі пряма взаємодія з об’єктом соціоінженерної атаки. На цьому кроці передбачається використання однієї або кількох технік соціальної інженерії.

Примушення до потрібних дій містить переконання об'єкта атаки вплинути на системи кібербезпеки організації для допуску соціального інженера власне у цю систему. Або, якщо це відповідає меті атаки, цей крок може означати вплив співробітника власноруч на мережу організації, як от видалення даних.

Останній етап – необхідний результат. Соціоінженерна атака здійснена і зловмиснику залишається лише правильно її закінчити. Тобто потрібно не залишити можливості дізнатися про атаку та суб’єкта, який цю атаку здійснював.

Для кращого розкриття поняття соціальної інженерії доцільним завданням вважається аналіз класифікації соціальної інженерії, як це показано на рис. 1.4. Так, за типом впливу соціоінженерні атаки можуть бути класифіковані таким чином: соціотехнічні, технічні, психологічні, соціальні.

За каналом реалізації соціоінженерні атаки можуть бути класифіковані наступним чином: електронна пошта, телефон, соціальні мережі, веб-сайт, фізична атака.

Класифікація реалізації атак соціальної інженерії за оператором: програмне забезпечення, людина [8].

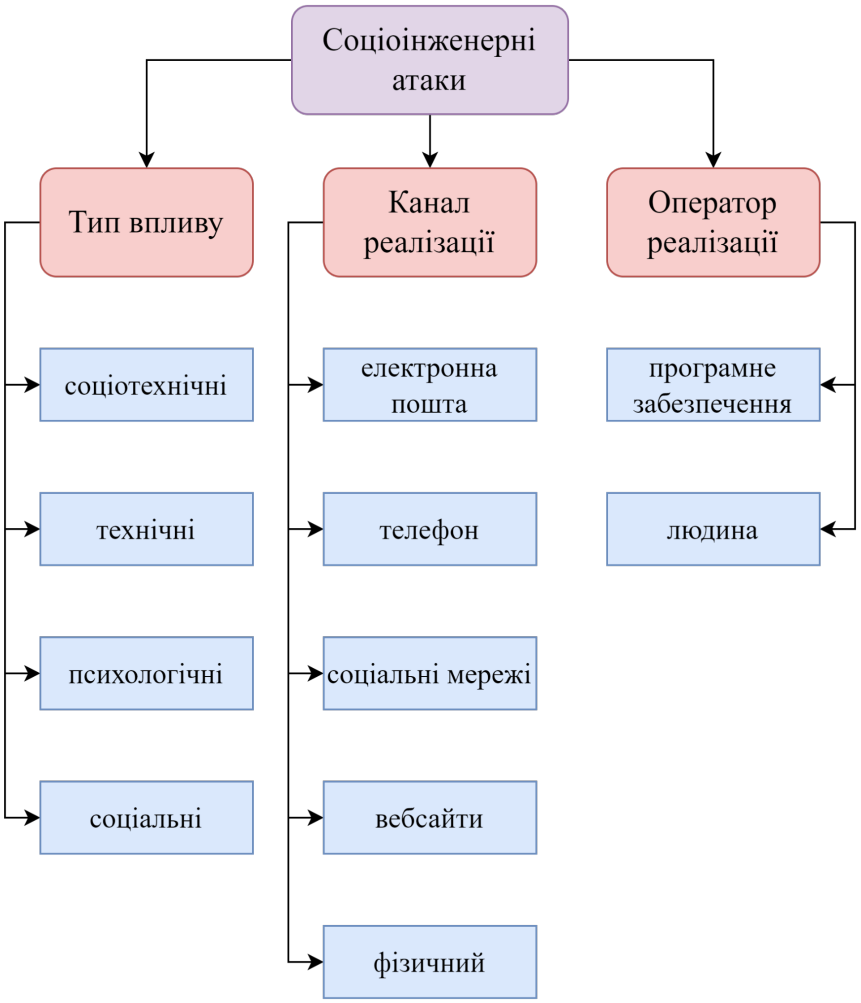

Рис. 1.4. Класифікація соціоінженерних атак

Атаки соціальної інженерії можна розділити на окремі категорії, виходячи з різних точок зору. На рис. 1.5 зображена схема з видами атак, основою яких є соціальна інженерія.

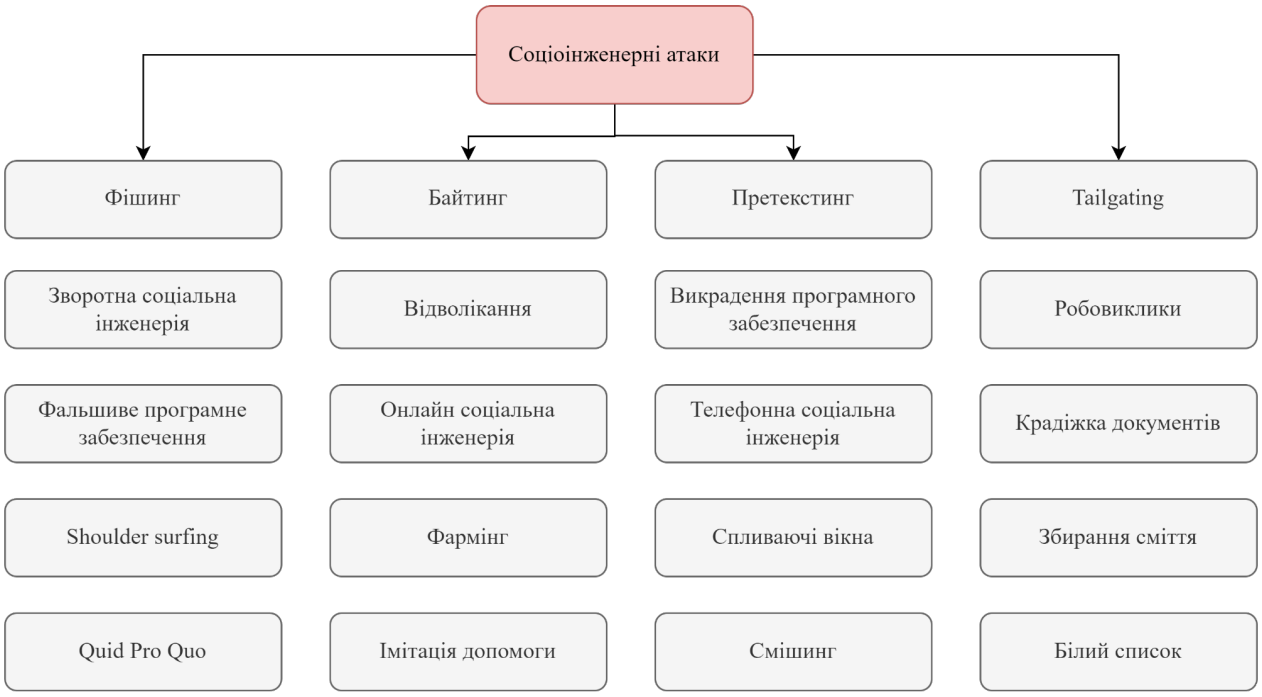

Рис. 1.5. Види соціоінженерних атак

Основним елементом фішингової атаки є повідомлення, надіслане електронною поштою, або іншими електронними засобами зв'язку. Соціальний інженер може використовувати публічні ресурси, щоб зібрати важливу інформацію про особистий та професійний досвід об'єкта впливу. Ці ресурси використовуються для збору такої інформації, як ім'я та прізвище потенційного об'єкта атаки, місцезнаходження та адресу електронної пошти, інтереси та діяльність.

Соціальний інженер може використовувати цю інформацію для створення персоналізованого фейкового фішингового повідомлення. Зазвичай, електронний лист, який отримує об’єкт впливу, виглядає як лист від відомої особи або організації. Атаки здійснюються за допомогою шкідливих вкладень або посилань на шкідливі веб-сайти. Зловмисники часто створюють фальшиві веб-сайт, які начебто належать надійній організації, наприклад, банку, робочому місцю або університету об'єкта атаки. Зловмисники намагаються зібрати конфіденційну інформацію, наприклад, імена користувачів і паролі або платіжну інформацію через ці веб-сайти.

Претекстинг-атаки полягають у створенні фальшивих і правдоподібних сценаріїв для крадіжки персональних даних об’єкту впливу. Вони покладаються на приводи, які змушують об’єкт впливу повірити та довіритися зловмиснику. Атака здійснюється за допомогою телефону, електронної пошти або фізичних засобів [9]. Зловмисники публікують інформацію в довідниках співробітників, на публічних веб-сайтах або на особистих конференціях, щоб здійснити атаку. Приводом може бути пропозиція надати послуги або знайти роботу, попросити особисту інформацію, допомогти другу отримати доступ до інформації.

Байтинг – це вид соціальної інженерії, коли шахрай використовує неправдиві обіцянки, щоб заманити об’єкт атаки в пастку, яка може призвести до крадіжки особистої та фінансової інформації або встановлення шкідливого програмного забезпечення в системі. Пастка може мати вигляд шкідливого вкладення зі спокусливою назвою. Найпоширеніша форма приманки передбачає використання фізичних методів для поширення шкідливого програмного забезпечення. Наприклад, зловмисники можуть вставляти інфіковані шкідливим програмним забезпеченням флеш-накопичувачі у видимі місця, де, на їхню думку, потенційні об’єкти впливу їх побачать. Коли об’єкт атаки вставляє флешку в комп'ютер на роботі чи вдома, шкідливе програмне забезпечення автоматично інсталюється в систему. Шахрайські програми-приманки також доступні в Інтернеті у вигляді привабливих рекламних оголошень, які перенаправляють користувачів на шкідливі веб-сайти або спонукають їх завантажити заражену шкідливим програмним забезпеченням програму.

Tailgating («тейлгейтинг») – це різновид соціальної інженерії, коли несанкціонований користувач отримує фізичний доступ до забороненого місця, наприклад, захищеної системою контрою доступу зони, з наміром викрасти конфіденційну інформацію, пошкодити майно, скомпрометувати облікові дані користувача або навіть встановити шкідливе програмне забезпечення на комп'ютери [10]. Хоча терміни «хвостові атаки» та «piggybacking» часто використовують як взаємозамінні, важливо пам'ятати, що вони мають чіткі відмінності. Tailgating – це випадки, коли зловмисник стежить за користувачем,

який нічого не підозрює, з наміром отримати доступ до несанкціонованого домену. І навпаки, в атаці «piggybacking» співробітник або колишній співробітник свідомо надає доступ до захищеного середовища неавторизованій особі в рамках скоординованої атаки.

Програми-вимагачі – це різновид шкідливого програмного забезпечення, призначеного для того, щоб відмовити користувачам або компаніям у доступі до файлів на їхніх комп'ютерах. Зламуючи ці файли і вимагаючи викуп за ключ до розшифрування, зловмисники ставлять організації в ситуацію, коли сплата викупу є найпростішим і найдешевшим способом повернути доступ до цих файлів. Деякі варіанти програм-вимагачів додають нові функції, такі як крадіжка даних, щоб ще більше заохотити об’єкти впливу до сплати викупу. Програми-вимагачі швидко стали найбільш значущим і помітним типом шкідливого програмного забезпечення. Нещодавні атаки програм-вимагачів призвели до того, що лікарні не змогли надавати основні послуги, порушили роботу державних служб у мегаполісах і завдали значної шкоди різним фірмам [11].

Атаки з фальшивим програмним забезпеченням базуються на використанні підроблених сайтів, щоб обдурити об’єкт впливу і змусити її повірити в те, що це відомі і надійні сайти або програмне забезпечення. Об’єкт впливу вводить свої дані для входу на фальшивому сайті, який потім надає зловмиснику облікові дані об’єкту впливу для використання на легальному сайті. Це може бути використано, наприклад, для отримання доступу до банківських рахунків в Інтернеті. Одним із прикладів таких загроз є перехоплення вкладок, при якому використовується підроблений веб-сайт, що імітує сторінку входу на популярний веб-сайт, який часто відвідує об’єкт впливу. Це може бути онлайн-банкінг, Facebook або Twitter. Об’єкт атаки вводить свої дані для входу, не звертаючи увагу на можливі відмінності в оформленні сторінки для авторизації або в доменному імені. Таким чином, після успішної авторизації об’єктом атаки на фальшивому веб-сайті, зловмисник отримує доступ до його облікових даних.

Використання зворотної соціальної інженерії включає три основні кроки: створення проблеми, наприклад, блокування мережі; реклама того, що

зловмисник є єдиною людиною, яка може вирішити цю проблему; і вирішення проблеми шляхом вилучення потрібної інформації і залишення її так, щоб її не помітили.

Ряд інших типів атак можна узагальнити наступним чином:

- атаки-пастки, які пропонують безкоштовні послуги зі звабленням об'єкта впливу, що вимагають обміну інформацією в обмін на послугу або товар;
- онлайн-атаки, що здійснюються особами, які видають себе за мережевих адміністраторів і запитують імена користувачів і паролі у об’єктів впливу, які нічого не підозрюють.
- фармінг-атаки, що полягають у перенаправленні трафіку з певного веб-сайту на підроблений, що дозволяє зловмиснику отримати передану інформацію.

1.3 Оцінка впливу соціальної інженерії на інформаційну безпеку організацій

Успішна реалізація соціоінженерної атаки може завдати серйозної шкоди організації в різних аспектах. Важливо вміти відмічати, до яких втрат може призвести та чи інша атака. Правильне та швидке усвідомлення втрат здатне покращити планування ресурсів та бюджету, дозволити краще оцінювати ризики, пріоритезувати заходи безпеки та покращити стратегії реагування.

Розуміння того, до яких витрат може призвести та чи інша атака є важливим аспектом управління інформаційною безпекою, який сприяє ефективному використанню ресурсів, підвищенню захищеності організації та забезпеченню безперервності бізнесу. Наслідки успішної реалізації соціоінженерної атаки для організації можуть бути розділені на 4 категорії (рис. 1.6).

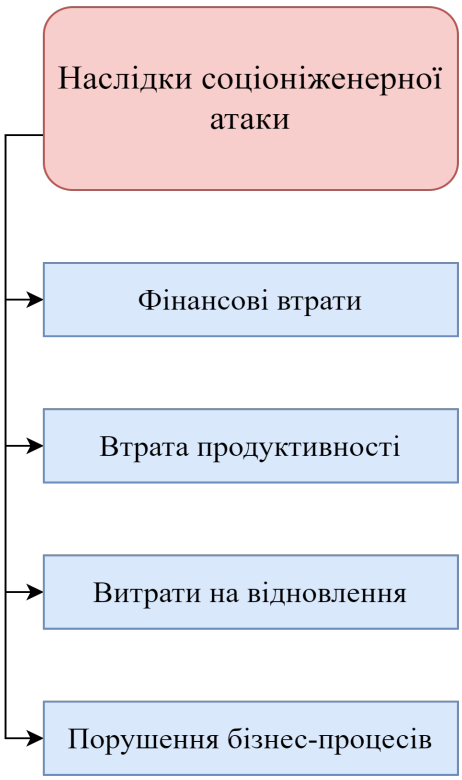

Рис. 1.6. Наслідки соціоінжерної атаки

Фінансові втрати є одним із найбільш відомих наслідків атак соціальної інженерії. Кількість грошей, яку організація може втратити безпосередньо внаслідок такої атаки, може значно варіюватися залежно від масштабів компанії та апетитів зловмисника, починаючи від десятків тисяч до мільйонів доларів.

Успішні кібератаки серйозно порушують нормальну ділову діяльність IT-відділу та деяким керівникам доводиться відкладати свої основні завдання для усунення наслідків атаки, повідомлення всіх працівників про інцидент і навчання їх щодо запобігання подібним атакам у майбутньому. Це відволікає співробітників від їх основних обов'язків, суттєво знижуючи загальну продуктивність праці.

Ще одним значним фінансовим тягарем є витрати на відновлення після атаки. Це включає оплату роботи команди реагування на інциденти, придбання нових програмних рішень для попередження майбутніх атак, а також вирішення проблем із клієнтами, чиї дані могли бути викрадені.

Атаки соціальної інженерії також призводять до порушення бізнес-процесів. Це відбивається на рівні задоволеності клієнтів і функціонуванні ланцюга поставок. Переривання звичайних операцій може призвести до зупинки виробництва, затримок у доставці та інших процесів, що в результаті може спричинити втрату клієнтів та постачальників. Крім того, страхові компанії та банки можуть переглядати свої відносини з компанією після таких інцидентів.

Репутаційні втрати є ще одним важливим наслідком атак соціальної інженерії. Клієнти та постачальники можуть втратити довіру до компанії, яка зазнала значного порушення кібербезпеки, що часто призводить до втрати ділових відносин. Багато підприємств після таких атак втрачають значну частину своєї клієнтської бази та постачальників, оскільки люди не хочуть наражати себе та свою інформацію на небезпеку.

1.4 Аналіз способів протидії кібератакам з елементами соціальної інженерії

З огляду на те, що кібератаки з використанням соціальної інженерії залишаються актуальною проблемою вже протягом певного часу, були розроблені різні стратегії для вирішення цієї проблеми.

Першим способом є тестування на проникнення за соціоінженерним підходом, який є одним з ефективних методів протидії соціальній інженерії. Цей підхід передбачає використання спеціальних інструментальних засобів, таких як Social-Engineer Toolkit (SET), який дозволяє автоматизувати процес створення та реалізації векторів атак, спрямованих на соціальну інженерію. Однією з ключових переваг цього методу є його автоматизованість, що дозволяє значно зменшити час та зусилля, необхідні для проведення тестування. Інтерфейс SET показаний на рис. 1.7. Крім того, за допомогою SET можна створити досить правдоподібні сценарії атаки, що дозволяє оцінити рівень вразливості системи до соціоінженерних атак.

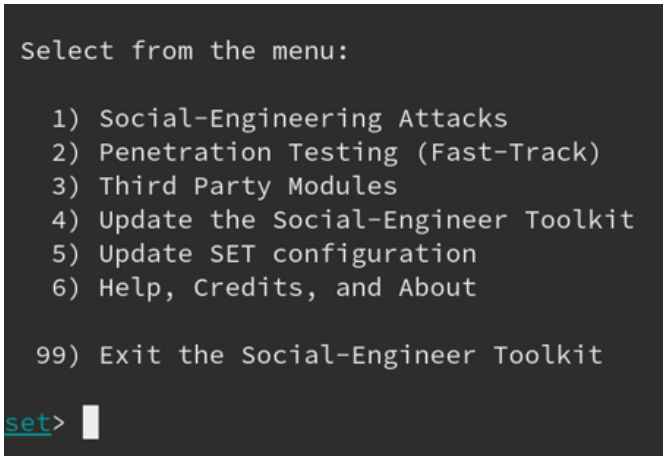

Рис. 1.7. Інтерфейс SET [12]

Проте, необхідно враховувати, що для успішного використання цього методу необхідна відповідна кваліфікація користувача. Навички та знання в галузі кібербезпеки є важливими для ефективного використання SET та аналізу результатів тестування. Також важливо мати розуміння процесів та технік, які використовуються соціальними інженерами, для того щоб адекватно оцінювати створені вектори атак та їхні наслідки. Тому, не дивлячись на потенційну ефективність методу, його успішність залежить від професійної підготовки та досвіду фахівця, який здійснює тестування на проникнення.

Другим способом є метод моделювання дій об’єкта та суб’єкта соціоінженерного впливу. Це стратегічний підхід до протидії соціальній інженерії, який базується на розподілі ролей між нападником і захисником. Цей підхід передбачає аналіз та моделювання дій обох сторін з метою оцінки ефективності заходів протидії.

На початковому етапі методу виокремлюються дві ключові ролі: нападника та захисника. Нападник спрямовує свої зусилля на реалізацію соціоінженерних атак, тоді як захисник протидіє цьому впливу, застосовуючи відповідні заходи безпеки.

Після визначення ролей об’єкта та суб’єкта впливу, проводиться моделювання їхніх дій. Це може включати аналіз потенційних сценаріїв атак та реакції на них з обох сторін. Шляхом цього моделювання визначається

ефективність заходів протидії та виявляються можливі слабкі місця в системі захисту.

Необхідно враховувати, що результативність цього методу значно залежить від наявності і адекватності шаблонів атак, які використовуються для моделювання. Крім того, успішна протидія соціальній інженерії в цьому контексті вимагає розробки та впровадження ефективних стратегій та технік захисту, які враховують специфіку цього виду загроз.

Третім способом є метод виявлення і повідомлення про атаки соціальної інженерії, заснований на взаємодії та активній участі користувачів у процесі виявлення та реагування на потенційні загрози. Основною ідеєю цього методу є залучення людського фактору до процесу забезпечення кібербезпеки.

Для реалізації цього підходу використовуються спеціальні інструментальні засоби, такі як Cogni-Sense, які дозволяють автоматично виявляти можливі загрози та сповіщати про них персонал. Основною перевагою даного методу є можливість активної участі користувачів у забезпеченні безпеки інформації в організації.

Проте, ефективність цього методу обмежується досвідом персоналу та наявністю відповідних шаблонів атак. Без належного розуміння типових сценаріїв та методів, використовуваних соціальними інженерами, персонал може недооцінити загрози або неправильно реагувати на них. Тому для ефективного використання цього методу необхідно надавати належний тренінг та підготовку персоналу.

Метод виявлення і повідомлення про атаки соціальної інженерії людиною. Цей метод практично реалізовано як інструментальний засіб Cogni-Sense. Тому для виявлення і, як наслідок, повідомлення про випадки реалізації атак соціальної інженерії достатньо тільки одного повідомлення від користувача. Такий підхід дозволяє залучати працівників організації не тільки для профілактики за допомогою, наприклад, кібергігієни, а й для активного повідомлення про загрози кібербезпеці [13].

Наступним способом є метод протидії використанню соціальної інженерії за SEDF (Social Engineering Defensive Framework). Це комплексний підхід до кібербезпеки, спрямований на виявлення, аналіз та ефективну протидію атакам соціальної інженерії. До основних компонентів цього методу відносяться:

- оцінка контрзаходів, яка є ключовим компонентом методу SEDF і допомагає визначити наявні можливості та ресурси для ефективної протидії атакам соціальної інженерії;
- підготовка персоналу, яка передбачає підготовку та навчання персоналу з питань кібербезпеки для підвищення обізнаності та готовності реагувати на потенційні загрози;
- однією з ключових переваг SEDF є його здатність адаптуватися до конкретних вимог та операційного контексту організації. Крім того, вона пропонує гнучкість у впровадженні, що дозволяє кожній організації обирати найбільш відповідні заходи захисту відповідно до своїх потреб.

Висновки до розділу 1

У першому розділі було розглянуто теоретичні основи соціальної інженерії та її вплив на інформаційну безпеку. Було детально проаналізовано поняття соціальної інженерії, визначено її сутність та ключові аспекти, що дозволяють зловмисникам маніпулювати людською психологією для отримання конфіденційної інформації. Було охарактеризовано основні методи та техніки соціальної інженерії, такі як фішинг та його різновиди, претекстинг, фізичні атаки соціальної інженерії тощо, що демонструють різноманітність підходів до обману користувачів. Розглянуто вплив соціальної інженерії на інформаційну безпеку організацій, де підкреслено вразливість людського фактору як одного з найбільш суттєвих ризиків для захисту інформаційних систем.

Окрім того, було здійснено огляд існуючих способів протидії кібератакам, основою яких є соціальна інженерія. Визначено, що ефективна протидія вимагає комплексного підходу, включаючи технічні засоби захисту, підвищення рівня

обізнаності співробітників та впровадження процедурних заходів. Наведено приклади успішних стратегій, таких як моделювання дій об’єкта та суб’єкта атаки, SET, SEDF, Cogni-Sense, що використовуються в сучасних організаціях для зменшення ризиків, пов’язаних із соціальною інженерією.

Таким чином, перший розділ надає фундаментальне розуміння природи соціальної інженерії та її значення для інформаційної безпеки, створюючи основу для подальших досліджень і практичних рекомендацій у цій сфері.

Розділ 2 АНАЛІЗ СЦЕНАРІЇВ ЗАГРОЗ З ВИКОРИСТАННЯМ НОВИХ МЕТОДІВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ В ЦИФРОВОМУ СЕРЕДОВИЩІ

Для досягнення мети дослідження необхідно розглянути сучасні сценарії загроз з використанням новітніх методів соціальної інженерії в цифровому середовищі. Базуючись на розглянутих випадках, буде проведено аналіз вразливостей та потенційних наслідків успішних кібератак із застосуванням соціальної інженерії.

2.1. Соціальна інженерія в соціальних мережах та месенджерах

З розвитком інформаційних технологій та зростанням популярності соціальних мереж та месенджерів, ці платформи стали головною мішенню для соціальних інженерів. У розділі розглянуто, як соціальні інженери використовують соціальні мережі та месенджери для досягнення своїх цілей, які методи та техніки вони застосовують, та як можна ефективно протидіяти цим загрозам.

Найчастіше українці користуються такими соціальними мережами, як Telegram (71,3%), YouTube (66,2%) та Facebook (55%). Крім того, 50% респондентів читають новини у Viber, 29,5% – в Instagram, 25,1% – у TikTok та 8,3% – у Twitter (рис. 2.1) [14].

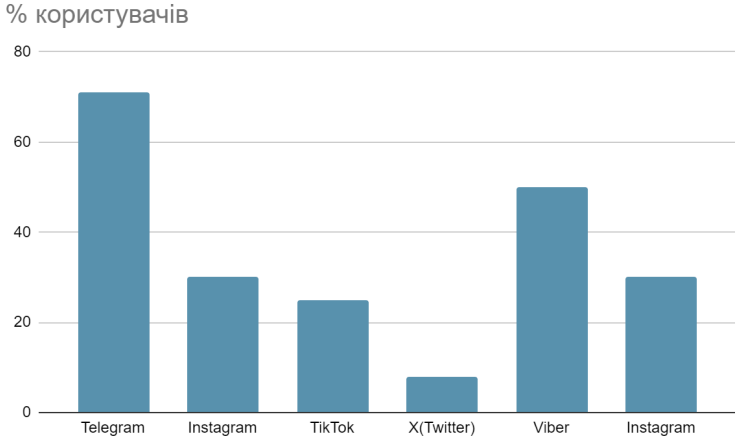

Рис. 2.1. Популярність соціальних мереж в Україні

Стрімкий ріст використання соціальних мереж та месенджерів слугує полем для атак соціальними інженерами, як простих людей так і працівників організацій. Використання соціальних мереж для здійснення соціоінженерних кібератак можна розділити на 7 видів (рис. 2.2).

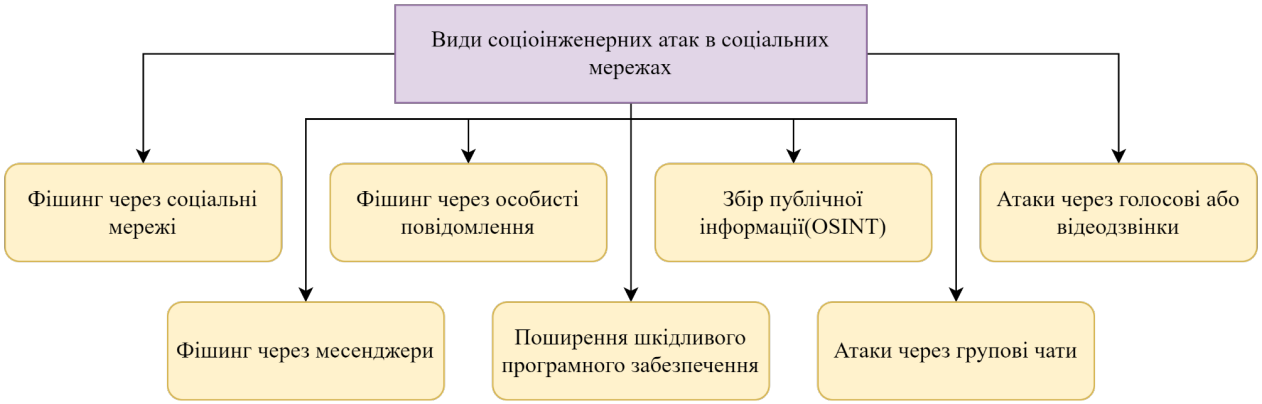

Рис. 2.2. Види соціоінженерних атак в соціальних мережах та месенджерах

Фішинг є однією з найпоширеніших технік соціальної інженерії, яка активно використовується у соціальних мережах. Зловмисники створюють підроблені сторінки або акаунти, що імітують відомі бренди або особистості, щоб обманом змусити користувачів надати свої облікові дані або іншу конфіденційну інформацію. Вони можуть надсилати повідомлення з посиланнями на фальшиві веб-сайт, де користувачі вводять свої облікові дані, думаючи, що вони знаходяться на легітимному ресурсі.

Соціальні інженери часто використовують особисті повідомлення для встановлення контакту з об’єктом впливу. Вони можуть прикидатися друзями, колегами або представниками офіційних установ, щоб завоювати довіру об'єкта атаки. Після встановлення контакту зловмисники можуть просити надати конфіденційну інформацію, як-от фінансові дані або паролі, або можуть направляти користувачів на шкідливі веб-сайти.

Соціальні мережі часто містять багато особистої інформації, яку користувачі викладають у публічний доступ. Соціальні інженери можуть використовувати цю інформацію для створення більш переконливих цілеспрямованих атак. Наприклад, знаючи дати народження, імена членів

родини або місця роботи, зловмисники можуть створювати більш достовірні сценарії атаки, які важче розпізнати як шахрайські.

Як і у випадку з соціальними мережами, месенджери також часто використовуються для фішингових атак. Зловмисники можуть надсилати повідомлення зі шкідливими посиланнями або вкладенням, які заражають пристрій об'єкта впливу або перенаправляють її на фальшиві сайти для збору облікових даних.

Соціальні інженери можуть використовувати голосові та відеодзвінки для більш прямого впливу на об’єкт атаки. Прикидаючись представниками офіційних установ або знайомими, вони можуть викликати відчуття терміновості або довіри, змушуючи об’єкт атаки надати конфіденційну інформацію або здійснити певні дії.

Месенджери також можуть бути використані для поширення шкідливого програмного забезпечення. Зловмисники надсилають файли або посилання, що містять шкідливе програмне забезпечення, які після відкриття заражають пристрій об’єкту атаки, надаючи зловмисникам доступ до його особистих даних або контролю над пристроєм.

Групові чати у месенджерах можуть стати майданчиком для соціальної інженерії. Зловмисники можуть приєднуватися до груп під фальшивими акаунтами, встановлювати довірчі відносини з учасниками і поступово отримувати доступ до конфіденційної інформації або переконувати інших учасників виконувати певні дії, наприклад, переходити за шкідливими посиланнями.

Особливу увагу слід звернути на LinkedIn: чимала кількість публічної інформації в профілях користувачів, як особиста, так і професійна, значно спрощує проведення атак, основою яких є соціальна інженерія. Відвідавши тільки профіль на вище вказаному сайті, за кілька хвилин можна дізнатися дату народження, місце навчання та, щонайважливіше, місце роботи та посаду. Також LinkedIn активно використовується для створення профілів для компаній, що значно спрощує пошуки та вибір об'єкта атаки.

Соціальні інженери добилися чималого успіху у проведенні реальних кібератак, використовуючи соціальні мережі та месенджери, і можна навести такий приклад подібної атаки. У липні 2020 року хакери здійснили атаку на соціальну мережу Twitter, отримавши доступ до облікових записів відомих особистостей, політиків, бізнесменів та компаній, таких як Барак Обама, Ілон Маск, Джефф Безос, Uber, Apple тощо. Від їх імені були розміщені хибні повідомлення про нібито роздачу біткоїнів у подвійному розмірі для тих, хто надішле свої біткоїни на певні гаманці [15].

Як виявилось, хакери не використовували жодних складних технічних прийомів чи вразливостей програмного забезпечення. Натомість, вони застосували класичну фішингову атаку: зловмисники здійснили телефонні дзвінки співробітникам Twitter, видаючи себе за працівників компанії, та обманним шляхом отримали від них облікові дані для входу в адміністративну панель управління соціальної мережі.

Хакерам вдалося отримати контроль над 130 акаунтами Twitter, з яких 45 були негайно заблоковані, проте, їм вдалося викрасти персональні дані деяких користувачів. Крім того, від імені скомпрометованих облікових записів були розміщені фішингові твіти, внаслідок чого зловмисники змогли виманити близько 13 біткоїнів (майже $118 000 за тодішнім курсом).

Ключовою вразливістю виявився людський фактор – недостатня обізнаність та підготовка співробітників у питаннях кібербезпеки, зокрема, соціальної інженерії, а також відсутність належних процедур верифікації запитів на доступ до адміністративних панелей від персоналу. Водночас варто відзначити, що успіх атаки базувався на високому рівні довіри до Twitter як авторитетного джерела інформації.

Цей випадок ілюструє кілька ключових тенденцій у сфері соціальної інженерії:

- посилене використання традиційних методів, таких як фішинг, шахрайські телефонні дзвінки та підроблення особистості;

- експлуатація високого рівня довіри користувачів до популярних інтернет-платформ та відомих персон;
- нехтування елементарними правилами кібергігієни персоналом навіть у великих організаціях;
- цілеспрямована атака на найбільш резонансні та впливові акаунти для максимізації шкоди.

Атака на Twitter продемонструвала високу актуальність загроз від соціальної інженерії навіть для передових IT-компаній. Приклад такої атаки показаний на рис. 2.3. Існує нагальна необхідність у розробці комплексних заходів захисту, включаючи технологічні рішення (багаторівнева автентифікація, шифрування, моніторинг аномалій), організаційні процедури (принцип мінімальних привілеїв, жорсткі вимоги до взаємодії з клієнтами) та, що найголовніше, підвищення обізнаності персоналу щодо соціальної інженерії шляхом навчання та тренінгів.

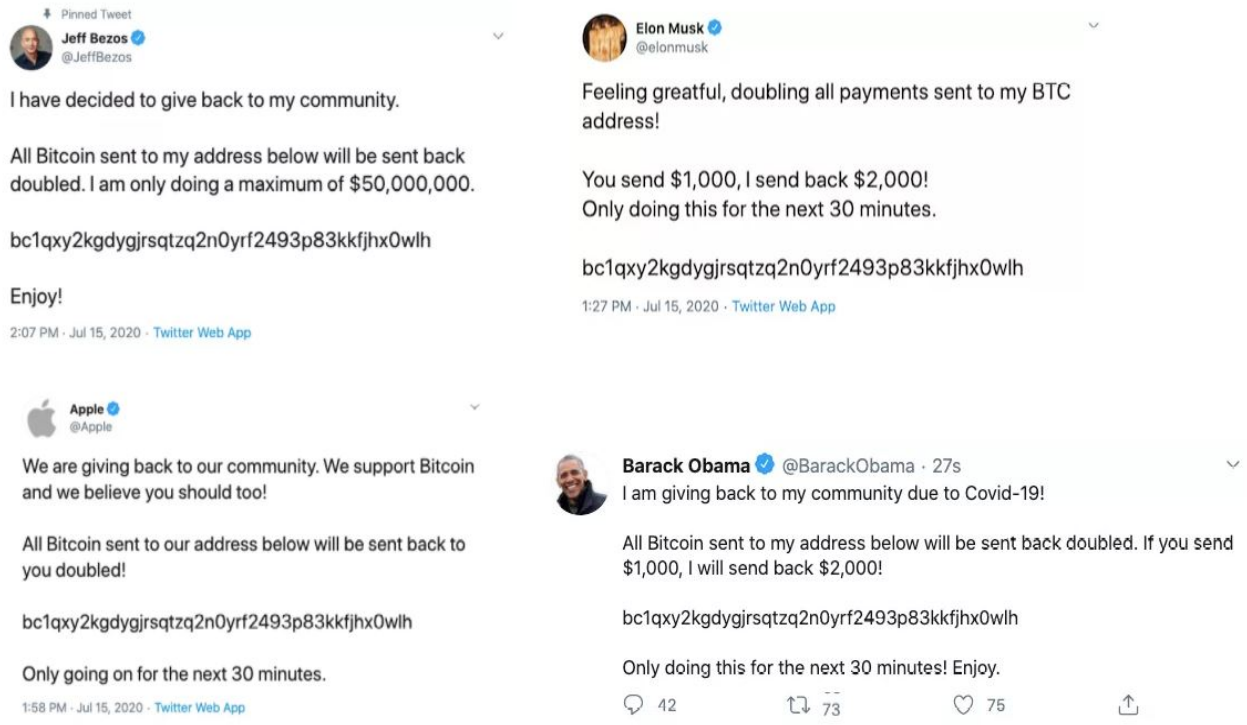

Рис 2.3. Приклад соціальної інженерії в соціальній мережі X (Twitter) [16]

2.2 Використання штучного інтелекту в соціальній інженерії

Штучний інтелект (ШІ) – це імітація процесів людського інтелекту машинами, особливо комп'ютерними системами. Конкретні застосування ШІ включають експертні системи, обробку природної мови, розпізнавання мови та машинний зір [17].

ШІ стає все більш впливовою технологією у різних галузях, включаючи кібербезпеку. Його здатність аналізувати великі обсяги даних, виявляти патерни та передбачати можливі загрози робить його потужним інструментом для захисту інформаційних систем.

Для здійснення кібератак, основою яких є соціальна інженерія, можуть використовуватися різні технології ШІ, що виконують безліч функцій та автоматизують весь процес за зловмисника. На рис. 2.4 зображено, які алгоритми ШІ підходять для яких соціоінженерних атак.

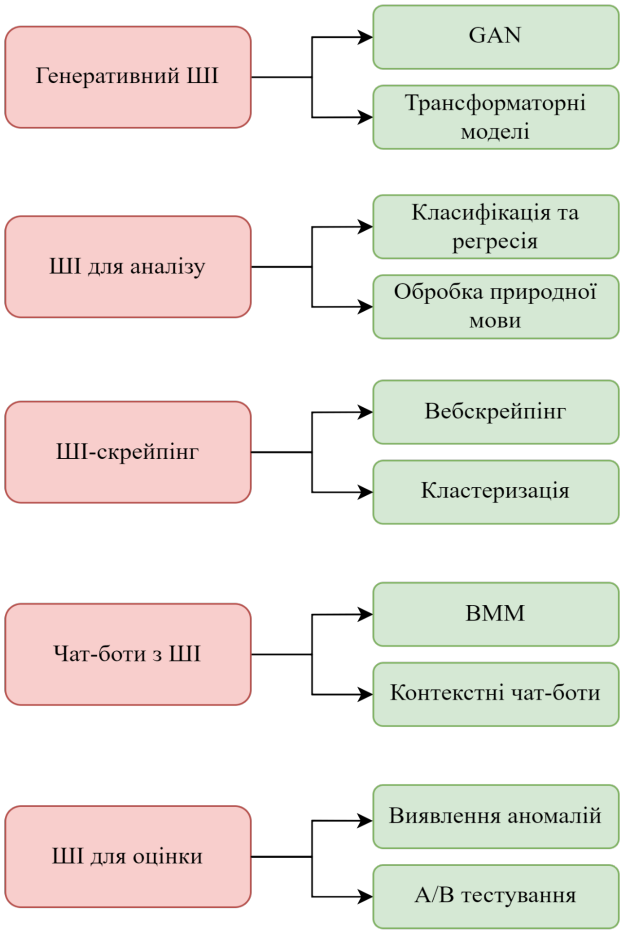

Рис. 2.4. Відповідність завдань та алгоритмів або методів ШІ

Генеративний ШІ включає алгоритми, які можуть генерувати контент, наприклад, текст, зображення або відео, на основі шаблонів, вивчених з наявних даних. В атаках соціальної інженерії генеративний ШІ може створювати реалістичні та переконливі вектори атаки, наприклад, фішингові електронні листи, імітуючи стилі та контекст людського спілкування. Для цієї задачі використовуються GAN, трансформаторні моделі.

ШІ-аналіз – це застосування методів машинного навчання та аналізу даних для обробки та інтерпретації даних. В атаках соціальної інженерії ШІ-аналіз може ідентифікувати потенційні цілі, оцінювати їхні вразливості та прогнозувати їхню поведінку на основі закономірностей у зібраній інформації. Для цієї задачі використовуються класифікація та регресія, обробка природної мови (NLP).

ШІ-скрейпінг передбачає використання автоматизованих інструментів, часто керованих машинним навчанням, для збору інформації з різних онлайн-джерел. У соціальній інженерії ШІ-скрейпінг може швидко збирати дані з профілів у соціальних мережах, публічних баз даних та інших джерел, щоб створювати детальні профілі цілей. Для цієї задачі використовуються бібліотеки веб-скрейпінг, інтелектуальний аналіз даних, методи кластеризації.

ШІ-автоматизація за допомогою ШІ – це використання систем, керованих ШІ, для автоматизації різних завдань і процесів. У соціальній інженерії автоматизація ШІ може ініціювати та підтримувати комунікацію з цілями, забезпечуючи послідовну взаємодію та знижуючи ризик виявлення. Для цієї задачі використовуються системи на основі правил, автоматизація процесів, управління документообігом.

Чат-боти з ШІ – це комп'ютерні програми, які можуть імітувати людську розмову. Під час атак соціальної інженерії чат-боти зі ШІ можуть вступати з об’єктами атаки в діалоги, щоб побудувати довіру, збирати інформацію та маніпулювати емоціями, імітуючи при цьому людську взаємодію. Для цієї задачі використовуються BMM, фреймворки контекстних чат-ботів, моделі “від послідовності до послідовності”.

Координація ШІ передбачає організацію завдань і взаємодії між різними агентами або компонентами ШІ. У соціальній інженерії координація ШІ може забезпечити плавні переходи між різними фазами атаки та підтримувати безперервність, навіть якщо зловмисники змінюються. Для цієї задачі використовуються мультиагентні системи, алгоритми координації, методи розподілу завдань.

ШІ для оцінки передбачає використання алгоритмів для відстеження, аналізу та оцінки успішності атаки. У соціальній інженерії ШІ для оцінки може відстежувати результати, такі як скомпрометовані акаунти або витік даних, щоб визначити ефективність атаки та вдосконалити майбутні стратегії. Для цієї задачі використовуються показники ефективності, виявлення аномалій, A/B тестування.

ШІ здатен автоматизувати процеси збору інформації про потенційні об’єкти впливу, аналізувати великі обсяги даних для виявлення вразливостей та створювати переконливіші обманні сценарії. ШІ дозволяє їм проводити атаки з більшою точністю та ефективністю.

Поява і широке впровадження передових мовних моделей, таких як ChatGPT, відкрили нову еру потенційних загроз кібербезпеці. За даними аналітичної компанії SlashNext Threat Labs, з моменту запуску ChatGPT наприкінці 2022 року кількість зловмисних фішингових листів зросла на 1265% [18]. Ця тривожна статистика підкреслює зростаюче занепокоєння тим, що зловмисники використовують можливості великих мовних моделей (ВММ) для створення більш витончених і переконливих атак соціальної інженерії [19].

Фішинг, практика обману людей з метою розкриття конфіденційної інформації або виконання шкідливих дій, вже давно є поширеною проблемою кібербезпеки. Однак інтеграція ШІ в екосистему фішингу вивела ці атаки на новий рівень витонченості та правдоподібності. Завдяки своїй здатності генерувати текст, схожий на людський, і розуміти контекст, ВММ можуть використовуватися зловмисниками для створення дуже переконливих і

персоналізованих фішингових електронних листів, що ускладнює для одержувачів можливість відрізнити легітимні повідомлення від шкідливих.

ШІ зробив великий внесок у полегшення використання фішингу для здійснення кібератак. Фішинг зазвичай відбувається, коли шахрай видає себе за компанію або приватну особу і намагається отримати персональну інформацію, таку як паролі, дані кредитних карток і фізичні адреси.

Користувачі можуть вміло протистояти певним видам фішингу, але більш витончені зловмисники можуть використовувати ШІ та інші інструменти, описані далі в розділі, що може швидко перевантажити команду.

Шахраї можуть спробувати отримати доступ до цієї конфіденційної інформації через відкрите текстове поле, наприклад, у приватних повідомленнях або публічних повідомленнях на дошці оголошень.

Повідомлення пишеться таким чином, щоб обманом змусити користувача перейти за шкідливим посиланням або відкрити шкідливе програмне забезпечення, яке викраде його персональні дані. Кіберзлочинець може також продати інформацію цієї особи в Інтернеті іншим шахраям або використати її для створення фальшивої особи.

Фішинг націлений не лише на клієнтів, але й на співробітників організації. Це називається компрометацією ділової електронної пошти, коли шахрай видає себе за керівника і націлює фішинг-атаки на співробітників компанії. Зазвичай вони шукають корпоративну інформацію (наприклад, доступ до інтрамережі або зовнішньої мережі компанії) або доступ до корпоративних банківських рахунків.

Раніше ознаками того, що повідомлення є фішинг-шахрайством, було використання типового привітання, незвичне форматування та/або безліч орфографічних і граматичних помилок у тексті. Все це часто поєднується з терміновим запитом, нібито від вищого керівництва компанії, як правило, від людини, чиї прохання виконуються без жодної перевірки.

Але технологія ШІ уможливлює більш витончені спроби фішингу, з якими команда може бути не навчена справлятися. Завдяки ШІ шахраї можуть

спілкуватися більш чітко, масштабувати свої атаки і надсилати повідомлення, які виглядають легітимними.

Як уже згадувалося вище, погана граматика, орфографічні помилки і навіть любовна лексика вже давно вважаються ознаками фішингу. За допомогою ШІ-фішингу зловмисники можуть використовувати ВММ, щоб усунути ці особливості та звучати як носій мови, заманюючи об'єкти впливу оманливим відчуттям безпеки.

Багато програм для виявлення шахрайства покладаються на виявлення ключових слів або фільтрацію точних текстових рядків/фраз, але ця тактика більше не застосовується, коли копія позбавлена традиційних тестів.

Шахраї також можуть використовувати генеративний ШІ для сканування платформ соціальних мереж та інтернету в пошуках користувацького контенту та іншої публічної інформації. Результатом є персоналізовані фішингові електронні листи, які важко відрізнити від справжньої кореспонденції.

Шахраї знають, що їм потрібно масово розсилати фішингові повідомлення, щоб знайти об'єкт впливу. Раніше на створення різних повідомлень з різними цілями йшли години або дні. Тепер, завдяки ШІ, це займає лічені хвилини. Маючи доступ до ВММ, шахраї можуть просканувати сотні соціальних акаунтів, створити реалістичне повідомлення, а потім масово контактувати з користувачами. Вони також можуть використовувати ботів зі ШІ для дослідження та аналізу тисяч пристроїв, що дозволяє їм використовувати величезні обсяги даних для створення реалістичних повідомлень. Для фішингу також можуть використовуватися інструменти ШІ для написання нових рядків коду і реалізації більш складних афер, які раніше вимагали набагато більше роботи.

Створення реалістичних аудіо та відео підробок, відомих як діпфейки (рис. 2.5), стало можливим завдяки досягненням у галузі глибинного навчання та ШІ. Ключову роль відіграють два типи новітніх алгоритмів: генеративні змагальні мережі (GAN) та моделі трансформерів.

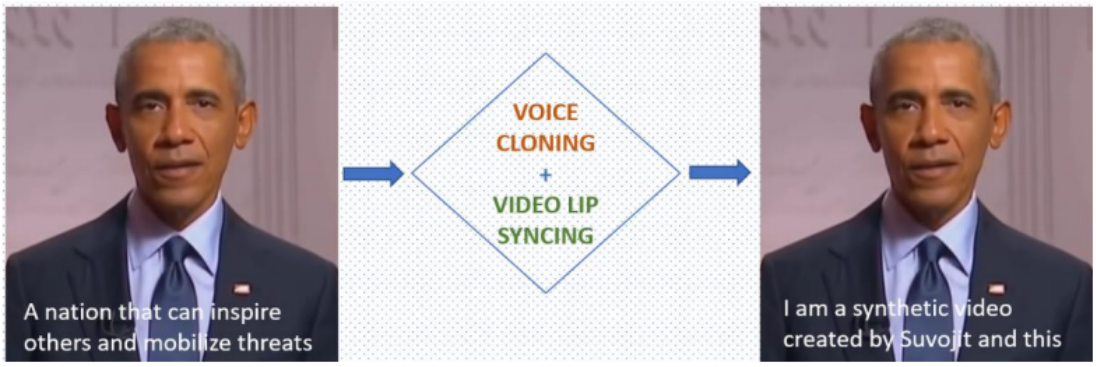

Рис. 2.5. Діпфейк Барака Обами [20]

GAN складаються з двох нейронних мереж, які навчаються одна проти одної в ітераційному процесі, коротке зображення дії яких відображено на рис. 2.6. Генеративна мережа намагається створювати переконливі підроблені зразки (зображення, аудіо чи відео), тоді як дискримінаційна мережа намагається відрізнити ці фейки від справжніх даних. У процесі навчання обидві мережі постійно вдосконалюються, що врешті-решт дозволяє генератору створювати високоякісні підробки.

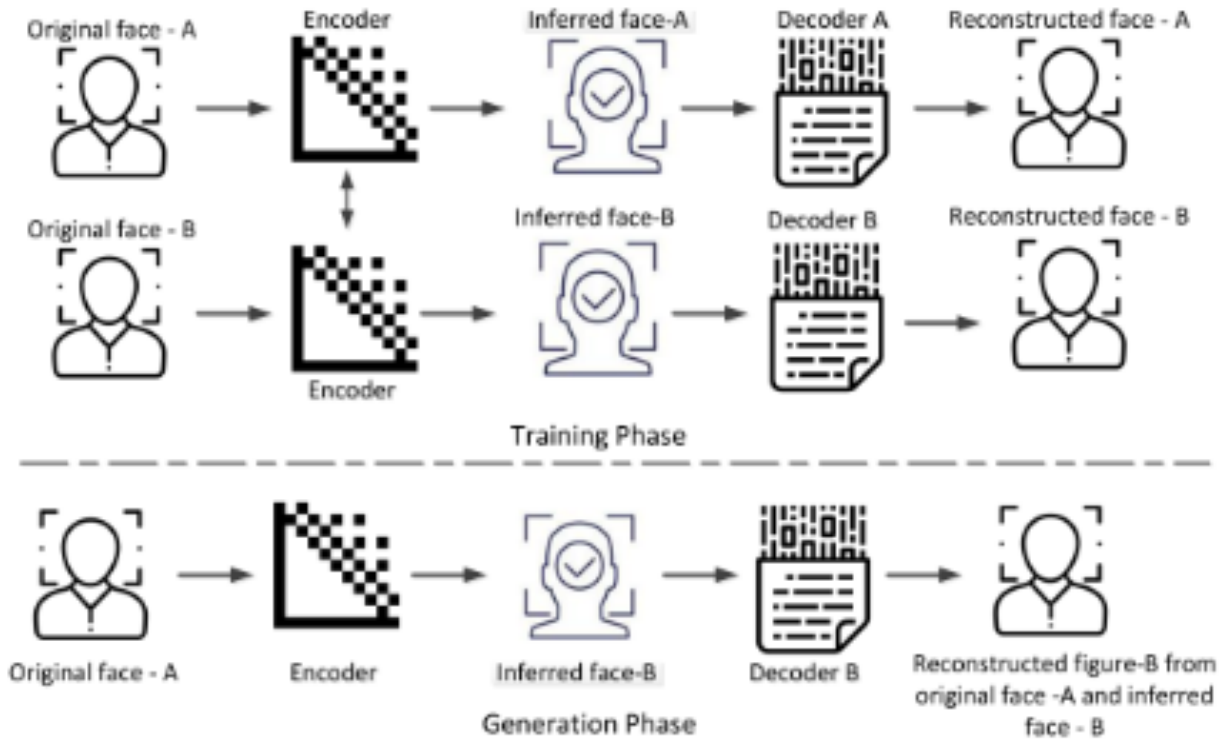

Рис. 2.6. Процес навчання та генерації діпфейків [21]

GAN широко використовуються для створення діпфейків, здатних імітувати зовнішність, міміку, артикуляцію та рухи губ людини на відео. Найновіші моделі GAN можуть навіть генерувати фотореалістичні зображення облич, збираючи риси з багатьох вихідних зображень.

Моделі, такі як BERT, GPT та спеціалізовані мережі для голосового синтезу, використовуються для генерації аудіодіпфейків. Ці потужні мовні моделі навчаються на великих наборах аудіо- та текстових даних і можуть імітувати манеру мовлення, тон, акцент і тембр голосу будь-якої особи з надзвичайною вірогідністю.

Для ефективного тренування моделей ШІ потрібні великі обсяги вихідних даних певної особи. Для відеодіпфейків це можуть бути зображення обличчя під різними кутами, світлом та з різними виразами. Для аудіо – зразки голосу людини в різних ситуаціях. Зловмисники часто збирають такі дані з публічних джерел: соцмереж, YouTube, телеінтерв'ю тощо.

Зловмисники можуть використовувати діпфейки у фішингових кампаніях різними способами, застосовуючи вектори атак, спрямованих на обман користувачів і отримання несанкціонованого доступу до конфіденційних даних чи систем.

Зловмисники генерують аудіо чи відео діпфейк, що імітує представника вищого керівництва, співробітника певного відділу чи іншу довірену особу. Це дозволяє переконливо видавати себе за авторитетне джерело і вимагати від об'єкта впливу виконання певних дій, передачі паролів, облікових даних чи іншої інформації.

За допомогою діпфейків генеруються фальшиві записи нарад, відеоконференцій чи телефонних розмов, де учасники нібито обговорюють конфіденційну інформацію чи приймають певні рішення. Такі підробки можуть використовуватися для соціальної інженерії, шантажу чи корпоративного шпигунства.

Шахраї можуть видавати себе за клієнтів, постачальників чи ділових партнерів організації, використовуючи діпфейки їхніх голосів чи зображень. Це

дозволяє отримувати доступ до внутрішніх систем, фінансових рахунків або впливати на бізнес-процеси.

Вішинг (від слів фішинг та voice (голос)) – це будь-яка кібератака з використанням телефону або голосових повідомлень. У більшості випадків мета зловмисника – переконати об’єкт впливу в тому, що він є авторитетною особою, наприклад, начальником або співробітником банку. Оскільки це різновид фішингу, для успіху афери потрібен високий рівень соціальної інженерії. Наприклад, люди навряд чи піддадуться на ці атаки, якщо вішинг-атака не намагається представити банк, з яким вони ведуть бізнес.

Але зібрати достатньо інформації про об’єкт впливу це лише початок. З появою нових технологій ШІ хакери почали використовувати технологію діпфейків для здійснення своїх вішинг-атак.

Найбільшому ризику піддаються фінансова сфера, виробництво, медицина, роздрібна торгівля та е-комерція. Адже доступ до даних цих галузей може приносити злочинцям величезні прибутки. Організації змушені суворо контролювати всі аспекти кібербезпеки, аби не стати об’єктами атак новітніх шахрайських схем.

Для реалізації вішинг-атак вже існує чимало загальнодоступних сервісів, вартість місячної підписки на які не перевищує кілька десятків доларів, що робить їх доступними кожному. Одним з таких прикладів є Elevenlabs.

ElevenLabs – це стартап у сфері ШІ, який пропонує послугу клонування голосу, що дозволяє підписникам генерувати майже ідентичні голоси за допомогою ШІ на основі завантажених аудіозразків тривалістю кілька хвилин. Не дивно, що як тільки функція була випущена в бета-версії, її одразу ж почали використовувати, щоб видавати себе за знаменитостей, іноді навіть без їхнього попереднього відома та згоди. Хоча Elevenlabs та подібні сервіси були розроблені для законних цілей, таких як озвучення відео, аудіокниг чи віртуальних помічників, вони також можуть бути використані зловмисниками з метою вішингу [22].

У контексті вішингових атак, зловмисники можуть зібрати невелику кількість аудіозразків голосу об'єкта атаки з публічно доступних джерел, таких як інтерв'ю, виступи чи соціальні мережі. Ці дані можуть бути використані для створення переконливого клона голосу за допомогою сервісів, подібних до Elevenlabs. Згенерований синтетичний голос може бути використаний для створення фейкових аудіозаписів, в яких нібито авторитетна особа надає інструкції чи вимагає конфіденційної інформації.

Реалістичність таких підроблених аудіозаписів робить їх потенційно ефективним інструментом для соціальної інженерії та маніпуляції. Об’єкти атаки, почувши знайомий голос і не маючи змоги відрізнити справжній запис від підробки, можуть бути введені в оману та виконати шкідливі дії, такі як розголошення паролів, передача конфіденційних документів чи здійснення фінансових операцій.

Крім того, сервіси генерації синтетичного мовлення можуть бути використані у поєднанні з технологіями створення відеодіпфейків, що підсилює переконливість та ефективність вішингових атак. Об'єднання штучно згенерованого аудіо та відео створює надзвичайно реалістичну імітацію справжньої людини, що значно ускладнює виявлення підробки.

Вплив генерації контенту та діпфейків на стан кібербезпеки росте. У березні 2019 року сталося серйозне порушення безпеки, коли генеральний директор британської енергетичної фірми став об’єктом атаки складного підробленого аудіо шахрайства [23]. Виконавчий директор був обманутий телефонним дзвінком, який бездоганно видавав голос генерального директора фірми, виконавчого директора німецької материнської корпорації компанії, і помилково перерахував близько 200 000 фунтів стерлінгів на рахунок угорського банку. Він миттєво передав платіж на рахунок угорського постачальника, вважаючи, що це законний запит його керівника, не знаючи, що це шахрайська афера, вчинена особою, яка використовує технологію мовлення ШІ, щоб імітувати голос генерального директора.

Під час складної кампанії з шахрайства генерального директора в грудні 2021 року французька організація зазнала збитків у розмірі 38 мільйонів доларів протягом декількох днів [24]. Зловмисник, видаючи себе за генерального директора, виконав схему соціальної інженерії, терміново попросивши бухгалтера компанії передати 300 тисяч доларів банку в Угорщині. Шахрайство спочатку залишилося непоміченим, що призвело до розслідування, яке виявило не тільки озвучення, але й неодноразові напади на забудовника, що призвело до передачі 38 мільйонів доларів. Пізніше вісім підозрюваних були заарештовані. Аналогічно, в 2020 глибокому підробленому шахрайстві генерального директора проти японської компанії шахраї видавали себе за директора по телефону, направляючи переказ на суму 35 мільйонів доларів для передбачуваного придбання [25]. Попри більш пізнє розслідування, гроші були втрачені через використання технології підробки голосу для імітації голосу режисера.

Окрім впливу генеративного контенту та діпфейків в тому числі на фінансовий стан організацій, атаки з використанням чужих голосів значно впливають на політичні процеси навіть в найрозвиненіших країнах. До прикладу, ряд американців отримали дзвінки від президента Америки Джо Байдена, який просив їх не голосувати на майбутніх виборах. Дослідники зійшлися на тому, що шахраї використовували для своїх цілей Elevenlabs[26].

Виявлення діпфейків розглядається насамперед як проблема бінарної класифікації, мета якої – відрізнити автентичні відео від маніпуляцій з ними. Цей процес значною мірою спирається на великі бази даних як справжніх, так і фальшивих відео для навчання моделей класифікації. Незважаючи на зростаючу доступність фальшивих відео, їхня кількість все ще недостатня для створення всеосяжного еталона для перевірки різних методик виявлення. Відео, отримані з бази даних VidTIMIT, демонструють реалістичні вирази обличчя, рухи рота і моргання очей, які є важливими для перевірки ефективності різних методів виявлення підробок.

Методи глибокого виявлення підробок можна умовно поділити на ті, що призначені для виявлення підроблених зображень, і ті, що спрямовані на

виявлення підроблених відео. Останні поділяються на методи, які зосереджуються на візуальних артефактах в окремих кадрах відео, і методи, які використовують часові характеристики в декількох кадрах. Методи, засновані на часових характеристиках, зазвичай використовують моделі рекурентної класифікації з глибоким навчанням, тоді як ті, що використовують візуальні артефакти в межах відеокадрів, можуть бути реалізовані за допомогою глибоких або поверхневих класифікаторів.

Методи на основі традиційних нейронних мереж (CNN) виділяють зображення обличчя з відеокадрів і використовують їх для навчання та прогнозування, щоб отримати результати на рівні зображення. Однак ці методи використовують лише просторову інформацію з окремих кадрів. На відміну від них, методи на основі регіональних звичайних нейронних мереж (RCNN) вимагають для навчання послідовності відеокадрів, що дозволяє їм отримувати результати на рівні відео. RCNN поєднує в собі CNN і рекурентні нейронні мережі (RNN), таким чином повністю використовуючи просторову і часову інформацію в глибоко підроблених відео. Цей подвійний підхід дає змогу проводити всебічний аналіз відеоданих, що є надзвичайно важливим з огляду на складну природу діпфейків.

Нинішні методи виявлення підробок мають низку недоліків. Наприклад, методи, засновані на машинах опорних векторів (SVM) і метриках якості зображення, часто дають високий рівень помилок, коли їх застосовують до нових високоякісних наборів даних для діпфейків. Крім того, фотографії облич, оброблені за допомогою передових методів глибокого навчання, таких як CNN, GAN, SVM, випадковий ліс і багатошаровий персептрон, стає дедалі важче відрізнити від справжніх зображень. Це значною мірою пов'язано зі здатністю GAN генерувати високоякісні зображення, які точно імітують розподіл вхідних даних. Крім того, через значну втрату даних кадру після аудіовізуального стиснення, багато методів глибокого розпізнавання підробок на основі зображень не підходять для відео.

2.3 Аналіз життєвого циклу кібератаки з елементами соціальної інженерії

Стандартний життєвий цикл кібератаки з елементами соціальної інженерії не відрізняється від життєвого циклу звичайних атак і його спрощена версія містить 4 етапи: розслідування, гачок, виконання, вихід [27]. Втім, слід розглянути цикл дещо детальніше, щоб мати змогу побачити можливості для зменшення ризиків на кожному етапі.

Перший блок життєвого циклу – розвідка або розслідування. Головна мета цього блоку – ідентифікувати ціль – підібрати об’єкт впливу, людський чинник якого можна використати для отримання вигоди та проведення соціоінженерної атаки. Для ідентифікації цілі в більшості випадків використовуються соціальні мережі та ШІ. Зловмисники збирають відкриті дані у соціальних мережах, це називається OSINT (Open Source Intelligence). Проводиться моніторинг публікацій, коментарів та іншої активності для отримання особистої інформації, уподобань, зв’язків та іншої інформації. Крім популярних Facebook, Instagram, Telegram та інших використовується орієнтована на нетворкінг соціальна мережа LinkedIn, що дозволяє дізнатися про професійні зв’язки, посади, історію роботи та навички співробітників, а також визначити ключових осіб в організації. Для полегшення та прискорення цього етапу атаки, зловмисниками використовуються техніки скрейпінгу та парсингу, що дозволяє швидко зібрати великий обсяг даних із загальнодоступних ресурсів. Все частіше на себе цю функцію беруть автоматизовані боти на базі ШІ та алгоритмів ML.

Другий етап – розробка ресурсів, яка включає в себе створення, покупку або компрометацію/крадіжку ресурсів, які можуть бути використані для проведення атаки. Такі ресурси включають інфраструктуру, облікові записи в соціальних мережах та інше. Також даний етап може включати в себе розробку або придбання програмного забезпечення на базі ШІ, яке здатне генерувати правдоподібний контент, якщо соціальний інженер йде шляхом видавання себе за іншу особу. Якщо для проведення кібератаки планується реалізація

фішингової атаки, то можуть розроблятися або використовуватися ВММ, що здатні генерувати гіперперсоналізовані повідомлення на основі даних, що були отриманні в ході попереднього етапу – розвідки.

Третій етап – початковий доступ. На цьому етапі зловмисник отримує доступ до мережі, в яку була ціль проникнути. Цей етап передбачає фішинг, компрометацію, експлуатацію публічних застосунків, встановлення довірчих відносин або отримання доступу до дійсних облікових записів.

Четвертий етап – виконання атаки. На цьому кроці проведення соціальні інженери вводять шкідливе програмне забезпечення в мережу організації, що може використовуватися для низки цілей: викрадення інформації, знищення інформації, створення збоїв в роботі інфраструктури або отримання віддаленого доступу до робочих місць працівників.

П’ятий етап – закріплення. Основною метою цього етапу є закріплення зловмисників у мережі організації. Для цього вони можуть використовувати маніпуляції з вже існуючими обліковими засобами (зміна паролів та налаштувань), створювати нові облікові засоби, впроваджувати скрипти для автоматичного запуску шкідливого програмного забезпечення при вході в систему або запуску операційної системи та створювати заплановані завдання, які будуть виконуватися на користь зловмисників з певною циклічністю.

Шостий етап – розширення привілеїв. Після того, як зловмисник вже втримався та закріпив своє перебування в мережі організації, він розширює “горизонти своїх можливостей”. Зловмисники можуть обійти механізми, призначені для контролю підвищення привілеїв, щоб отримати дозволи вищого рівня. Більшість сучасних систем містять вбудовані механізми контролю рівня привілеїв, які призначені для обмеження привілеїв, які користувач може виконувати на комп'ютері. Для виконання завдань, які можна вважати ризикованими, повноваження мають бути надані конкретним користувачам. Зловмисник може використовувати вбудовані механізми контролю для підвищення рівня привілеїв у системі.

Сьомий етап – уникнення виявлення. Зловмисникам важливо уникнути виявлення та залишатися у системі якомога довше. Для цього вони змінюють налаштування системи та її програмного забезпечення. Наприклад, можуть навіть видалятися програмне забезпечення, призначене для захисту операційної системи або приховування/шифрування даних.

Восьмий етап – збір. Зловмисник на цьому етапі збирає дані, що становлять інтерес для його мети. Збір складається з методів, які зловмисник може використовувати для збору інформації, і джерел, з яких збирається інформація. Наступною метою після збору даних є їх викрадення (витік). Джерелами є різні типи накопичувачів, браузери, аудіо-, відео- та електронна пошта. Тут значно підвищити швидкість дозволяє ШІ. Автоматизовані боти для збору інформації на базі ШІ здатні за дуже малий проміжок часу зібрати багато інформації, та за потреби виділяти тільки найважливіше, що може принести найбільше користі зловмиснику.

Дев’ятий етап – витік інформації. На цьому етапі зловмисник намагається викрасти дані. Зібравши дані, зловмисники часто проводять певні маніпуляції над ними, щоб уникнути виявлення під час видалення, наприклад, стиснення та шифрування. Методи вилучення даних з цільової мережі зазвичай включають передачу їх через свій канал управління або альтернативний канал, а також можуть включати обмеження на розмір переданих даних.

Десятий етап – вплив. Даний етап повністю залежить від мети зловмисника, яку він визначив перед атакою. Зазвичай метою може бути знищення, фальсифікація або використання даних у власних цілях.

Вплив нових методів соціальної інженерії на проведення кібератак важко недооцінити. Відтепер використання соціальних мереж та ШІ дозволяють швидко, легко та масовано впливати на об’єкт атаки, використовуючи дані, які вона сама залишає в публічних джерелах. Генеративний ШІ, використовуючи цю сучасну вразливість створює тексти, відео або аудіо, що здатне вплинути на об’єкт атаки та збільшити шанси успішної соціоінженерної атаки, в ході якої буде порушена інформаційна цілісність організації, що може призвести до

значних витрат на пом’якшення завданого збитку та покращення системи кібербезпеки в майбутньому.

Висновки до розділу 2

Дослідження, представлене у другому розділі, забезпечило всебічне вивчення нових методів соціальної інженерії, які використовують різні цифрові платформи та технології. Оскільки цифровий ландшафт продовжує стрімко розвиватися, зловмисники адаптували свої стратегії, щоб використовувати нові можливості для атак соціальної інженерії, створюючи значні виклики для кібербезпеки організацій.

Однією з ключових сфер, що розглядаються в розділі, є використання соціальних мереж для цілей соціальної інженерії. Було приділено увагу таким видам соціоінженерних атак, як фішинг через соціальні мережі, фішинг через месенджери, збір публічної інформації, фішинг через особисті повідомлення, атаки через голосові або відеодзвінки, атаки через групові чати, поширення шкідливого програмного забезпечення через соціальні мережі та месенджери.

Крім того, було досліджено життєвий цикл соціоінженерних атак, який включає в себе 10 етапів, серед яких: розвідка, розробка ресурсів, початковий доступ, виконання атаки, закріплення, розширення привілеїв, уникнення виявлення, збір, витік інформації, вплив.

На додаток до використання цифрових платформ, у розділі розглядається нова загроза використання ШІ в цілях соціальної інженерії, а саме генеративного ШІ, ШІ-аналізу, ШІ-скрейпінгу, чат-ботів з ШІ, ШІ для оцінки. Оскільки технології ШІ стають все більш досконалими і доступними, зловмисники можуть використовувати їхні можливості для автоматизації та масштабування своїх кампаній соціальної інженерії. Від створення реалістичних фейкових медіа до розробки розмовних ШІ-агентів для цілей соціальної інженерії – потенційні наслідки атак з використанням ШІ викликають значне занепокоєння з точки зору організаційної безпеки.

Розділ 3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЙ ШЛЯХОМ ПРОТИДІЇ КІБЕРАТАКАМ З ЕЛЕМЕНТАМИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Для досягнення мети дослідження необхідно розробити рекомендації щодо підвищення інформаційної безпеки організацій шляхом протидії кібератакам з елементами соціальної інженерії. У цьому розділі досліджено методи захисту від таких атак, а також запропоновано підходи до навчання персоналу з метою мінімізації ризиків, пов'язаних з людським фактором.

3.1 Дослідження сучасних стратегій захисту IT-індустрії від витоку інформації

Як правило, витоки конфіденційної інформації призводять до втрат, незалежно від досліджуваної області. IT-індустрія не є винятком. Організації повинні робити все можливе, щоб мінімізувати ризик поширення інформації та можливі шкідливі наслідки. Історія про кіберзлочинців, які зламують і розповсюджують бази даних і вимагають грошей, більше не є дивною, але саме працівники допомагають конкурентам і клієнтам отримувати конфіденційну інформацію за певну плату або роблять це самі з причин, таких як звільнення. Тому організаціям необхідно не тільки захищати себе ззовні, а й контролювати внутрішні процеси.

Для цього робота менеджера в IT-секторі дуже складна, оскільки необхідно вміти керувати всіма процесами компанії. Тенденції постійно змінюються, і їх не можна залишати позаду, а оцифровка лише прискорить ці зміни. Але навіть висококваліфіковані менеджери мають проблеми на цьому шляху.

Поняттями "кіберзлочинність у вузькому розумінні" і "кіберзлочинність у широкому розумінні" можна назвати різні види злочинів.

- кіберзлочинність у вузькому розумінні ("комп'ютерна злочинність"): це незаконна дія, здійснена за допомогою електронних транзакцій, метою яких є захист комп'ютерних систем та захист інформації, яку вони здійснюють;
- кіберзлочинність у широкому розумінні ("злочин, пов'язаний з комп'ютером"): незаконні дії, вчинені комп'ютерною системою або мережею або у зв'язку з нею (включаючи такі злочини, як незаконне зберігання, надання або розповсюдження інформації через комп'ютерну систему або мережу) [28].

Існує 4 групи кіберзлочинців. До першої групи належать злочини проти конфіденційності, цілісності та доступності комп'ютерних даних та систем. Незаконний доступ, незаконне втручання, втручання в дані, втручання в системи, неправомірне використання пристроїв. До четвертої групи належать злочини, пов'язані з порушенням авторських і суміжних прав [29].

Згідно з результатами опитування Infosecurity Europe, проведеного за ініціативою Британського інституту стандартизації, 37% респондентів заявили, що, на їхню думку, внутрішні загрози становлять основну небезпеку для бізнесу роботодавця, а саме нечесну, а іноді й злочинну поведінку співробітників організації [30].

Існують такі типи інсайдерів, які сприяють витоку інформації: необережний інсайдер; маніпульований інсайдер; ображений інсайдер; нечесний інсайдер; фальшивий інсайдер; впроваджений інсайдер.

Зовсім недавно на ринку праці спостерігалася нестача висококваліфікованих IT-фахівців, і навіть великі компанії наймали новачків, і з кінця 2022 року почалися масові звільнення. Організаціям необхідно зосередитися на талантах і створити команди, здатні адаптуватися до непередбачених обставин, що виникають на ринку праці. Але незалежно від галузі, пошук відповідного таланту є безпрецедентним завданням [31].

Не варто недооцінювати важливість персоналу. Чим вища цінність працівника з правильними характеристиками, тим більша ймовірність досягнення цілей компанії. Часта зміна співробітників не призведе до того, що стан організації покращиться. Навпаки існує високий ризик витоку

конфіденційної інформації, збільшуються фінансові витрати на розвиток людських ресурсів і навчання, знижується ймовірність створення професійного персоналу, підвищується вразливість організації перед зовнішніми факторами, мінливі умови зростають, а кількість неякісних послуг зростає [32].

До цього часу національне законодавство та існуюча практика не розробили ефективних превентивних заходів щодо запобігання витокам інформації або способів захисту правовласників після розкриття інформації. Труднощі виникли вже на етапі визначення обсягу інформації, що підлягає захисту, і може виявитися неможливим довести факти незаконного поширення такої інформації в ході судових розглядів, а також чітко розрахувати і обґрунтувати суму збитків і упущеної вигоди. Однак, хоча немає чіткого способу уникнути цього, можна визначити деякі ефективні способи зменшення ризику.

Співробітники, розробники та постачальники зобов'язані підписувати угоди про конфіденційність конфіденційної інформації та угоди про відповідальність за витік інформації.

У деяких випадках організація надсилає новачкам підроблені фішингові електронні листи, щоб з'ясувати, чи хтось потрапив у таку пастку. Цей метод необхідний для безпеки організації, оскільки шахраї вже можуть надсилати справжні листи.

Впровадження нових програмних рішень, що дозволяють застосовувати політики безпеки і забезпечувати додатковий захист від втрати даних. Він може керувати програмами та пристроями, антивірусними рішеннями для мобільних пристроїв, програмними рішеннями для управління та захисту мобільних пристроїв, надавати доступ лише певним працівникам або шифрувати код та дані на знімних носіях.

Найбільші труднощі виникають через проблеми, викликані "людським" фактором. Найважливіші з них включають вразливості та помилки у встановленому програмному забезпеченні, а також випадкові порушення даних працівниками. Таким чином, основи безпеки та конфіденційності, дотримання правил і безперервного підвищення кваліфікації мають першорядне значення.

Спеціальна перевірка персоналу або документів, анкетування, інтерв'ю або тестування систем контролю також є важливим заходом для підтримки інформаційної безпеки. Проведення профілактичних IT-аудитів дозволяє систематизувати інформаційну структуру підприємства, виявити основні тенденції в розвитку, визначити, де можна знизити витрати на IT, а також захистити організацію від витоку інформації.

Важливим заходом забезпечення фізичної безпеки є захист приміщень, де зберігається обладнання, ресурси і носії даних, використання камер відеоспостереження і різних датчиків для виявлення зловмисників. Система кібербезпеки з декількох елементів, включаючи безпеку додатків, безпеку даних, безпеку критичної інфраструктури, мережеву та операційну безпеку, хмарну безпеку та планування аварійного відновлення. Може бути захищено все, що вразливе до злому, кібератак та несанкціонованого доступу, а саме комп'ютери, пристрої, мережі, сервери та програми. У той же час це стосується лише захисту даних, що існують у цифровій формі.

Програмні рішення мають вирішальне значення для захисту інформації від витоку. Класифікація даних за рівнями чутливості та впровадження систем моніторингу для відстеження руху даних є важливими заходами. Організації повинні забезпечити контроль, щоб лише уповноважені особи мали доступ до конфіденційних даних. Крім того, необхідно регулярно переглядати права доступу. Впровадження стратегій управління скріншотами робочого столу та обмежень на копіювання і вставку може ефективно запобігти як ненавмисному, так і навмисному порушенню даних через захоплення екрана або копіювання конфіденційної інформації. Рекомендується використовувати спеціалізоване програмне забезпечення для регулювання та обмеження цих функцій.

Однією із сучасних стратегій захисту від витоку інформації внаслідок дій працівників є аудити або тести на проникнення з елементами соціальної інженерії. План такого тестування для та варіанти застосовуваних технік соціальної інженерії для доступу до мережі організації зображено на рис. 3.1.

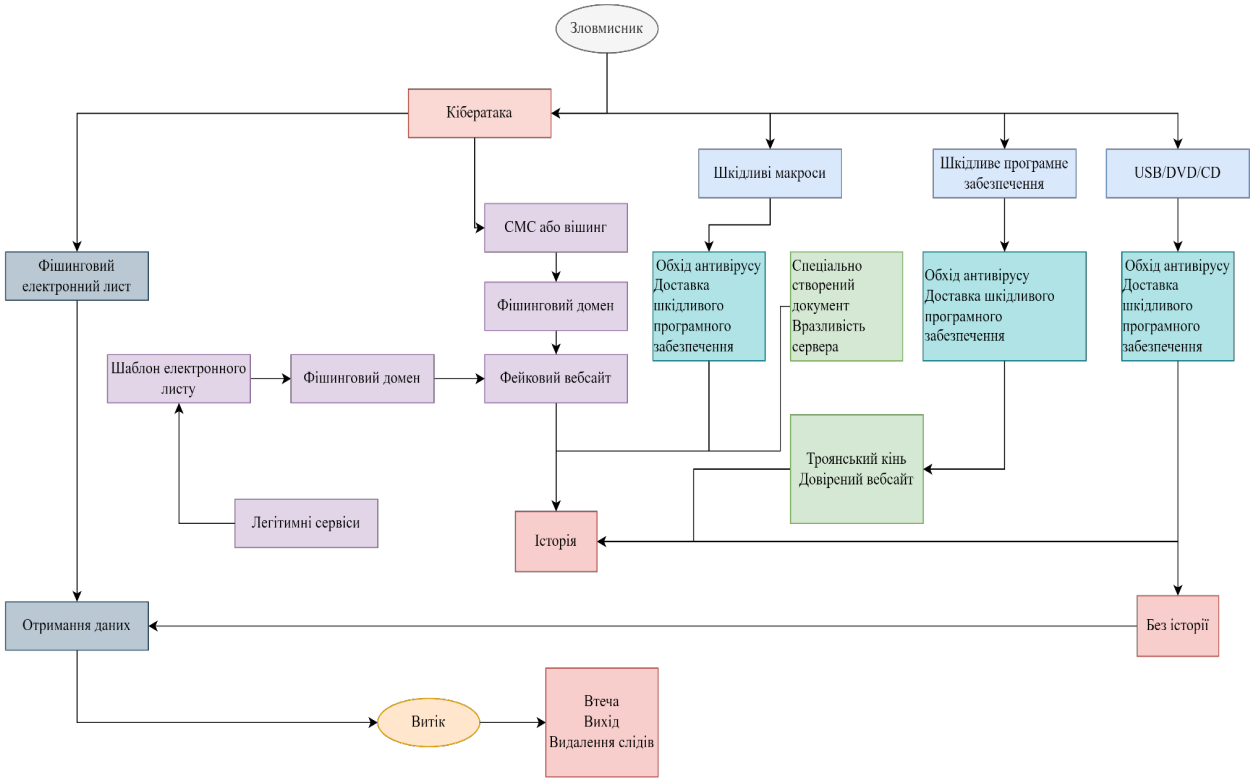

Рис. 3.1. Сценарій тестування з використанням соціальної інженерії

До того ж, тестування включає в себе перевірку можливості фізичного доступу на захищений об'єкт. Для цього пропонується застосовувати план фізичного вторгнення, зображений на рис. 3.2.

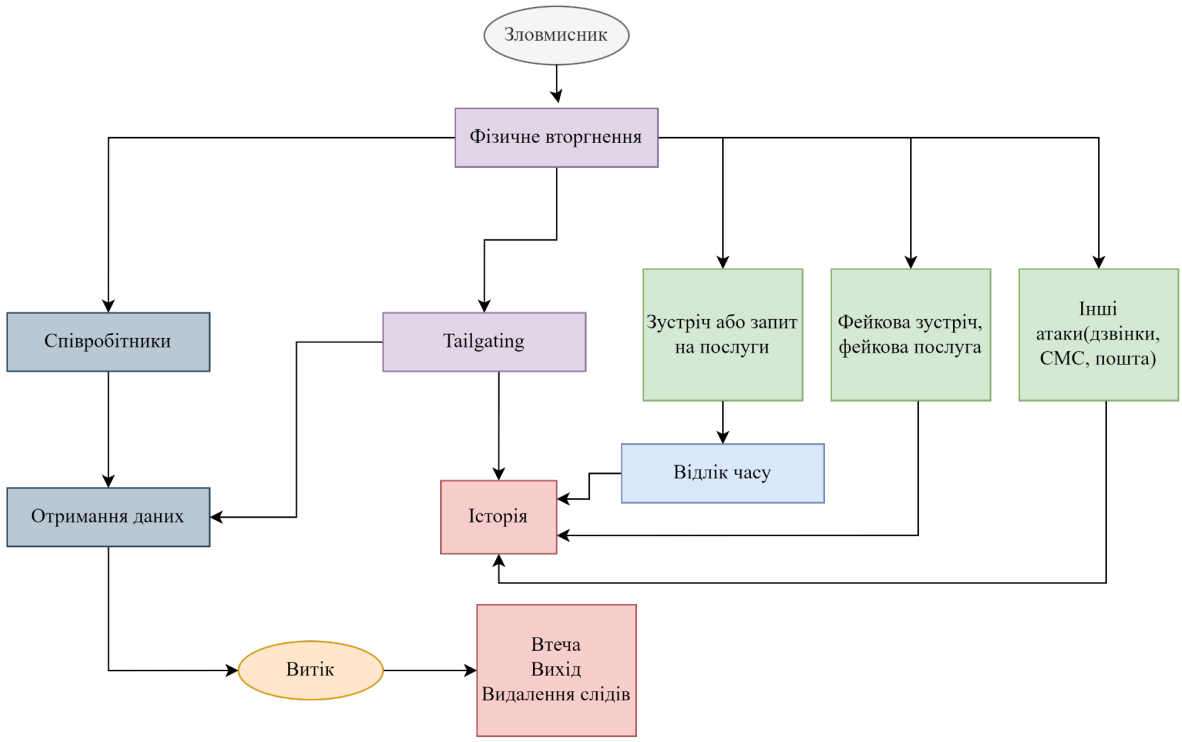

Рис. 3.2. Сценарій отримання фізичного доступу

3.2 Управління обізнаністю персоналу в питаннях протидії методам соціальної інженерії

Соціальні інженери під час проведення соціоінженерних атак опираються на вразливості людини та використання людського фактору. Соціальна інженерія використовує людську поведінку, щоб обійти заходи безпеки, тому працівники повинні бути добре поінформованими та пильними. Тому, у цьому розділі розглядаються стратегії підвищення обізнаності працівників, виявлення загроз соціальної інженерії та впровадження превентивних заходів. Розвиваючи культуру безпеки, організації можуть значно знизити ризики, пов'язані з атаками соціальної інженерії.

Виходячи з цього, внутрішні загрози можуть виникати внаслідок таких факторів:

- непрофесійна поведінка співробітників;
- низький освітній статус і профілактична робота в організації;
- неповна система оплати і стимулювання персоналу;
- декомунізація правил роботи персоналу, невідповідність кадрової політики та умов праці в організації;
- психологічні та комунікативні характеристики співробітників;
- відсутність нормативно-правової бази для організацій, що визначає форму їх діяльності та правила поведінки персоналу.

Поки немає чіткої і всеосяжної математичної моделі, що описує поведінку людей в різних ситуаціях, їх реакцію на певні впливи і загальні обставини, а також можливі помилки. Природно, цей фактор грає на руку зловмисникам.

Атака з використанням методів соціальної інженерії складається з 3 основних етапів: збір, профілювання і реалізація.

1. Збір даних про об’єкт атаки – найважливіший етап. Завдання полягає в тому, щоб визначити характеристики цілі атаки, включаючи зовнішні впливи. Джерелами даних є соціальні мережі, опублікована інформація тощо. Також

ефективно спілкуватися з родиною, друзями та колегами, відстежувати ефективність цілі та навіть взаємодіяти з нею.

2. На етапі профілювання аналізується зібрана інформація для побудови моделі атаки. Визначаються особливості та недоліки потенційної цілі. Обирається можливий вектор атаки, який може бути використаний залежно від способу взаємодії з ціллю через певний канал комунікації (електронна пошта, телефон, особистий контакт тощо). Канал комунікації може бути залучений для різних цілей: вербування, неформального спілкування, тиску тощо. Вибраний вектор атаки має на меті досягнення конкретних результатів.

3. На етапі виконання атаки модель реалізується і створюється на етапі профілювання. Тут в повну силу вступають психологія, нейролінгвістичне програмування (НЛП) і технічні інструменти. Якщо початкова хвиля атак була успішно реалізована, слід використовувати нові вхідні дані, щоб повернутися до фази збору інформації, і повторювати кроки, поки нова інформація не продовжить відображатися або поки атака не досягне бажаної глибини.

Активне використання Інтернету, крім своїх переваг, має ряд істотних недоліків. Це додаткові канали зв'язку з об’єктом атаки, "сліди", залишені власне об’єктом атаки, вивчивши які, можна скласти портрет потенційного об’єкту атаки. Інтернет дає зловмисникам можливість автоматизувати свою роботу і значно знижує "трудовитрати" на виконання атак.

У той же час багато компаній одночасно бояться і не розуміють, чому необхідна оцінка персоналу на основі використання методів соціальної інженерії. Їх часто лякають тим, що такі процеси не регулюються законом або міжнародними стандартами. Він більш професійний, і часто його ефективність залежить від навичок конкретного виконавця.

Окрім використання технічних заходів для захисту інформації (контроль доступу, мінімізація дозволів, моніторинг інцидентів та трафіку тощо), заходи також можуть бути використані для захисту інформації), основний захід захисту від використання методів соціальної інженерії полягає в тому, що навчання "безпека через освіту" є регулярним, простим і легким для розуміння.

Зазвичай в організаціях до процесу навчання формально підходять вимоги і практики інформаційної безпеки. Таким чином, виникає ситуація, коли співробітники компанії мають низький рівень обізнаності та грамотності в питаннях інформаційної безпеки. Це супроводжується їх недбалим і недбалим ставленням до потоку інформації, що надходить. На додаток до навчання, також варто підвищити пильність співробітників, регулярно перевіряючи співробітників [33].

На закінчення слід зазначити, що людські проблеми не можуть бути вирішені тільки технічними методами. Тільки комплексний підхід може бути використаний для захисту від атак з використанням методів соціальної інженерії. Збираючи, обробляючи, порівнюючи та аналізуючи дослідження в галузі протидії атакам із використанням методів соціальної інженерії, необхідно визначити та систематизувати систему заходів та методів для підвищення кваліфікації персоналу в галузі протидії атакам із використанням методів соціальної інженерії.

Існує чимало методів для захисту від соціальної інженерії. Вони поділяються на технічні та нетехнічні. Методи захисту від соціальної інженерії:

1. Організація навчання з кібербезпеки для всіх співробітників, включаючи вище керівництво та IT-фахівців. Освіта повинна демонструвати та моделювати реальні випадки, починаючи з життєвого циклу соціальної інженерії. Освіта призначена для користувачів з низьким рівнем обізнаності про кібербезпеку.

2. Сканування слабких паролів, які потенційно може використовувати зловмисник, наприклад, для отримання доступу до мережі організації. Слід використовувати двофакторну автентифікацію, щоб створити додатковий рівень захисту.

3. Впровадження рішень для забезпечення безпеки, щоб попереджати і повідомляти про можливі випадки шахрайства, а також виявляти спам та фішинг.

4. Створення політики безпеки та складання чіткого плану дій, якого повинні дотримуватися працівники у випадках зіткнення з проявами соціальної інженерії.

5. Використання спеціалізованих рішень для централізованого управління корпоративними мережами, в т.ч. повний огляд мережі, всіх рішень безпеки та інцидентів для виявлення та усунення потенційних загроз.

Пропонується ввести простий список запитань та порад, які детально будуть проходитися на тренінгах щодо забезпечення обізнаності у сфері кібербезпеки та соціальної інженерії. Наприклад, у відповідь на прохання надати певні відомості, то необхідно забезпечити впевненість у тому, що:

- співрозмовник видає себе за того, ким насправді є;
- співрозмовник має право запитувати про це.

Тому у разі прохання повідомити будь-що з наступного списку, обов'язково потрібно або відмовляти, або ж дотримуватися правил використання даних організації. Існують типи запитів, на які слід давати негативну відповідь, зокрема:

- пароль;
- співробітники компанії або структура компанії;
- телефони співробітників компанії;
- особисті дані;
- інформація про комп'ютерні системи та процедури;
- будь-які конфіденційні дані.

У ході атаки соціальні інженери можуть просити об'єкт впливу вчинити будь-які дії і дуже важливо бути готовим до цього та мати список дій, які точно не можна виконувати у разі прохання. Нижче наведено приклад таких прохань:

- відкрити прикріплений додаток до e-mail;
- змінити пароль;
- надіслати електронну версію певного документа;
- виконати певні команди на комп'ютері;

- власноруч проводити якісь операції над програмним забезпеченням, як от видалення, вилучення або встановлення;
- змінювати налаштування мережі або персонального комп'ютера.

Обов'язкове правило відносно прохання виконання певних дій – "не слід довіряти комусь без підтвердження особи".

Також співробітникам у ході тренінгів потрібно надати чіткі інструкції щодо того, що пароль, виданий в компанії є власністю організації та не може бути використаний у власних цілях.

Організація повинна укласти чіткий звід правил щодо відвідувачів організації. Особливу увагу слід приділити випадкам, коли працівники зустрічають сторонніх осіб на робочих місцях. Радиться розробити порядок коректного вирішення цього питання.

Повинні існувати певні правила щодо інформації, яку працівник може та не може розголошувати у приватних розмовах зі сторонніми людьми. У цьому повинний допомогти список запитань та прохань, наданий вище.

Крім того, надані вище поради існують не лише для правильної реакції на спроби атаки з використанням соціальної інженерії, а й для того, щоб повідомляти відповідальних осіб про підозрілі спроби атак, щоб вони могли провести розслідування та підтвердити або спростувати такі намагання.

Розроблено звід порад для організацій, який буде спонукати працівників повідомляти про спроби атаки, а не приховувати їх:

- некаральна політика компанії;
- нагорода за хорошу поведінку.

Однією з головних причин, чому люди не повідомляють про те, що вони стали об'єктами атак фішингових повідомлень електронної пошти, таких як натискання посилань, завантаження шкідливих файлів або введення інформації у веб-форми, є те, що вони бояться покарання або навіть втрати роботи. Однак успішна незареєстрована спроба фішингу може привести до значного простою і, якщо організація стане об'єктом атаки програм-вимагачів, до покупки величезної кількості біткоїнів для розшифровки даних.

Співробітники повинні знати, що допустимо і необхідно повідомляти про те, що вони стали об'єктами атаки соціальної інженерії. Потім їх можуть направити на додаткове навчання, але в результаті їм не доведеться відправляти своє резюме в пошуках нової роботи. Багато компаній, що займаються соціальною інженерією, включають у свої контракти з клієнтами положення, що забороняють звільнення співробітників за результатами перевірок.

У рідкісних випадках працівників слід звільняти за нерозуміння (або небажання дотримуватися) важливих принципів безпеки. Такі співробітники стають скоріше тягарем, ніж перевагою. Але розірвання трудового договору з працівником має бути крайнім заходом. Слід почати з відмови від усіх спроб навчити співробітників, включаючи вихід за рамки звичайної програми підвищення кваліфікації. Також необхідно постаратися впровадити додаткові технічні засоби контролю.

Карати людей за помилки не у інтересах організації, але заохочення доброї поведінки може допомогти. Але, знову ж таки, робити все правильно – це тонке мистецтво. Причина делікатності цієї проблеми полягає в тому, що іноді люди намагаються обдурити систему.

Слід уникати прямого винагородження за повідомлення про більшість спроб фішингу, щоб співробітники не порушували роботу системи. Це може спонукати їх навмисно підписуватись на фішингові розсилки, створюючи додаткове навантаження для служби безпеки. Ідея полягає в тому, щоб винагороджувати якісні повідомлення, а не їх кількість. Якщо організація зосереджується на кількості винагород, це може призвести до реальної фішингової атаки, яка обійдеться дорого для компанії [34].

Тренінги з обізнаності з протидії атакам, основою яких є соціальна інженерія, слід проводити для всіх працівників організації. Слід запровадити графік проведення таких тренінгів, щоб одночасно і підтримувати актуальність інформації, і не відволікати працівників від їх прямих обов'язків. До прикладу, пропонується проводити тренінги з оновленим змістом, згідно нових тенденцій кіберзагроз, раз на рік. Щоквартально слід запровадити короткі нагадування або

презентації для того, щоб освіжити основні моменти в пам’яті працівників. Для нових співробітників тренінги мають проводитися при вступі на роботу, щоб забезпечити їх всіма необхідними знаннями перед виконанням їх обов’язків. У разі потреби, слід проводити додаткові цільові тренінги, якщо були впроваджені нові системи або виявлені нові вразливості.

У ході проведення тренінгів слід звернути увагу на те, як протидіяти новим методам соціальної інженерії, а саме “діпфейкам” та підробці голосу і вішингу. Існує кілька способів виявити фейкові відео. Відео, де людина ніколи не кліпає, кліпає занадто часто або кліпає неприродним чином, є результатом зусиль сучасних фальсифікаторів, які намагаються переконливо оживити обличчя. Бажано звертати увагу на будь-які проблеми з обличчям, такі як нерівності шкіри або волосся, або обличчя, які виглядають більш розмитими, ніж навколишнє середовище. Крім того, варто звернути увагу на аномально м'яке фокусування. Також важливо враховувати освітлення. Оскільки освітлення в цільовому відео часто краще, ніж у зразкових кліпах, які використовуються для створення фейкового відео, алгоритми глибокої підробки часто зберігають освітлення з цих кліпів. Якщо відео було сфабриковане, а оригінальний аудіозапис – ні, може здатися, що голос не належить людині.

Для виявлення випадків, коли хакери намагаються клонувати або підробляти голос, в смартфон або програмне забезпечення голосового помічника можна вбудувати нове рішення, відоме як Void (Voice liveness detection). Void працює шляхом визначення різниці в спектральній потужності між живим людським голосом і голосом, відтвореним через динамік. Якщо є підстави підозрювати, що абонент відповідає на ваш діалог за допомогою заздалегідь записаного матеріалу, бажано поставити те саме запитання ще раз і прослухати відповідь, щоб з'ясувати, чи відрізняється вона від попередньої. Доцільно ставити відкриті запитання, на які буде складно відповісти за допомогою сценарію. Оптимальною позицією під час такого дзвінка буде більш напористий, авторитетний і вимогливий тон, щоб спрямовувати розмову і здійснювати більший контроль над тим, що вони хочуть «розіграти». Якщо розмова

відхилиться від теми, цей план виявиться неефективним. Тому, якщо ініціатор не впевнений у напрямку дискусії, доцільно поставити питання, яке не має прямого відношення до обговорюваної теми.

Форма навчання може включати такі види діяльності:

- теоретичні заняття;
- практикум;
- онлайн-семінари;
- рольові ігри (наприклад, створення моделі атаки).

Важливо зазначити, що саме підвищення обізнаності та навчання у сфері кібербезпеки та протистояння атак, основою яких слугує соціальна інженерія значно впливають на зменшення ризиків успішних атак. Це показує дослідження, яке провела компанія KnowBe4 [35].

У 2022 році загальний середній базовий рівень Phish-prone Percentage (PPP) у всіх галузях та розмірах організацій становив 32,4%, що означає, що менше третини працівників середньої компанії можуть бути під загрозою кліку на фішинговий електронний лист. Однак лише 17,6% тих самих користувачів проваляться протягом 90 днів після завершення першого навчання на платформі KnowBe4. Після принаймні року використання платформи KnowBe4 лише 5%, цих користувачів провалять тест на фішинг. Організації покращили свою вразливість до фішингових атак у середньому на 85% за один рік, дотримуючись рекомендованого підходу, що можна побачити на рис 3.3.

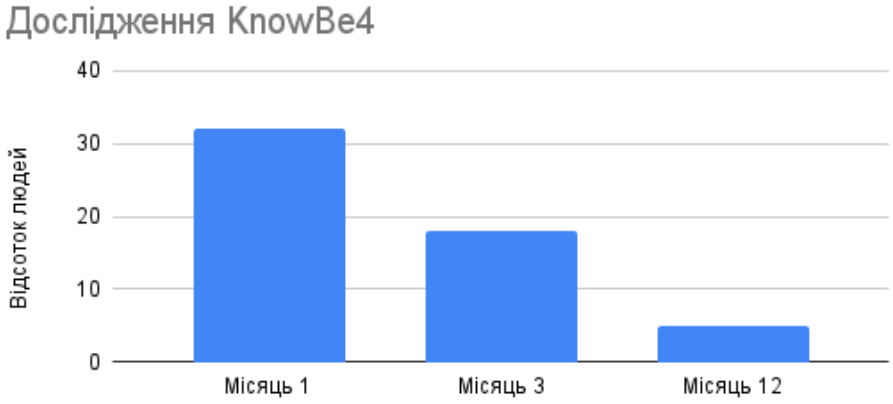

Рис 3.3. Результати проведення навчання компанією KnowBe4

У процесі впровадження навчання для співробітників організації важливо зацікавити їх та надати правильні ресурси для покращення вмінь та знань в галузі кібербезпеки та кібергігієни. Пропонується запровадити навчання працівників на одній з запропонованих нижче платформ, хоча ними можливості для навчання не обмежуються.

Таким чином обов’язковими складовими програми підвищення обізнаності працівників у питаннях протидії соціальній інженерії мають бути:

- роз'яснення щодо правил використання паролів, виданих компанією:
  - пароль є власністю організації;
  - пароль не може використовуватися для інших сервісів;
- навчання працівників правилам безпечної роботи з електронною поштою:
  - перевірка відправника та одержувача повідомлення на легітимність;
  - виявлення ознак машинного перекладу в текстах листів;
  - пошук помилок, некоректностей, підозрілих пропозицій у листах;
  - реагування на ознаки фішингу, спаму, шахрайства;
- інструктаж щодо взаємодії з відвідувачами:
  - процедури перевірки легітимності особи відвідувача;
  - супроводження відвідувачів;
  - повідомлення про зустріч особи, яка не є співробітником;
- правила поведінки в соціальних мережах:
  - обмеження публікації персональних даних у соціальних мережах;
  - методи виявлення підробок (діпфейків, вішингу);
  - ознаки фейкового відео;
  - способи розпізнавання підробленого голосу;
- форми проведення занять:
  - лекції;
  - практикуми;
  - онлайн-семінари;
  - рольові ігри;

- мотиваційна політика:
  - некаральний підхід до помилок працівників;
  - заохочення правильної реакції.

3.3 Рекомендації щодо впровадження передових технологічних рішень для пом'якшення загроз соціальної інженерії

Незважаючи на те, що соціоінженерні атаки зазвичай спрямовані на вразливості людини та використання людського фактору, впровадження передових технологій для запобігання та пом’якшення впливу атак, основою яких є соціальна інженерія дозволяють значно покращити стан інформаційної безпеки організації. Неефективно опиратися тільки на обізнаність та навчання співробітників, а й слід звернути увагу на інші рішення протидії загрозам соціальної інженерії. У цьому розділі пропонується низка рекомендацій щодо впровадження технологічних рішень, що здатні значно знизити ризик соціоінженерних атак для організацій.

Зазвичай передбачається використання стандартних методів для протидії соціоінженерним атакам. Наприклад впровадження протоколів DMARC, SPF та DKIM для автентифікації відправників електронної пошти та зменшення ризику підміни доменів та впровадження захисту кінцевих точок.

DMARC, що розшифровується як «Domain-based Message Authentication, Reporting & Conformance» – це протокол автентифікації, політики та звітності електронної пошти. Він базується на широко розповсюджених протоколах SPF і DKIM, додаючи посилання на доменне ім'я автора («From:»), опубліковані політики для обробки одержувачами помилок автентифікації та звітність від одержувачів до відправників, щоб покращити та контролювати захист домену від шахрайської електронної пошти[36].

Sender Policy Framework (SPF) – це метод автентифікації електронної пошти, який допомагає визначити поштові сервери, яким дозволено надсилати електронну пошту для певного домену. Використовуючи SPF, інтернет-

провайдери можуть ідентифікувати електронну пошту від шахраїв і тих, хто займається фішингом, коли ті намагаються надіслати шкідливу електронну пошту з домену, що належить компанії або бренду.

Хоча SPF забезпечує певний захист від спаму та підміни, він не є повноцінним рішенням для захисту електронної пошти. Переадресований лист не пройде SPF-тест, а протокол SPF не може виявити електронну пошту, яка підміняє лише адресу «від» – адресу електронної пошти, яку бачать користувачі. Крім того, щоб SPF працював, організації повинні постійно оновлювати свої записи SPF – трудомістке і громіздке завдання, яке стає ще складнішим, коли компанії змінюють провайдерів інтернет-послуг [37].

DKIM, або DomainKeys Identified Mail, – це метод автентифікації електронної пошти, який використовує цифровий підпис, щоб повідомити одержувачу, що повідомлення було надіслано й авторизовано власником домену. Як тільки одержувач визначає, що електронний лист підписаний дійсним DKIM-підписом, він може підтвердити, що вміст листа не був змінений. У більшості випадків підписи DKIM невидимі для кінцевих користувачів, перевірка відбувається на рівні сервера. Якщо DKIM використовується разом з DMARC або SPF, ви можете захистити свій домен від шкідливих листів, надісланих з доменів, що видають себе за ваш бренд [38].

Використання системи запобігання витоку даних (DLP) є життєво важливим для зменшення ризику витоку даних через різні канали, включаючи електронну пошту, веб-трафік та передачу файлів. Основними завданнями DLP-систем є:

- формалізація опису даних, що захищаються (налаштування системи);
- розпізнавання даних, що захищаються, у вихідному потоці з внутрішньої інформаційної мережі компанії (розпізнавання дій, спрямованих на переміщення конфіденційної інформації);
- реагування на виявлені спроби витоку даних та формування доказової бази для розслідування інцидентів [39].

Одним із засобів усунення вразливостей і одночасно профілактичним заходом є встановлення Web Application Firewall (WAF), що є програмним або апаратним міжмережевим екраном для веб-додатків. Такого роду міжмережевий екран установлюється перед веб-додатком і надає ширші можливості, ніж звичайні програмні міжмережеві екрани, для системи. WAF у змозі контролювати всі об'єкти, які можуть бути доступні користувачам, – URL, що вводяться, а також параметри запитів GET і POST. Також міжмережевий екран не дозволяє користувачам запускати об'єкти, що не належать до веб-ресурсу [40].

Також важливим залишається використання IPS/IDS. IDS розшифровується як Intrusion Detection System – система виявлення вторгнень. IPS, або Intrusion Prevention System, – система запобігання вторгненням. У порівнянні з традиційними засобами захисту, IDS/IPS забезпечують вищий рівень захисту мережі. IPS та IDS-системи мають ряд корисних можливостей:

- аналіз сигнатур – трафік перевіряється на відповідність вже відомим атакам, що дозволяє виявити атаки, шкідливі коди, рух хибного трафіку та інші ризики;
- виявлення аномальної поведінки – системи можуть розпізнавати нешаблонні варіанти атак;
- спостереження в реальному часі – алгоритми збирають дані, комплексно аналізують їх, що дозволяє не лише знаходити проблеми, а й точно ідентифікувати джерело, час та спосіб розповсюдження загрози [41].

Оскільки традиційні методи однофакторної автентифікації стають все більш недостатніми, багатофакторна автентифікація (MFA) стає надійним контрзаходом. MFA посилює безпеку, вимагаючи більш ніж одну форму перевірки для підтвердження особи користувача. Зазвичай MFA поєднує два або більше з наступних факторів:

- знання (користувач знає пароль або PIN-код);
- володіння (користувач володіє карткою, смартфоном, USB-накопичувачем);

- невід’ємність (біометричні дані користувача, такі як відбиток пальця, долоня, обличчя).

Для проактивного запобігання атакам MFA найпростіший спосіб – оптимізувати конфігурацію процесів автентифікації MFA. Рекомендується посилити безпеку та контроль MFA, виконавши наступні дії:

- скоротити проміжок часу між факторними автентифікаціями;
- обмежити кількість невдалих спроб доступу, дозволених протягом певного періоду часу;
- додати геолокаційні або біометричні вимоги;
- збільшити кількість факторів, необхідних для надання доступу;
- відмічати надмірну кількість невдалих спроб доступу або будь-які неправильні конфігурації MFA та направляти до аналітика з безпеки [42].

Ключовою стратегією є поєднання поведінкової аналітики, машинного навчання (ML) та ШІ. Це дозволяє аналізувати шаблони у спілкуванні та виявляти аномалії. До того ж ML та ШІ можуть вчитися на поточних загрозах, що, як наслідок, значно покращить виявлення загроз соціоінженерних атак.

Поведінкова аналітика використовує поєднання аналізу великих даних і ШІ на основі даних про поведінку користувачів для виявлення закономірностей, тенденцій, аномалій та іншої корисної інформації, що дозволяє вживати відповідних заходів [43]. Таким чином, поведінкова аналітика здатна відстежувати типові дії користувача і визначати відхилення, що може свідчити про те, що обліковий запис працівника організації був скомпрометований або проводяться якісь інші дії зі зловмисним наміром.

Алгоритми ML здатні аналізувати та виявляти приховані зв'язки у великих обсягах даних, що робить їх потужним інструментом для виявлення складних закономірностей та аномалій, які часто зустрічаються в атаках соціальної інженерії. Ці алгоритми можуть обробляти величезні обсяги різноманітних даних, таких як мережевий трафік, журнали активності користувачів, електронні листи та повідомлення, щоб розпізнавати і прогнозувати тактику зловмисників.

Наприклад, моделі ML можуть аналізувати вміст електронних листів і виявляти ознаки фішингових атак, такі як підозрілі посилання, спроби видати себе за легітимні організації або неправильний синтаксис. Вони також можуть відстежувати і класифікувати моделі поведінки користувачів, виявляючи аномальну активність, яка може вказувати на скомпрометовані акаунти або зловмисну діяльність інсайдерів.

Крім виявлення атак, моделі ML здатні прогнозувати майбутні спроби соціальної інженерії, аналізуючи історичні дані про попередні атаки, тактику зловмисників і вразливості системи. Це дозволяє організаціям впроваджувати превентивні заходи та адаптивно вдосконалювати свої стратегії захисту.

ШІ може швидко адаптуватися до нових стратегій, забезпечуючи динамічний захист, який еволюціонує разом із ландшафтом загроз. Така адаптивність має особливе значення в контексті соціальної інженерії, де тактика зловмисників постійно розвивається і змінюється. Системи ШІ здатні аналізувати великі обсяги різноманітних даних, включно з мережевим трафіком, журналами подій, змістом повідомлень та іншими джерелами, щоб виявити нові шаблони та індикатори атак [44].

Для протидії атакам, заснованим на автоматизації за допомогою ШІ, слід впровадити обмеження швидкості, багатофакторну автентифікацію (MFA) та автоматизований захист. Обмеження швидкості для надсилання повідомлень або публікації контенту на платформах ускладнює масові фішингові атаки, засновані на автоматизації. Використання MFA ускладнює отримання несанкціонованого доступу для автоматизованих систем, навіть якщо у них є деякі облікові дані користувачів. Автоматизований захист на основі ШІ, який включає аналіз поведінки, супротивне навчання та симуляцію атак, дозволяє системам автоматично зміцнюватися проти загроз [45].

Для протидії атакам, заснованим на створеному ШІ реалістичному контенті, слід використовувати такі методи, як ідентифікація обману, перевірка контенту, цифрове водяне маркування та відновлення контенту. Варто розробляти ШІ-рішення, які можуть розпізнавати та позначати контент,

створений штучним інтелектом. Наприклад, інструменти для виявлення діпфейків, що аналізують невідповідності у відео. Також важливо впровадити практику маркування оригінального контенту водяними знаками, що сигналізують користувачам про його автентичність. У випадку шкідливих змін контенту за допомогою ШІ, генеративні моделі ШІ можуть відновлювати або виправляти такий контент.

Методи розпізнавання підробленого відео можна розділити на дві групи: ті, що використовують хронологічні характеристики, і ті, що досліджують візуальні артефакти в кадрі. Візуальні артефакти в кадрі часто включають невідповідності в текстурі обличчя, наприклад, відсутність дрібних деталей, таких як зморшки, які складно точно синтезувати для моделей поточного покоління. Методи згладжування, що використовуються на завершальному етапі створення фейкового кадру, можуть призвести до втрати цих текстурних особливостей, що ускладнює виявлення. Часові характеристики передбачають вивчення послідовності рухів і виразів обличчя в різних кадрах. Оскільки деякі моделі глибокої підробки відео не можуть ідеально відтворити хронологічні властивості справжнього відео, ці невідповідності можуть свідчити про фальсифікацію.

Один із підходів полягає в аналізі часових патернів моргання очей за допомогою довготривалої рекурентної згорткової мережі (LRCN). Цей метод ґрунтується на спостереженні, що частота моргання в глибоко підроблених відео значно нижча порівняно з нормальними відео. Інший метод полягає у виявленні внутрішньокадрових і часових невідповідностей. Згорткова нейронна мережа (CNN) використовується для вилучення ознак на рівні кадру, які потім вводяться в мережу довготривалої короткочасної пам'яті (LSTM) для побудови дескриптора послідовності, корисного для класифікації.

Також використовується дослідження артефактів викривлення обличчя для виявлення глибоких підробок. Ці артефакти виявляються за допомогою моделей CNN, які фокусуються на невідповідності роздільної здатності між деформованою областю обличчя та навколишнім контекстом.

Підхід MesoNet представляє дві глибокі мережі, а саме Meso-4 і MesoInception-4, які досліджують підроблені відео на мезоскопічному рівні аналізу. Крім того, також використовуються відмінності в текстурі обличчя, а також відсутні відображення і деталі в області очей і зубів у підроблених відео. Для класифікації на основі цих ознак використовували логістичну регресію та нейронні мережі.

Спектр технологічних рішень для протидії соціальній інженерії широкий. Основні рішення та їх призначення наведені в табл. 3.1.

Таблиця 3.1

Призначення технологічних рішень для протидії соціальній інженерії

Технічна міра захисту	**Призначення**
DMARC	Покращення автентифікації та зменшення ризику підміни доменів для електронної пошти
SPF	Визначення поштових серверів, які мають дозвіл на надсилання електронної пошти для певного домену
DKIM	Автентифікація електронної пошти через цифровий підпис для підтвердження надсилання від власника домену
DLP	Зменшення ризику витоку даних через різні канали, включаючи електронну пошту, вебтрафік та передачу файлів
WAF	Виявлення та запобігання вторгненням у мережу та захист від різних видів загроз
IPS/IDS	Виявлення та запобігання вторгненням у мережу та захист від різних видів загроз
Класифікація даних	Визначення рівня чутливості даних та відповідних заходів захисту від витоку
Контроль доступу	Обмеження доступу до ресурсів і даних на основі ролей та прав користувачів
Шифрування резервних копій	Запобігання несанкціонованого доступу до даних
MFA	Посилення безпеки шляхом вимоги більш ніж однієї форми перевірки для підтвердження особи користувача
ШІ	Виявлення діпфейків та реагування на складні атаки та аномалії в реальному часі, автоматизація процесів безпеки

Висновки до розділу 3

У розділі було розглянуто два важливі аспекти підвищення організаційної стійкості до загроз соціальної інженерії: вивчення сучасних стратегій захисту IT-індустрії від витоку інформації та управління обізнаністю персоналу в питаннях протидії методам соціальної інженерії.

Були розглянуті сучасні стратегії, які застосовуються в IT-індустрії для захисту від витоку інформації, що є поширеним наслідком успішних атак соціальної інженерії. Вивчаючи різні технічні засоби захисту та найкращі практики, в розділі надано аналіз заходів, які організації можуть вжити для посилення свого захисту від спроб витоку даних.

Було висвітлено критично важливу роль обізнаності та навчання співробітників протидії методам соціальної інженерії. Оскільки людський фактор залишається однією з найважливіших вразливостей, яку використовують соціальні інженери, забезпечення працівників знаннями та навичками, необхідними для розпізнавання тактик соціальної інженерії та реагування на них, має першочергове значення. Запропоновано проведення тренінгів з такими основними темами:

- роз'яснення щодо правил використання паролів, виданих компанією;
- навчання працівників правилам безпечної роботи з електронною поштою;
- інструктаж щодо взаємодії з відвідувачами;
- правила поведінки в соціальних мережах;
- обмеження публікації персональних даних у соціальних мережах.

У розділі запропоновано використання передових технологічних рішень, таких як DMARC, SPF, DKIM, DLP, WAF, MFA, ШІ для пом’якшення загроз соціальної інженерії. Також були розглянуті та запропоновані до використання ML-алгоритми та ШІ-інструменти для виявлення діпфейків. Впровадження новітніх технологій запропоноване для зниження залежності від людського фактору як основної небезпеки та опори соціальних інженерів.

ВИСНОВКИ

Соціальна інженерія залишається одним з найбільших ризиків для кібербезпеки, оскільки експлуатує людський фактор, обходячи технічні засоби захисту. З розвитком цифрових технологій виникають нові методи соціальної інженерії, адаптовані до Інтернет-середовища.

У ході виконання поставлених завдань були отримані такі результати:

- було розглянуто теоретичні аспекти соціальної інженерії, а саме життєвий цикл реалізації кібератак, основою яких є соціальна інженерія, різновиди атак та існуючі засоби протидії соціоінженерним атакам;
- було досліджено нові методи соціальної інженерії, що застосовуються в цифровому середовищі, такі як фішинг через соціальні мережі та месенджери, а також використання діпфейків для вішингу.
- була визначена роль соціальних мереж, месенджерів та інструментів ШІ в реалізації соціоінженерних атак, особливо в контексті автоматизованого збору інформації для визначення об'єкта впливу. Крім того, були розглянуті ефективні методи виявлення діпфейків;
- було проаналізовано вплив месенджерів на проведення соціоінженерних атак і дослідження показало, що зростання використання месенджерів значно спрощує завдання соціальних інженерів, що приводить до необхідності підвищення обізнаності співробітників організації про потенційні загрози;
- були розглянуті сучасні стратегії захисту організацій від витоку інформації, як от використання IPS, IDS, MFA, ШІ, особливу увагу було приділено нетехнічним способам захисту від соціоінженерних атак, як навчання персоналу, зміна політики організації та впровадження системи винагород.

Для ефективного захисту від атак, основою яких є соціальна інженерія було запропоновано комплекс вдосконалення освітньої програми організації та створення системи винагород за повідомлення про соціоінженерну атаку.

У кваліфікаційній роботі були запропоновані наступні рекомендації:

- проводити навчання для співробітників організацій для виявлення та запобігання проведенню соціоінженерних атак;
- впровадити систему нагород за виявлення соціоінженерних атак та повідомлення про них до служби безпеки;
- використовувати передові технічні рішення, такі як, IPS, IDS, MFA, SPF, для зменшення ризиків проведення соціоінженерних атак;
- використовувати передові інструменти ШІ для виявлення діпфейків;
- запровадити практику використання водяних знаків для маркування оригінального контенту, що сигналізуватиме про його автентичність;
- впровадити обмеження швидкості для надсилання повідомлень або публікації контенту на платформах для ускладнення масових фішингових атак;
- використовувати автоматизовані системи захисту на основі ШІ, які аналізують поведінку на виявлення аномалій, що можуть свідчити про проведення атаки та сповіщати про це відповідних працівників організації.

Таким чином, дотримуючись наведених у кваліфікаційній роботі порад, можна покращити рівень кібергігієни та зменшити вплив ризиків проведення атак, основою яких є соціальна інженерія, для організацій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Social Engineering Fundamentals. URL: http://scribd.com/doc/19676093/SocialEngineering-Fundamentals (дата звернення: 22.05.2024).

2. Кевін Д. Мітнік, Вільям Л. Саймон. Мистецтво обману. 2004. 360 с.

3. Кузнецов Н. Інформаційна взаємодія як об'єкт наукового дослідження. 2011. 23 с.

4. Чалдіні Р. Психологія впливу. 2017. 124 с.

5. Mouton, F., Leenen, L., Venter, H.S.: Social engineering attack examples, templates and sce-narios. 2019, 186–209 c.

6. Walter Fuertes, Diana Arevalo. Impact of Social Engineering Attacks. 2022.

7. The attack cycle. URL: https://www.social-engineer.org/framework/attack-vectors/attack-cycle/#:~:text=There%20is%20a%20predictable%20four,rapport%2C%20exploitation%2C%20and%20execution (дата звернення: 22.05.2024).

8. Цуркан О., Герасимов Р., Крук О. Методи протидії використанню соціальної інженерії. 2019. URL: https://ela.kpi.ua/server/api/core/bitstreams/9feea6ee-1a2b-4a4b-9364-f471cf50ed5a/content (дата звернення: 22.05.2024).

9. Wilcox, H.; Bhattacharya, M. A framework to mitigate social engineering through social media within the enterprise. 2016. 1039–1044 pp.

10. What Are Tailgating Attacks and How to Protect Yourself From Them. URL: https://www.mcafee.com/blogs/internet-security/what-are-tailgating-attacks/#:~:text=Tailgating%20is%20a%20type%20of,even%20install%20malware%20on%20computers (дата звернення: 22.05.2024).

11. Salahdine, F. & Kaabouch, N. Social engineering attacks: A survey Future Internet. URL: https://doi.org/10.3390/fi11040089 (дата звернення: 22.05.2024).

12. Social-Engineer Toolkit. URL: https://www.sciencedirect.com/topics/computer-science/social-engineer-toolkit (дата звернення: 22.05.2024).

13. R. Heartfield, G. Loukas. Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework.

14. Як українці орієнтуються у новинному онлайн-середовищі – дослідження ОПОРИ. URL: https://www.oporaua.org/polit_ad/iak-ukrayintsi-oriientuiutsia-u-novinnomu-onlain-seredovishchi-doslidzhennia-opori-24797 (дата звернення: 22.05.2024).

15. Манжай О.В., Носов В.В. Робочий зошит для учасників тренінгу з питань кібергігієни. 2021. 9 с. URL: https://www.osce.org/files/f/documents/5/1/492667.pdf (дата звернення: 22.05.2024).

16. Social engineering attack: how some famous twitter accounts were hacked in recent days? URL: https://patancollege.edu.np/social-engineering-attack/ (дата звернення: 22.05.2024).

17. What is artificial intelligence (AI)? Everything you need to know. URL:https://www.techtarget.com/searchenterpriseai/definition/AI-Artificial-Intelligence (дата звернення: 22.05.2024).

18. Довгань О., Литвинова Л., Дорогих С. Кібербезпека в інформаційному суспільстві. 2024. 172 с. https://ippi.org.ua/sites/default/files/2024-2.pdf (дата звернення: 22.05.2024).

19. The State of Phishing 2023. 2023.URL: https://slashnext.com/wp-content/uploads/2023/10/SlashNext-The-State-of-Phishing-Report-2023.pdf#:~:text=SlashNext%20Threat%20Labs%20intelligence%20saw%20a%201%2C265%25%20increase,cybercriminals%20were%20able%20to%20launch%20sophisticated%20attacks%20quickly (дата звернення: 22.05.2024).

20. An Introduction to Deepfakes with Only One Source Video. URL: https://www.analyticsvidhya.com/blog/2021/10/an-introduction-to-deepfakes-with-only-one-source-video/ (дата звернення: 22.05.2024).

21. Murtaza Ahmed Siddiqi, Wooguil Pak, and Moquddam A. Siddiqi. A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. 2022. 6 с.

22. Стартап ElevenLabs, який робить дубляж за допомогою ШІ, додав підтримку української мови. URL: https://dev.ua/news/elevenlabs-dodav-pidtrymku-ukrainskoi-movy-1697097982 (дата звернення: 22.05.2024).

23. Franco-Israeli gang behind EUR 38 million CEO fraud busted. URL: https://www.europol.europa.eu/media-press/newsroom/news/franco-israeli-gang-behind-eur-38-million-ceo-fraud-busted

24. CEO Fraud. URL:https://sosafe-awareness.com/glossary/ceo-fraud/ (дата звернення: 22.05.2024).

25. Fraudsters Cloned Company Director's Voice In $35 Million Heist, Police Find. URL:https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/?sh=39001cea7559 (дата звернення: 22.05.2024).

26. Researchers Say the Deepfake Biden Robocall Was Likely Made With Tools From AI Startup ElevenLabs. URL: https://www.wired.com/story/biden-robocall-deepfake-elevenlabs/ (дата звернення: 22.05.2024).

27. Social Engineering Attack Cycle. URL: https://www.researchgate.net/figure/Social-Engineering-Attack-Cycle_fig1_307606034#:~:text=These%20four%20phases%20can%20be,et%20al.%2C%202015 (дата звернення: 22.05.2024).

28. Юртаєва К. В. Визначення місця вчинення злочинів з використанням комп'ютерних технологій. Форум права. 2009. 434–441 с. URL: http://nbuv.gov.ua/j-pdf/FP_index.htm_2009_2_69.pdf (дата звернення: 22.05.2024).

29. Конвенція про кіберзлочинність : від 23.11.2001 // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: https://zakon.rada.gov.ua/laws/show/994_575/

30. Вітолінський, Великоіваненко. Дослідження ризиків в економіці та підприємництві: Монографія. 2020. 480 с

31. Корольов В., Бенінг Е., Шоргін С. Математична основа теорії ризику, 2019.620 с.

32. Лістер Демарко. Управління ризиками в проектах розробки програмного забезпечення. 2020.196 с.

33. Соціальна інженерія. Низка нетехнічних прийомів маніпулювання користувачами, які використовуються кіберзлочинцями під час атак. URL:https://www.eset.com/ua/support/information/entsiklopediya-ugroz/sotsialnaya-inzheneriya/ (дата звернення: 22.05.2024).

34. №8. Хакінг у практичному застосуванні та соціальна інженерія (Захист від соціальної інженерії). URL:https://hackyourmom.com/kibervijna/%E2%84%968-haking-u-praktychnomu-zastosuvanni-ta-soczialna-inzheneriya-zahyst-vid-soczialnoyi-inzheneriyi/ (дата звернення: 22.05.2024).

35. KnowBe4's 2022 Phishing By Industry Benchmarking Report Reveals that 32.4% of Untrained End Users Will Fail a Phishing Test. URL:https://blog.knowbe4.com/knowbe4-2022-phishing-by-industry-benchmarking-report (дата звернення: 22.05.2024).

36. What is DMARC? URL: https://dmarc.org/ (дата звернення: 22.05.2024).

37. What are Behavioral Analytics? URL: https://www.opentext.com/what-is/behavioral-analytics#:~:text=Behavioral%20analytics%20utilizes%20a%20combination,insights%20to%20enable%20appropriate%20actions (дата звернення: 22.05.2024).

38. What Is DKIM? Get started with DKIM and DMARC to ensure your brand is not being exploited by cybercriminals. URL: https://www.mimecast.com/content/dkim/#:~:text=DKIM%20protocol%20uses%20a

%20cryptographic,not%20been%20changed%20in%20transit (дата звернення: 22.05.2024).

39. Вовчановський П. Демчинський В. Архітектура DLP-систем в умовах політики BYOD. 2020. URL: https://www.researchgate.net/publication/347525260_Arhitektura_DLP-sistem_v_umovah_politiki_BYOD#pf4 (дата звернення: 22.05.2024).

40. Web Application Firewall. URL: https://www.owasp.org/index.php/Web_Application_Firewall (дата звернення: 22.05.2024).

41. Цар О. Коробейнікова Т. Аналіз сучасних відкритих систем виявлення та запобігання вторгнень. 2023. 317 с.

42. MFA Fatigue Attack. URL: https://www.beyondtrust.com/resources/glossary/mfa-fatigue-attack (дата звернення: 22.05.2024).

43. What are Behavioral Analytics? URL: https://www.opentext.com/what-is/behavioral-analytics#:~:text=Behavioral%20analytics%20utilizes%20a%20combination,insights%20to%20enable%20appropriate%20actions (дата звернення: 22.05.2024).

44. Guardians of the Digital Realm: How to Protect Yourself from Social Engineering. URL: https://www.proofpoint.com/uk/blog/user-protection/five-ways-prevent-social-engineering-attacks (дата звернення: 22.05.2024).

45. M. Schmitt. I. Flechais. Digital Deception: Generative Artificial Intelligence in Social Engineering and Phishing. 11 p.