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: “МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ
В ОБЛАСТІ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ”

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 навідповідне джерело

_____ Володимир ДВОРНИЧЕНКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД 41

Володимир ДВОРНИЧЕНКО
Ім’я, ПРІЗВИЩЕ

Керівник: Світлана ЛЕГОМІНОВА
Д.е.н., професор Ім’я, ПРІЗВИЩЕ

Рецензент: Олександр ТУРОВСЬКИЙ
д.т.н., професор 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 кафедрою УІКБ
_____ Світлана ЛЕГОМІНОВА
“____”_____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дворниченку Володимиру Олександровичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Методи захисту інформаційного простору в області соціальної інженерії ”,
керівник кваліфікаційної роботи ЛЕГОМІНОВА Світлана, д.е.н., професор,
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологійвід “27“ лютого 2024 р. №36.

2. Строк подання кваліфікаційної роботи “31” травня 2024р.

3. Вихідні дані до кваліфікаційної роботи: *захист інформаційного простору, атаки соціальної інженерії, методи захисту, соціальна інженерія, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
   1. Проаналізувати технологію атак та основну проблематику захисту інформаційного простору в області соціальної інженерії.
   2. Дослідити різновиди атак соціальної інженерії, проаналізувати поширені види атак та статистичні дані щодо їх реалізації, розглянути роль соціальної інженерії в когнітивній війні.
   3. Визначити основні методи та особливості забезпечення захисту інформаційного простору в області соціальної інженерії, розробити рекомендації з реалізації захисту від атак методами соціальної інженерії.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*
6. Дата видачі завдання “22“ лютого 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання Етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	13.03.2024	виконано
2.	Збір та аналіз літератури.	30.03.2024	виконано
3.	Аналіз технології атак та проблематики захисту інформаційного простору в області соціальної інженерії.	17.04.2024	виконано
4.	Дослідження різновиди атак соціальної інженерії, проаналізувати поширені види атак та статистичні дані щодо їх реалізації, розглянути роль соціальної інженерії в когнітивній війні.	01.05.2024	виконано
5.	Визначення методів та особливостей забезпечення захисту інформаційного простору в області соціальної інженерії, розробка рекомендацій з реалізації захисту від атак.	15.05.2024	виконано
6.	Формулювання висновків за результатами проведеного дослідження.	22.05.2024	виконано
7.	Оформлення роботи.	24.05.2024	виконано
8.	Оформлення презентації.	01.06.2024	виконано
9.	Отримання рецензії на роботу.	04.06.2024	виконано
10.	Захист в ЕК	13.06.2024	виконано

Здобувач вищої освіти _____ Володимир ДВОРНИЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Світлана ЛЕГОМІНОВА
(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 Дворниченко В.О. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код,найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: “ Методи захисту інформаційного простору в області соціальної інженерії”

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач ДВОРНИЧЕНКО Володимир у кваліфікаційній роботі проаналізував технології атак соціальної інженерії, дослідив основні проблеми захисту інформаційного простору, вивчив техніки та прийоми атак соціальної інженерії, розробив практичні рекомендації за темою дослідження.

ДВОРНИЧЕНКО Володимир 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 двох конференціях.

Все це дозволяє оцінити кваліфікаційну роботу здобувача ДВОРНИЧЕНКА Володимира на оцінку “відмінно” та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

“_____“____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Дворниченко В.О. допускається до захисту даної роботи в Екземанційній комісії.

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

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти ДВОРНИЧЕНКО Володимир
на тему “Методи захисту інформаційного простору в області соціальної інженерії”.

Актуальність. Дослідження соціальної інженерії та ролі людського чинника в інформаційній безпеці є сучасним завданням захисту інформаційного простору на рівнях макро- та мікросередовища, тому знаходження ефективних методів протидії негативному вплаву на безпекове становище, розробка способів удосконалення політик інформаційної безпеки проти атак соціальної інженерії з метою протидії діям зловмисника є актуальним та вносить вагомий внесок в вирішення проблеми захисту інформаційного простору в області соціальної інженерії.

Позитивні сторони.

1. У роботі досліджено методи захисту інформаційного простору, виявлено небезпеку зі сторони соціальної інженерії, вивчення технік та прийомів сучасний атак соціальної інженерії дозволило зрозробити та запропоновати практичні рекомендації протидії небезпечним.
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 опрацювала значну джерельну базу, більшисть публікацій англомовних.

Недоліки.

Доцільно було б проаналізувати існуючі технології захисту інформаційного простору в області соціальної інженерії та провести порівняльний аналіз певних прикладів, виявити основні позитивні риси та знайти недоліки.

Однак, вищезгадане зауваження не впливає на загальну позитивну оцінку кваліфікаційної роботи.

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

Рецензент: _____ Олександр ТУРОВСЬКИЙ
д.т.н., професор *підпис* Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню методів захисту інформаційного простору в області соціальної інженерії. Робота складається зі вступу, трьох розділів, що містять рисунки, висновки і список використаних джерел із 16 найменувань. Загальний обсяг роботи становить 61 сторінку, з яких 2 займають перелік умовних скорочень та список використаних джерел.

Метою роботи є дослідження методів захисту інформаційного простору в області соціальної інженерії.

Об'єктом дослідження є методи захисту від атак соціальної інженерії.

Предмет дослідження - особливості застосування методів характерних для захисту інформаційного простору в області соціальної інженерії.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані порівняння, експертна оцінка, класифікації та методи аналізу та синтезу.

Як результат у роботі проаналізовано основні методи захисту, технології від атак соціальної інженерії, досліджено основні проблеми захисту інформаційного простору, вивчено техніки та прийоми атак соціальної інженерії, розроблено практичні рекомендації.

Галузь застосування. Розроблені рекомендації можуть бути використані для застосування певних методів захисту інформаційного простору в області соціальної інженерії.

Ключові слова: ЗАХИСТ ІНФОРМАЦІЙНОГО ПРОСТОРУ, АТАКИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ, МЕТОДИ ЗАХИСТУ, СОЦІАЛЬНА ІНЖЕНЕРІЯ.

ABSTRACT

The qualification work is devoted to the study of methods of information space protection in the field of social engineering. The work consists of an introduction, three chapters containing figures, conclusions and a list of references of 16 titles. The total volume of the work is 61 pages, of which 3 pages are occupied by a list of abbreviations and a list of references.

The purpose of the work is to investigate methods of information space protection in the field of social engineering.

The object of research is methods of protection against social engineering attacks.

The subject of the study is the peculiarities of applying methods specific to the protection of information space in the field of social engineering.

Research methods. To solve the scientific task, the paper uses methods of comparison, expert evaluation, classification, as well as methods of analysis and synthesis.

As a result, the main methods of protection, technologies against social engineering attacks were analysed, the main problems of information space protection were investigated, the methods and techniques of social engineering attacks were studied, and practical recommendations were developed.

Scope of application. The developed recommendations can be used to apply certain methods of information space protection in the field of social engineering.

Keywords: PROTECTION OF INFORMATION SPACE, SOCIAL ENGINEERING ATTACKS, METHODS OF PROTECTION, SOCIAL ENGINEERING.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ІТ	Інформаційні технології
СІ	Соціальна інженерія
МЗ	Методи захисту
ІП	Інформаційний простір
ПЗ	Програмне забезпечення
КСЗІ	Комплексна система захисту інформації
ІКС	Інформаційно-комунікаційна система
ШІ	Штучний інтелект

ВСТУП

Актуальність теми. У світі, де держави, компанії та навіть окремі користувачі є об’єктом кібератак, забезпечення інформаційної безпеки набуває критичного значення. Разом з постійним розвитком IT-сфери зростають інформаційні ризики і загрози, що вимагають інноваційних підходів до захисту інформаційного простору в області соціальної інженерії. Формування культури безпеки серед персоналу підприємства набуває особливого значення, оскільки забезпечує працівникам необхідні знання й навички для виявлення загроз інформаційній безпеці. Інноваційні методи навчання персоналу з інформаційної безпеки можуть допомогти підтримувати співробітників у курсі останніх трендів та методів захисту, що в результаті підвищить рівень інформаційної безпеки підприємства.

Метою роботи є дослідження методів захисту інформаційного простору в області соціальної інженерії.

Об'єктом дослідження є методи захисту від атак соціальної інженерії.

Предмет дослідження - особливості застосування методів характерних для захисту інформаційного простору в області соціальної інженерії.

Для досягнення цієї мети в роботі необхідно виконати такі **завдання** як:

1. Теоретично оглянути технологію атак та основну проблематику захисту інформаційного простору в області соціальної інженерії.

2. Дослідити різновиди атак з використанням соціальної інженерії, проаналізувати поширені види атак та статистичні дані щодо їх реалізації, розглянути основні методи захисту від атак з використанням соціальної інженерії.

3. Визначити особливості забезпечення захисту інформаційного простору в області соціальної інженерії, розробити рекомендації з реалізації захисту від атак методами соціальної інженерії.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані порівняння, експертна оцінка,класифікації та методи

аналізу та синтезу.

Галузь застосування. Розроблені рекомендації можуть бути використані для застосування певних методів захисту інформаційного простору в області соціальної інженерії.

Практичне значення одержаних результатів. Застосування напрацювань дадуть змогу здійснити обґрунтований вибір методів і засобів захисту інформаційного простору в області соціальної інженерії.

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

РОЗДІЛ 1 ТЕОРЕТИЧНИЙ ОГЛЯД ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ В ОБЛАСТІ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

1.1 Технологія атак соціальної інженерії

Соціальна інженерія - це мистецтво маніпуляції людьми з метою отримання конфіденційної інформації або доступу до систем безпеки, часто використовуючи методи обману і психологічного тиску [1]. Технологія атак соціальної інженерії використовується зловмисниками для отримання незаконного доступу до систем, викрадення даних або виконання інших злочинних дій.

Перш за все, важливо розуміти, що соціальна інженерія не використовує технічні уразливості програмного забезпечення або мережі, але замість цього використовує людські чинники, такі як довіра, недбалість або необережність. Зловмисники використовують психологічні методи, щоб переконати людей надати їм доступ до конфіденційної інформації або виконати певні дії.

У підсумку, технологія атак соціальної інженерії є серйозною загрозою для безпеки інформації. Розуміння цих загроз і вжиття відповідних заходів безпеки є ключовими для захисту від потенційних атак.

Технологія атак соціальної інженерії включає в себе декілька етапів, що спрямовані на використання психологічних та соціальних механізмів для отримання неправомірного доступу до конфіденційної інформації. У книзі “The Art of Deception: Controlling the Human Element of Security” (Мистецтво обману: Контроль людського елементу безпеки) Кевіна Митника, одного з найвідоміших хакерів у світі, який став знаменитим завдяки своїм складним і успішним кібер-атакам, а також популярізації терміна “соціальна інженерія”, атаки соціальної інженерії розділяються на 5 етапів (рис. 1.1). Хоча з моменту публікації книги пройшло більше 20-и років, проте сама технологія атак соціальної інженерії не змінилася.

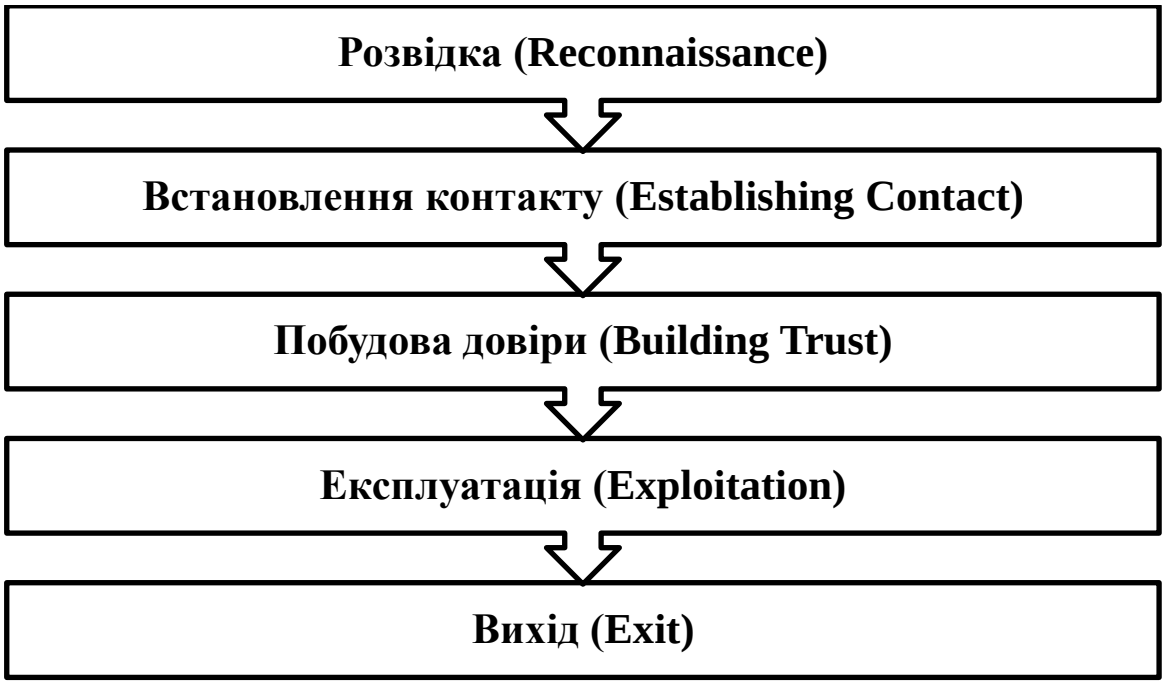

Рис. 1.1. Етапи атак соціальної інженерії

Розглянемо кожен з етапів більш детально:

Розвідка

Етап розвідки є одним з найважливіших у технології атак соціальної інженерії. На цьому етапі зловмисник збирає інформацію про потенційних жертв, щоб здійснити персоналізовану та ефективну атаку. Ключовими аспектами розвідки є вибір цільової аудиторії, збір інформації з відкритих джерел, та фізична розвідка (рис. 1.2).

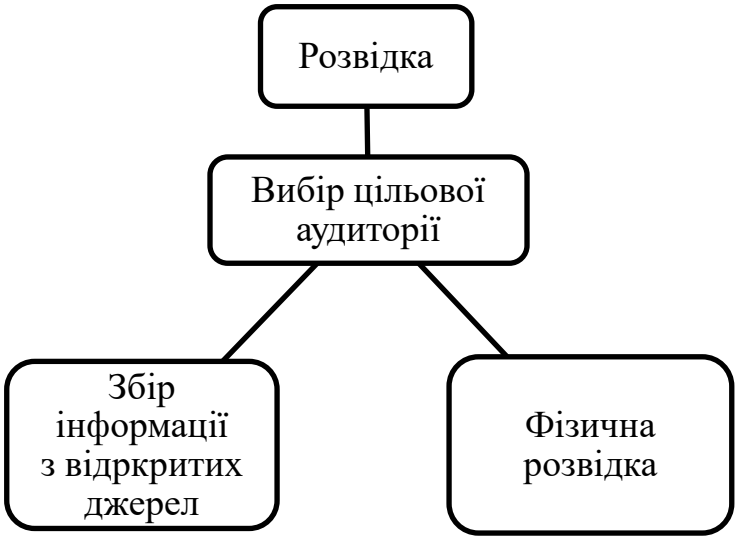

Рис. 1.2. Ключові аспекти етапи розвідки

•Зловмисник обирає свою цільову аудиторію, яка може бути окремою особою, групою користувачів, компанією або іншою установою. Вибір цільової аудиторії зазвичай залежить від цілей атаки, наприклад, отримання конфіденційної інформації або фінансової вигоди.

•Далі відбувається збір інформації про потенційних жертв з різних джерел, таких як соціальні мережі (Instagram, Facebook, Twitter, LinkedIn), веб-сайти, публічні бази даних, блоги, форуми тощо. Розвідку на основі відкритих джерел (OSINT) неможливо недооцінити, наприклад в фундаментальній книзі Майкла Баззела "Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information" автор наголошує, що OSINT дозволяє отримувати детальні профілі та аналізувати поведінку цілей, що є критично важливим для правоохоронних органів, фахівців з кібербезпеки та дослідників [2]. З розвитком IT та кіберзлочинності все більше інформації можна знайти у відкритому доступі, це стосується навіть приватної інформації. Яскравим прикладом є виток приватних повідомлень, телефонних номерів, ip-адрес пристроїв користувачів мессенджеру WhatsApp у 2020 та 2022 роках [3, 4]. Цей процес може здійснюватись як вручну, так і за допомогою ПЗ (MetaSploit, DarkOwl Vision, Cobwebs, WhoIs тощо).

•Також може здійснюватись і фізична розвідка: спостереження за офісами компанії, спілкування з працівниками у неформальних обставинах, аналіз доступної фізичної інформації, такої як сміття (так званий "dumpster diving").

Вся зібрана інформація може включати особисті дані, які вказують на інтереси, звички, професійну діяльність, контакти та інші важливі аспекти життя цільової аудиторії.

Встановлення контакту

Після вибору потенційної жертви та збору достатньої кількості інформації про неї відбувається перший контакт для подальшої взаємодії. Основна мета цього етапу - почати спілкування таким чином, щоб не викликати підозри і створити основу для подальшого впливу та маніпуляцій. Для цього є немало

варіантів, наприклад повідомлення в соціальній мережі, мессенджері, електронній пошті, телефонний дзвінок або особиста зустріч. Також слід виділити три основних компонента для успішного встановлення контакту: правдоподібність, спонукання до дії, психологічний вплив.

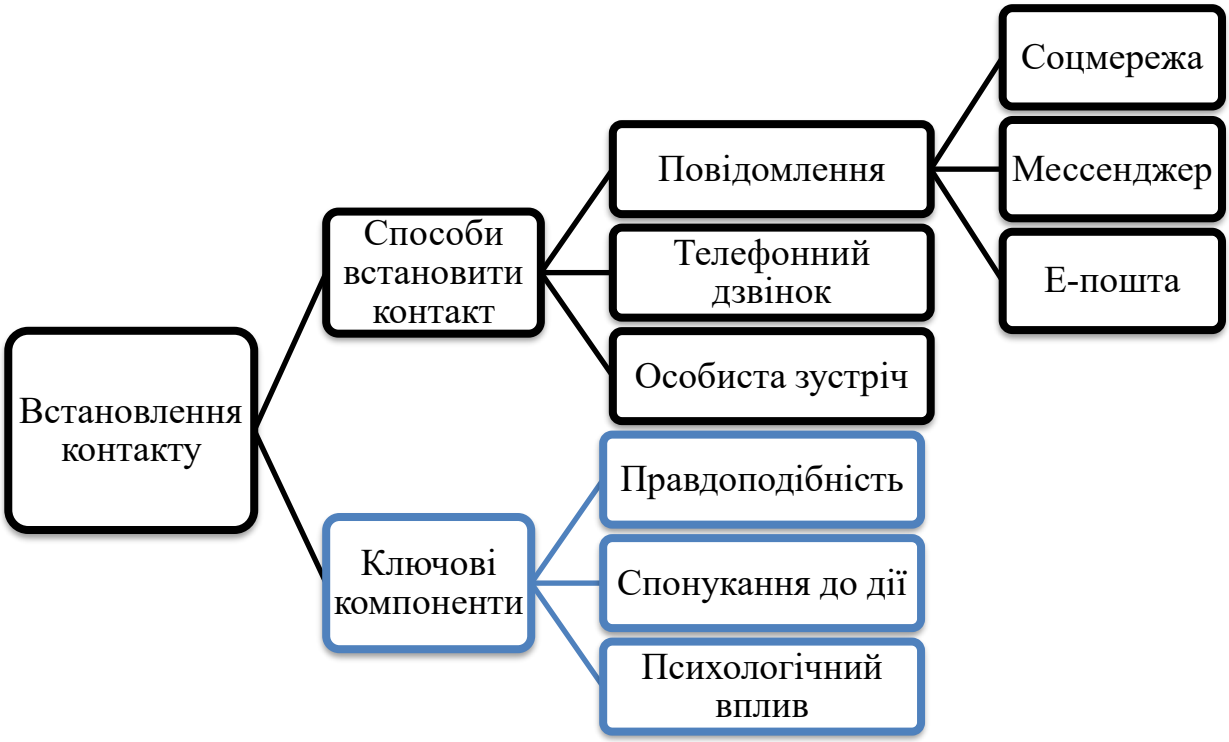

Рис. 1.3. Графічне зображення етапу встановлення контакту

•**Правдоподібність.** Зловмисник має бути добре підготовленим і вміло володіти зібраною інформацією про потенційну жертву, щоб виглядати переконливо і не викликати підозри. А саме: використовувати стиль спілкування, який відповідає внутрішній культурі компанії, включаючи жаргон, терміни та структуру повідомлень, імена і посади співробітників; розпочинати спілкування відповідно до часу (дзвінок у робочий час) і місця (випадкова особиста зустріч в закладі, де обідають співробітники); приділяти увагу до дрібних деталей, таких як правильний формат підпису в електронних листах, використання правильного логотипу компанії тощо.

•**Спонукання до дії.** Контакт має бути таким, щоб викликати відповідну реакцію жертви. Це може бути прохання, що виглядає терміновим або важливим.

Ось декілька прикладів таких повідомлень: “Ваш обліковий запис буде заблоковано, якщо ви негайно не змініте пароль”, “Через підозрілу активність на Вашому аккаунті, рекомендуємо терміново виконати заміну паролю” – створюється відчуття невідкладної, критичності ситуації; “Ви перемогли у нашому щорічному розіграші, щоб отримати приз підтвердить вашу особистість”, “Якщо сьогодні доробиш і відправиш мені цей звіт, то отримаєш підвищення/премію” - обіцянка винагороди, привілеї; “Якщо ми не вирішимо цю проблему зараз, це може призвести до серйозних витрат для компанії”, “Якщо Ви не надасте дані, то втратите доступ до акаунту” – попередження або загроза негативними наслідками.

- **Психологічний вплив.** Використовуються різноманітні техніки психологічного впливу, щоб змусити жертву діяти в інтересах зловмисника. Зловмисник може доводити, що інші люди (колеги, друзі, родичі) вже виконали певну дію, видавати себе за реального авторитета, співробітника, експерта, використовувати почуття зобов’язання після надання жертві якоїсь послуги або допомоги. Ось декілька прикладів: “Ваш колега з відділу маркетингу вже оновив свої дані”, “Ваш батько вже зареєструвався для участі в акції”, “Я з відділу IT безпеки, і ми проводимо перевірку”, “Я допоміг тобі з тим файлом минулого разу, тепер мені потрібна твоя допомога”.

Побудова довіри

На цьому етапі зловмисник намагається досягнути повної довіри жертви. Довіра є основним елементом для успішного проведення атак соціальної інженерної, оскільки без неї жертва може підозрювати що щось не так і відмовитися від співпраці.

Якщо минулий етап (встановлення контакту) був якісно виконаний, то потенційна жертва без сумнівів надасть інформацію необхідну для наступного етапу (експлуатації), наприклад паролі, секретні файли, службову або таємну інформацію тощо. Слід зазначити, що ключовими компонентами цього етапу будуть правдоподібність, спонукання до дії та психологічний вплив, як і на встановленні контакту з потенційною жертвою.

У разі недосконалої легенди, досвідченості, обізнаності потенційної жерти або інших причин втрати контакту з потенційною жертвою є декілька алгоритмів дій зображених на рис. 1.4 та 1.5.

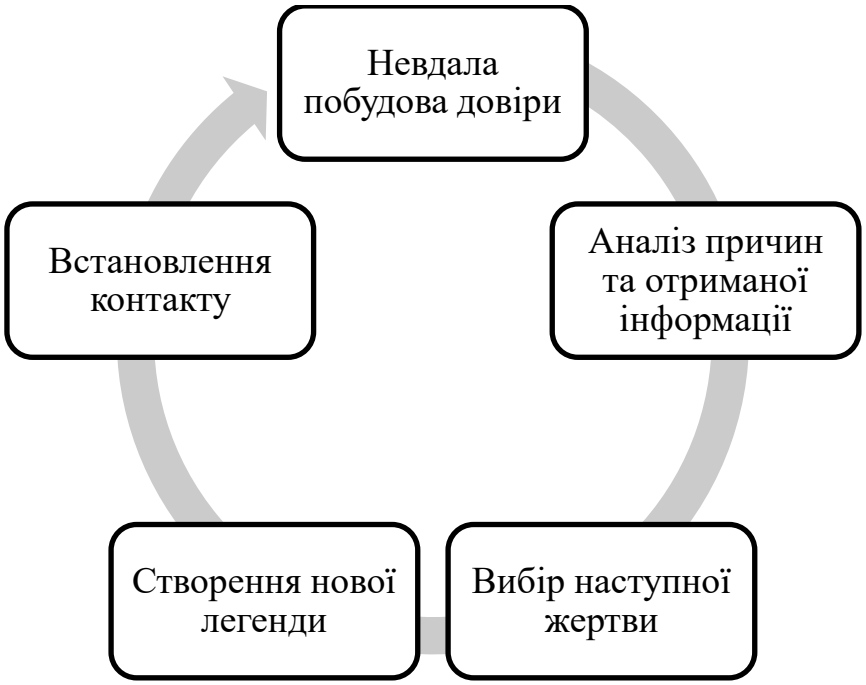

Рис. 1.4. Алгоритм дій в разі можливості змінити потенційну жертву

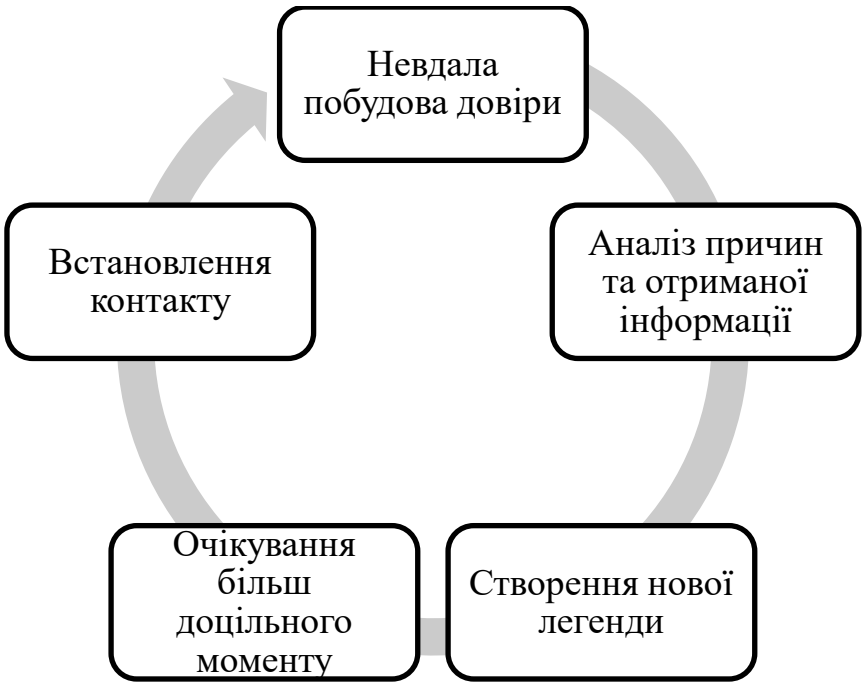

Рис. 1.5. Алгоритм дій в разі неможливості змінити потенційну жертву

Вибір алгоритму дій залежить від того, що стало причиною провалу і наявності можливості здійснити атаку на іншу жертву (наприклад співробітника того ж відділу).

Експлуатація

На етапі експлуатації зловмисник отримує доступ до цінної інформації або фізичних ресурсів, та використовує отримане в свої цілях. Отримання такої інформації здійснюється за допомогою запитів (рис. 1.6.), а саме:

- Запит на інформацію: зловмисник просить жертву надати конфіденційну інформацію, таку як паролі, дані кредитних карток, внутрішні документи. Наприклад, “Чи можете Ви надіслати мені ваші облікові дані для доступу в систему, щоб я зміг допомогти вам вирішити проблему?”, “Чи можете Ви надіслати мені цей файл, щоб я зміг перевірити його на наявність вірусів?”
- Запит на доступ: зловмисник просить доступ до приміщення. Наприклад, “Мені потрібно попасти у серверну кімнату, щоб перевірити справність обладнання. Чи можете Ви відкрити мені двері?”, “Мені потрібно перевірити справність вашого роутеру, який встановила наша компания. Чи можна зайти?”.
- Запит на дії: зловмисник просить жертву виконати певні дії, які призведуть до компроментації системи безпеки. Наприклад, “Чи можете Ви встановити це програмне забезпечення, щоб я мав можливість провести діагностику вашої системи?”.

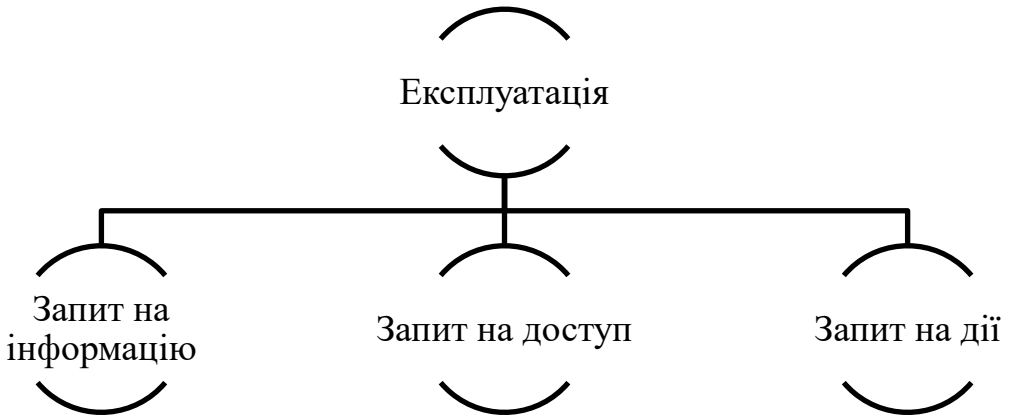

Рис. 1.6. Методи експлуатації жертви

Після отримання зловмисником чутливої інформації (паролів, секретних файлів, службової, таємну інформації) та її використання в своїх цілях це може призвести до наступних наслідків для жертви атаки:

• Фінансових втрат, якщо атака призвела до витоку паролів та кодів автентифікації банківських рахунків.

• Порушення приватності, якщо в результаті атаки конфіденційна особиста та/або службова інформація стала доступною для несанкціонованих осіб.

• Пошкодження репутації через витік таємної інформації.

• Втрати довіри клієнтів, партнерів, співробітників до жертви атаки.

Вихід

Після досягнення мети зловмисник завершує атаку таким чином, щоб не викликати підозри. Завершує контакт без зайвої уваги, наче не відбулося нічого надзвичайного, вживає заходів для видалення і приховування будь-яких доказів атаки (видаляє електронні листи, очищує історію дзвінків, завантажень тощо). У разі наявності можливісті залишення "бекдори", завдяки яким зможе здійснити нову атаку.

1.2 Основна проблематика захисту інформаційного простору в області соціальної інженерії

Інформаційний простір - це комплексна система, що включає в себе мережі інформаційних ресурсів, засобів і технологій обробки інформації, а також суб'єктів, які взаємодіють між собою в процесі створення, зберігання, передачі та використання інформації [5]. Захист інформаційного простору здійснюється як у фізичному, так і кіберпросторі. Основним методом атак на інформаційний простір є кібератака.

Кібератака - спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або

сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту [6].

Основною проблематикою захисту від атак соціальної інженерії в інформаційному просторі є недостатність використання лише програмного, мережевого і апаратного захисту, важливим аспектом в захисті від атак СІ є зменшення впливу людського фактору через ознайомлення людини (персоналу) з можливими атаками та навчанням реагування на них.

Для того, щоб зменшити вплив людського фактору потрібно розвивати культуру інформаційної безпеки у суспільстві. Культура інформаційної безпеки - це сукупність знань, умінь і навичок, а також високий рівень свідомості в інформаційній сфері, що дозволяє ефективно протистояти інформаційним загрозам[7]. Зазвичай, вона зароджується ще змалку. Прикладом такого може бути ситуація, коли дитина не відкриє двері, поки не буде впевнена, що це хтось з батьків. В дорослому віці це може спостерігатись як перевірка інформації іншими джерелами, співставлення з правовими документами, запит додаткової інформації для перевірки особистості. Наприклад, в разі телефонного дзвінку зловмисника від лиця певного банку, тоді потенційна жертва, щоб зрозуміти наскільки правдива інформація може запитати назву та відділення банку, уточнюючі дані про людину, яка йому телефонує. Потенційна жертва з високою культурою ІБ буде знати, що служба підтримки банка не питає ПІН та CVV коди, термін дії карти та останні операції з нею, тому успішно захиститься від атаки СІ.

Якщо розглядати персонал компанії, а не окремих поодиноких людей, то в такому випадку, основним методом захисту від СІ буде правильно розроблена і

впроваджена КСЗІ в ІКС компанії. Комплексна система захисту інформації (КСЗІ) - сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в ІКС. Для організації робіт зі створення КСЗІ в ІКС створюється служба захисту інформації, порядок створення, завдання, функції, структура та повноваження якої визначено в НД 1.4-001-2000.[8] Впровадження КСЗІ в компанію - складний, але необхідний процес для забезпечення захисту інформаційних ресурсів. Відповідальний підхід до кожного етапу, постійне навчання співробітників та регулярний моніторинг системи дозволяють мінімізувати ризики та забезпечити високий рівень інформаційної безпеки.

Рис. 1.7. Складові КСЗІ

Організаційні заходи - основна складова для захисту від атак СІ. Організаційні заходи включають в себе створення концепції інформаційної безпеки, а також:

- складання посадових інструкцій для користувачів та обслуговуючого персоналу;
- створення правил адміністрування компонент інформаційної системи, обліку, зберігання, розмноження, знищення носіїв інформації, ідентифікації користувачів;
- розробка планів дій у разі виявлення спроб несанкціонованого доступу до інформаційних ресурсів системи, виходу з ладу засобів захисту, виникнення

надзвичайної ситуації;

- навчання правилам інформаційної безпеки користувачів [9].

Отже, основною проблематикою захисту інформаційного простору в області соціальної інженерії буде:

Погана обізнаність людини (персоналу) в області захисту від соціальної інженерії. Незважаючи на наявність технічних засобів захисту, людський фактор залишається однією з найбільш вразливих ланок в ІКС, працівники можуть несвідомо встановлювати и користуватися шкідливим ПЗ, відкривати підозрілі посилання та файли. СІ спирається на маніпулювання людськими відчуттями, довірою та невігласністю, тому важливо усвідомлювати ці загрози та вміти розпізнавати їх.

Відсутність навчання у персоналу та/або недооцінка важливості ІБ призводять до недотримання політики ІБ, правил внутрішнього контролю, недбалого ставлення до захисту інформації, неправильних дій в потенційно небезпечних ситуаціях.

Використання слабких паролів, поганої автентифікації, відсутність шифрування для збережених паролів ускладнює захист інформації. Зловмисник може значно легше отримати доступ до системи, якщо паролі не є достатньо складними і не використовується двофакторна автентифікація.

Відсутність чіткої системи ролей та прав доступу в компанії, що призводить до того, що співробітник отримують доступ до інформації, яка не відповідає їхнім обов'язкам і потребам. Під час зміни посади або звільнення працівника може не відбуватися зміна прав доступу, що призведе до того, що колишній працівник все ще має доступ до конфіденційної інформації після того, як він покинув організацію. Брак автоматизованих систем управління доступом може призвести до того, що процеси призначення та скасування прав доступу відбуваються з помилками або затримками, що ще більше збільшує ризик порушень безпеки.

Недостатність (відсутність) моніторингу та аудиту доступа ускладнює виявлення як недозволених і неправомірних дій співробітників, так і

зловмисників, котрі можуть маніпулювати співробітником або навіть мати доступ до його акаунту. Без системи контролю за діями користувачів майже неможливо виявити всі порушення безпеки.

Також стрімкий розвиток та доступність генеративного штучного інтелекту призводять до того, що у зловмисників є можливість отримувати фейкові фотографії, чеки, веб-сторінки, підробляти голос тощо.

Висновки до розділу 1

Соціальна інженерія - це мистецтво маніпуляції людьми з метою отримання конфіденційної інформації або доступу до систем безпеки, часто використовуючи методи обману і психологічного тиску, тобто на відмінну від інших атак, в атаках СІ головний вплив йде на людину (персонал), а саме зловмисники використовують довіру та недбалість. Так званий людський фактор неможливо знизити до мінімуму, використовуючи лише програмні і апаратні засоби, тому що головною зброєю зловмисника є психологічні методи, які вдало використовуються для вводу в оману потенційних жертв. Атака СІ здійснюється поетапно і починається зі збору інформації, яка буде використовуватися для маніпулювання потенційною жертвою і створення правдоподібної легенди, потім здійснюється перший контакт, який не повинен викликати підозри. Пізніше отримують довіру жертви, котра добровільно надає доступ до конфіденційної інформації, приміщень, фінансових рахунків, потім здійснюється максимально непомітний вихід з гри. В подальшому отриманий доступ використовується зловмисником в злочинних цілях. Саме тому важливо розуміти наскільки небезпечними є атаки СІ.

У світі, де активно використовується соціальна інженерія для атак на інформаційний простір необхідно постійно навчати персонал розпізнаванню таких атак і правильному реагуванню на них. Персонал не зможе протистояти атакам без навчання і розуміння того, як треба діяти в подібних ситуаціях. Для запобігання цього потрібно проводити тренінги та постійно піднімати

обізнаність та кваліфікованість персоналу. Також, важливим фактом для зменшення впливу людського чиннику на захищеність ІП потрібно розвивати і підтримувати культуру ІБ в суспільстві.

РОЗДІЛ 2 РІЗНОВИДИ АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ ТА МЕТОДИ ЗАХИСТУ ВІД НИХ

2.1 Різновиди атак з соціальної інженерії

Атаки соціальної інженерії можуть виконуватися у різних форматах, але всі вони спрямовані на маніпуляцію людьми для отримання конфіденційної інформації або доступу до систем. Дослідивши такі джерела інформації, як статті стосовно соціальної інженерії від постачальників анти-вірусного ПЗ Eset [10], Zillya [11], Державної служби спеціального зв'язку та захисту інформації України [12], Вікіпедії [13], наукові роботи [14, 15] можна класифікувати атаки СІ за такими факторами, як засоби атаки, соціальне відношення до об’єкту атаки, отриманий рівень доступу до ІС, що відображено на рис. 2.1. та видами атак на рис. 2.2.

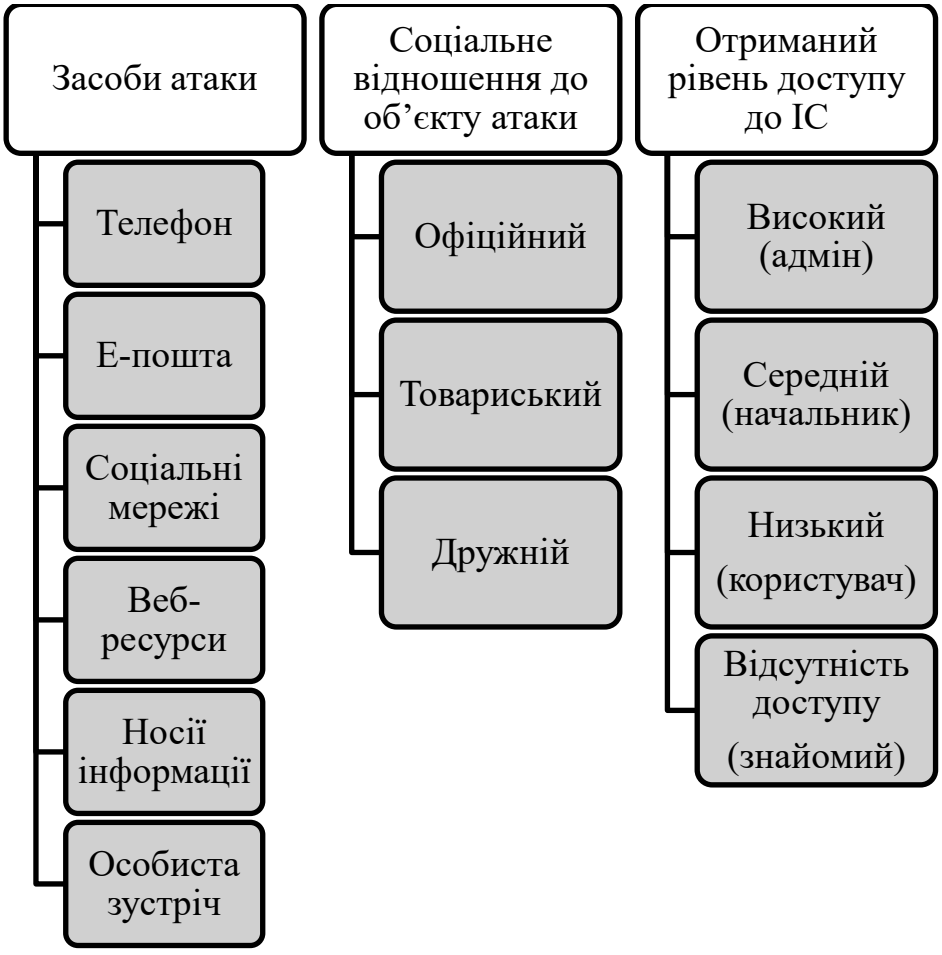

Рис. 2.1. Класифікація атак СІ

Засоби атаки. При використанні телефону основну складність становить голос. Якщо об'єкт знайомий з тим, ким зловмисник представляється, то необхідно зробити так, щоб ваш голос майже не відрізнявся від його голосу, що зазвичай досягається за допомогою ШІ. У разі використання електронної пошти, соцмереж, веб-ресурсів проблема голосу відпадає, натомість з'являється необхідність у максимальній відповідності вигляду листа, назви пошти відправника, візуальна відповідність фейкового веб-ресурсу, акаунту в соцмережі до оригінального. У разі особистої зустрічі можна впливати тільки на тих людей, які не зможуть стверджувати, що зловмисник не той, за кого себе видає. Звісно, за складних комбінацій може бути використано не один засіб, а, можливо, навіть усі, але зловмисник, який здійснює таку атаку, має бути не просто хорошим, а чудовим психологом.

Соціальне відношення до об’єкту атаки. Для того щоб атака виявилася успішною, потрібно вибрати відповідний стиль спілкування для кожного випадку. При виборі офіційного стилю спілкування неприпустимі нотки зневаги або дружності. Необхідно, щоб усе виглядало так, як має бути. Якщо був обраний товариський тон, то передбачається, що зловмисник володіє недостатньою кількістю інформації про людину, з якою збираєтеся розмовляти. Останній, дружній рівень - найскладніший і найдієвіший вид соціального відношення, але зловмисник повинен вміло володіти великою кількістю інформації.

Отриманий рівень доступу до ІС. У випадках коли зловмисник отримує доступ на рівні адміністратора або начальника результатом атаки гарантовано буде витік конфіденційної інформації, доступ до фінансових рахунків тощо. Отримання доступу на рівні користувача дає змогу зловмиснику впровадити шкідливе ПЗ в ІС. Отримання доступу до людей з кола спілкування адміністратора, начальника або користувача призведе до подальшого збору інформації зловмисником, для подальшого використання в атаках СІ і отримання вищого рівня доступу.

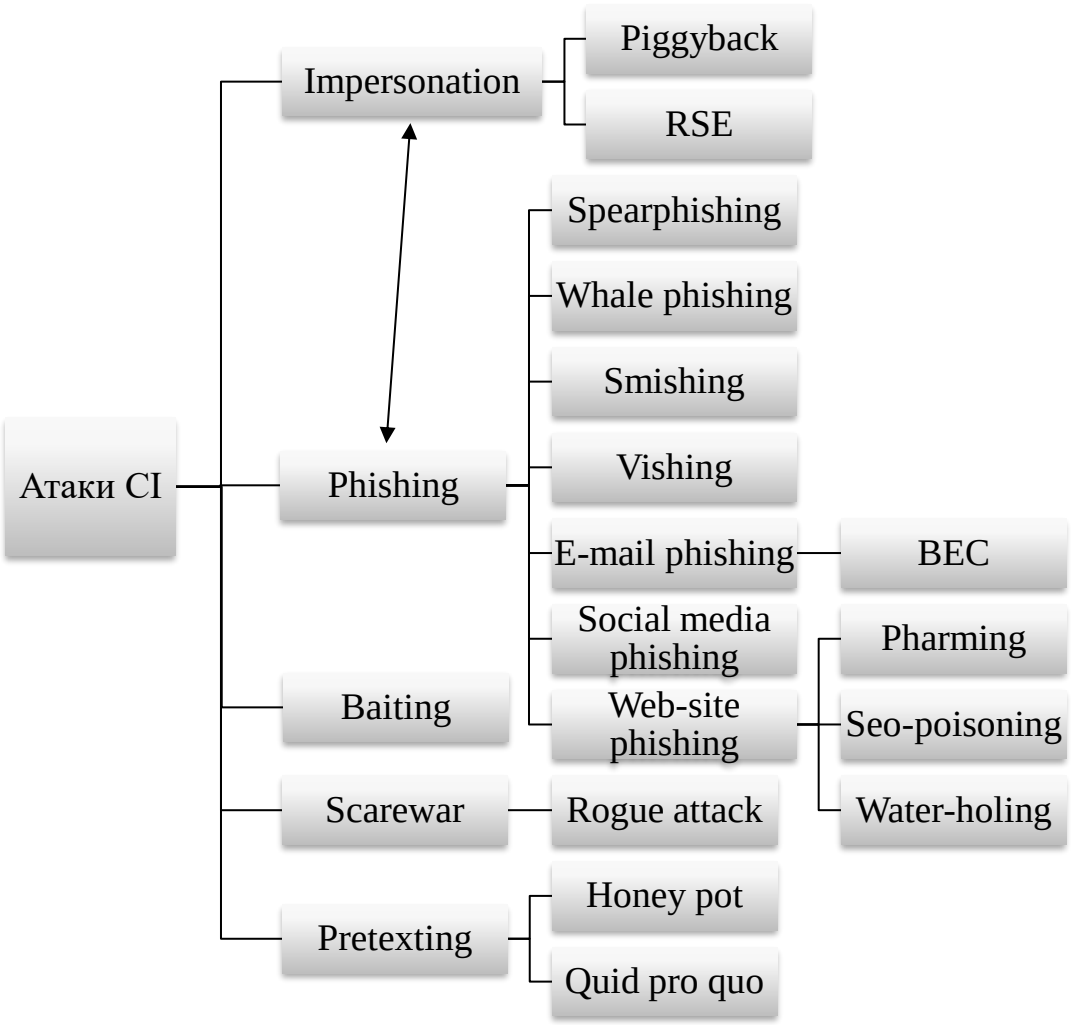

Рис. 2.2. Види атак CI

Impersonation (Імперсонація) - вид атаки CI, коли зловмисник видає себе за іншу особу, як у віртуальному, так і у фізичному середовищі, з метою отримання конфіденційної інформації, доступу до систем або здійснення інших шкідливих дій.

Piggyback (“Катання на спині”) - вид атаки CI, коли зловмсиник отримує доступ до приміщення, що охороняється, слідуючи за кимось із картою доступу. Мається на увазі, що зловмисник уже є “другом” співробітника з привілейованим доступом і проходить разом з ним у заборонену зону.

RSE (Зворотня соціальна інженерія) - вид атаки CI, коли потенційна жертва сама передає потрібні зловмиснику дані. У таких атаках додається новий етап: підлаштування труднощів потенційній жертві. Наприклад, зловмисник влаштовується на роботу прибиральником в охороняєму зону, на стіні з номером

техпідтримки вказує власний контакт замість правильного номера, створює апаратну або програмну проблему потенційній жертві та очікує дзвінка від засмученого співробітника, який готовий передати буквально всю інформацію, бо покладається на компетентність техпідтримки і вважає, що фахівець і так все це знає. Проблеми авторизації можна виключити, бо користувач сам ідентифікує вас, як йому зручніше, залишається тільки підіграти [13].

Phishing (Фішинг) - найпоширеніший вид атаки СІ, призначений для отримання конфіденційної інформації, такої як імена користувачів, паролі, номери кредитних карток, шляхом обману та використання підроблених веб-сайтів, електронних повідомлень тощо. Назва phishing походить від fishing - рибна ловля або вивудження і password - пароль, тобто мається на увазі витягування пароля. Є багато різновидів фішингу відповідно до того на кого направлена атака та яка легітимна інформація або інформаційний ресурс підробляється зловмисником.

Spearphishing (Цільовий фішинг) - різновид фішингу, котрий спрямований на конкретну особу або групу людей. Під час риболовлі з гарпуном ви спрямовуєте його на конкретну рибу. Звідси і назва. На відміну від масованих фішингових атак, які розсилаються на широку аудиторію, цей метод є персоналізованим і продуманим. Тому спочатку зловмисник збирає детальну інформацію про свою ціль, щоб подальша взаємодія мада максимально правдоподібний вигляд.

Whale phising або Whaling (Китобійний фішинг) – різновид фішингу схожий на цільовий, різниця полягає в тому, що атака націлена на високпосадовців, таких як гендиректор, фіндиректор, топ-менеджер тощо. Наприклад, Tessian (компанія яка надає послуги захисту від атак соціальної інженерії) у листопаді 2020 року повідомила про атаку на співзасновника австралійського хедж-фонду Levitas Capital. Співзасновник отримав електронний лист, що містив підроблене посилання в Zoom, яке впровадило шкідливе ПЗ в корпоративну мережу хедж-фонду і майже призвело до виведення 8,7 мільйона доларів США на рахунки шахраїв. Зрештою зловмисник зміг роздобути лише 800 000 доларів США, однак

репутаційний збиток, який послідував за цим, призвів до втрати найбільшого клієнта хедж-фонду, що змусило його закритися назавжди [16].

Smishing (SMS-фішинг) - різновид фішингу, коли зловмисник використовує SMS-повідомлення, які виглядають, як офіційні повідомлення від банків або інших компаній. Зазвичай такі повідомлення (рис. 2.3) містять посилання на фішингові сайти або нібито офіційний номер служби підтримки банку тощо.

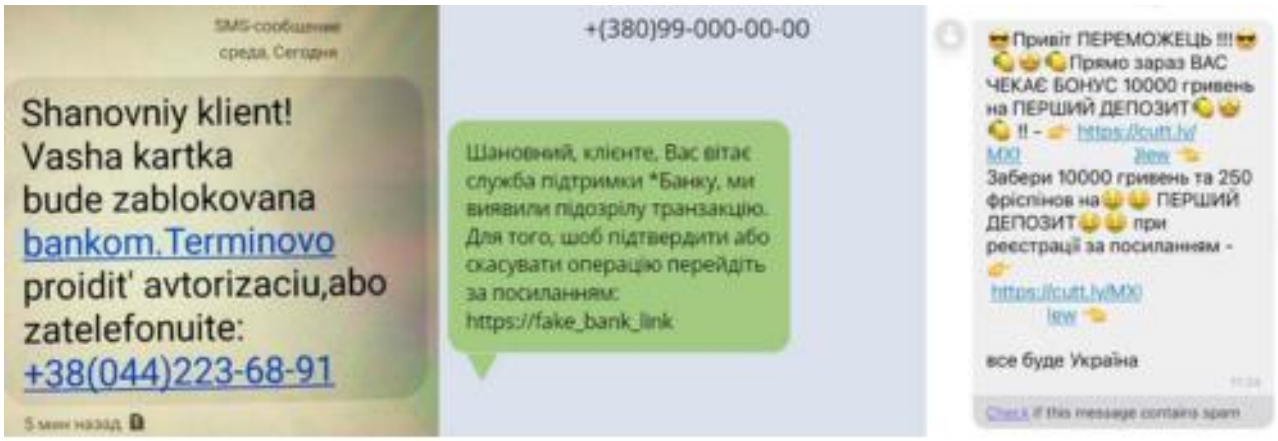

Рис. 2.3. Фішингові SMS-повідомлення

Vishing (Голосовий фішинг) - різновид фішингу, коли зловмисник використовує телефонні дзвінки і видає себе за співробітника банку або родича потенційної жерти і намагається отримати фінансову інформацію або грошовий переказ.

E-mail phishing (Фішинг через електронну пошту) - різновид фішингу, коли зловмисник використовує електронні листи схожі на ті, що відправляють відомі компанії або організації. В подібних листах міститься посилання на фішинговий веб-сайт, котрий вимагає ввести свої особисті дані, або файли, які містять шкідливе ПЗ. Для того, щоб впевнитися у тому, що електронний лист підроблений треба уважно проаналізувати адресу з якої він був відправлений. Електронна поштова адреса виглядає наступним чином: “<ім’я ящика>@<доменне ім’я>”. Слід звернути увагу, що можуть буду поштові адреси з однаковим ім’ям, але різним доменним ім’ям. Наприклад, легітимна адреса “reklama@**ukr**.net” і фішингова “reklama@**ykr**.net”.

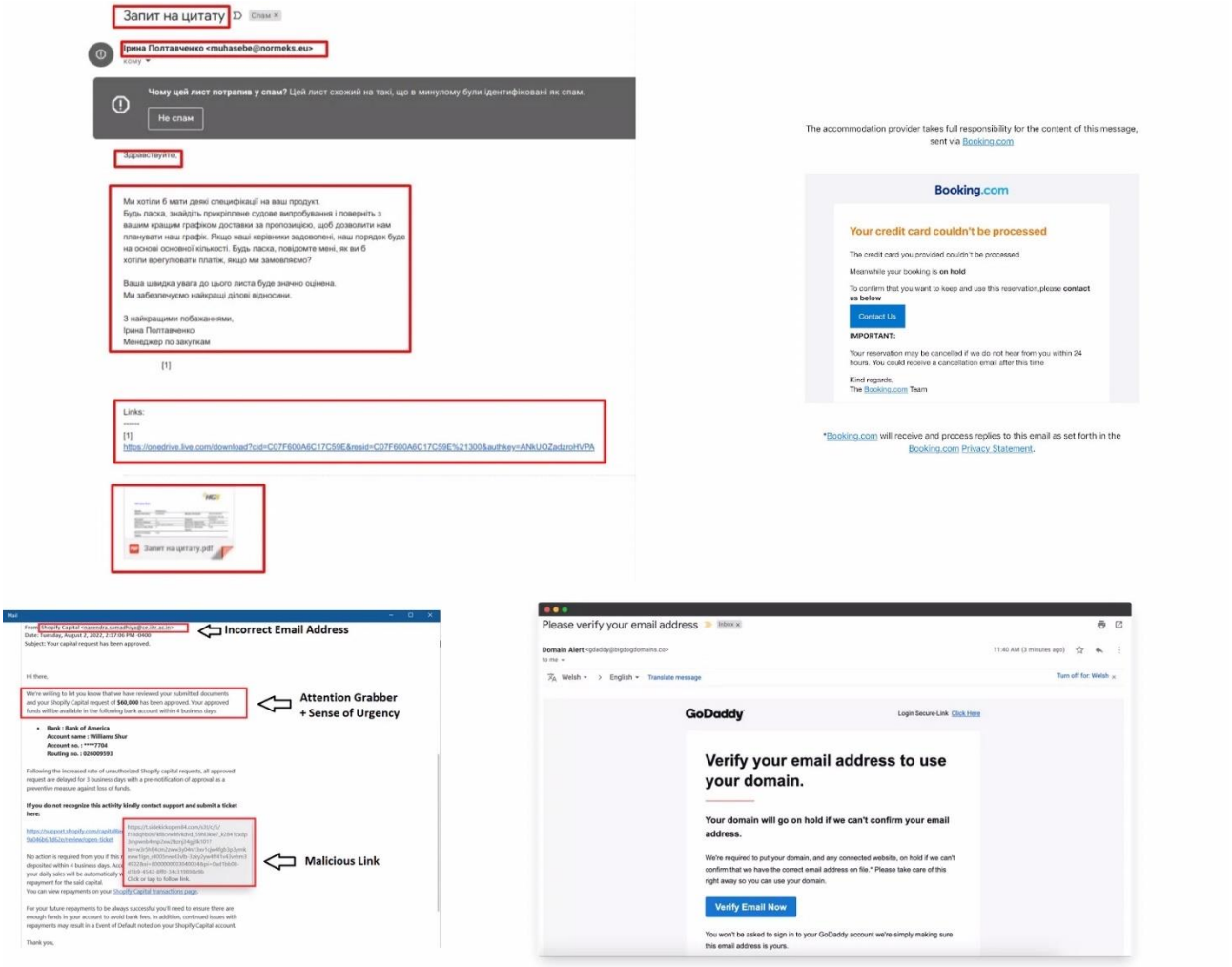

Рис. 2.4. Фішингові електронні листи

BEC (Компрометація ділової електронної пошти) - це різновид фішингу через електронну пошту. Під час BEC-атаки зловмисник фальсифікує повідомлення електронної пошти, щоб змусити жертву виконати певну дію - найчастіше це переказ грошей на рахунок, який контролює зловмисник. BEC-атаки відрізняються від інших типів атак на основі електронної пошти в кількох ключових аспектах: відсутність шкідливого програмного забезпечення, шкідливих посилань або вкладень в електронних листах, націлені на конкретну особу в організації і передбачають поглиблене дослідження інформації перед атакою. BEC-атаки є особливо небезпечними, оскільки вони не містять шкідливого програмного забезпечення, шкідливих посилань, небезпечних вкладень або інших елементів, які можуть бути виявлені фільтром безпеки електронної пошти. Електронні листи, що використовуються в BEC-атаках,

зазвичай не містять нічого, окрім тексту, що допомагає зловмисникам маскувати їх у звичайному електронному трафіку.

Social Media Phishing (Фішинг через соціальні мережі) - різновид фішингу, коли зловмисник використовує підроблені профілі в соціальних мережах або скомпрометовані акаунти для розповсюдження фішингових посилань або шкідливого ПЗ через приватні повідомлення, бесіди (групи), коментарі.

Web-site phishing (Фішинг через веб-сайти) - різновид фішингу, коли зловмисник використовує підроблений веб-сайт. Такі сайти можуть бути майже точною компією легітимних сайтів державних організацій, соціальних мереж, банків, інших крупних компаній. Через них зловмисники отримують логіни і паролі користувачів. Є декілька варіантів як потенційні жертви попадають на такі сайти, окрім посилань отриманих через SMS та E-mail фішинг, а саме:

- Pharming (Фармінг). Користувача автоматично перенаправляє на фішинговий сайт, навіть якщо він зайшов за перевіреним посиланням. Це відбувається через вірус, який встановлює шкідливий код на DNS-сервер.
- Seo-poisoning (SEO-отруєння). Фішингові сайти будуть у перших строках видачі пошукового запросу. Це досягається завдяки технікам пошукової оптимізації (SEO), такі як використання популярних ключових слів, створення великої кількості зворотних посилань та інших методів, щоб підняти рейтинг у пошукових системах.
- Water-Holing (“Водопій”). Заражаються сайти, які часто відвідує цільова група. Шкідливий код перенаправляє потенційних жертв із легітимних сайтів на фішингові.

Baiting (Приманка) - вид атаки CI, коли розрахунок робиться на цікавість потенційної жерти. Зловмисник навмисно залишає заражені шкідливим ПЗ пристрої, такі як USB-накопичувачі, в місцях, де їх обов'язково знайдуть (наприклад, на столі жертви, біля кофемашини, в місці для паління тощо). Жертва заковтує наживку і вставляє флешку до комп’ютера, внаслідок чого відбувається встановлення шкідливого ПЗ. Ще один вид наживок поширюється

через інтернет. Потенційним жертвам пропонується приваблива реклама, яка насправді веде на шкідливий сайт і спонукає користувачів завантажувати заражений шкідливим ПЗ “безкоштовний застосунок, котрий допоможе заробити мільйони”. Зазвичай така атак комбінується зі Scareware-атакою.

Scareware (Лякалка) - вид атаки CI, суть якої полягає в залякуванні жертви лякають, найчастіше спливаючими вікнами під час відвідування шкідливих сайтів. змушуючи думати, що комп’ютер потенційної жертви заражений шкідливим ПЗ або ж має завантажений нелегальний контент. Через деякий час, пропонується вирішення фіктивної проблеми, приклади зображені на рис. 2.3. Однак насправді та програма, яка пропонується потенційній жертві під виглядом антивірусу, являє собою шкідливе ПЗ, метою якого є отримати доступ до особистої інформації жертви. Лякалки використовують психологічний метод навіювання, викликаючи страх користувача і підштовхуючи його до встановлення, начебто, антивірусного ПЗ.

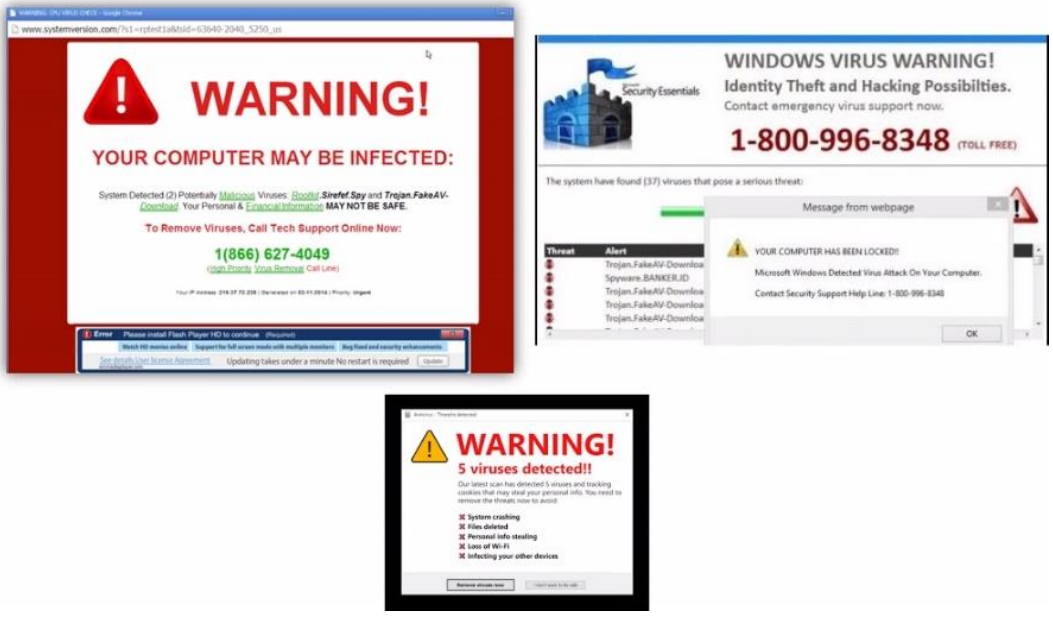

Рис. 2.5 Приклади Scareware

Rogue Attack (Розбійницька атака) - різновид Scareware атак. На комп’ютер потенційної жертви під приводом безпеки встановлюється шкідливе ПЗ, а зловмисник переконує жертву, що це програмне забезпечення повністю законне і безпечне. Встановлена програма потім створює спливаючі вікна та сповіщення, які радять жертві виконувати певні дії. Спливаючі вікна зазвичай показують

кілька варіантів угоди (з різними сценаріями), однак натиснувши на будь-який із цих варіантів призведе до того, що дія зловмисник виконуються від імені жертви.

Pretexting attack (Претекстинг) - вид атаки СІ, зазвичай зловмисник є недобросовісним співробітником, який вдає, що йому потрібна конфіденційна інформація від жертви для виконання важливого робочого завдання. Використовується психологічний вплив, який виглядає дуже природньо.

Quid pro quo (лат. “Послуга за послугу”) - різновид претекстингу, зловмисник надає жертві якусь послугу, допомогу з роботою і натомість просить послугу у відповідь, завдяки якій отримує доступ до акаунту жертви.

Honey Pot (“Горщик меду”) - різновид претекстингу, принцип атак типу полягає в тому, що зловмисник знайомиться з жертвою і прикидається, що відчуває до неї певний інтерес, почуття. Поступово зав'язуючи “стосунки”, які жертва починає сприймати всерйоз. А зловмисник намагається отримати доступ до комп’ютера жерти, збирає конфіденційну інформацію, яка потім може бути використана, наприклад, для злому акаунтів у соцмережах, електронної пошти тощо.

2.2 Статистичні дані щодо атак соціальної інженерії

Атаки СІ є однією з найбільших загроз у сфері кібербезпеки. Про це свідчать дослідження компаній, які займаються статистикою кібератак, державних компаній, дистриб’юторів в області захисту інформації. Кількість та успішність атак СІ почали активно зростати з пандемії COVID у 2019 році. Також спостерігається ріст використання генеративного ШІ для здійснення таких атак. А основною метою є фінансова вигода.

Ізумі Накаміцу, заступник Генерального секретаря ООН з питань роззброєння в інтерв’ю Associated Press заявила, що пандемія COVID-19 рухає світ до посилення технологічних інновацій та онлайн-співпраці, але “кіберзлочинність також зростає: під час нинішньої кризи кількість фішингу за допомогою електронних листів збільшилася на 600%” [17].

У звіті ENISA (Агентства Європейського Союзу з питань мережевої та інформаційної безпеки) за період з січня 2019 року по квітень 2020 року [18] надаються наступні дані щодо фішингових спам-розсилок:

- 85% від усіх електронних листів, якими обмінювалися у квітні 2019 року, були фішиноговим спамом, що є 15-місячним максимумом;
- 58,3% поштових скриньок пов’язаних з майнінгом криптовалюти були атаковані;
- 10% від загальної кількості виявлених фішингових спам-розсилок були націлені на німецькі поштові скриньки;
- 13% витоків даних були спричинені фішингової розсилкою;
- 83% компаній були незахищені від BEC-атак;
- 42% начальників відділів інформаційної безпекит (CISO) мали справу принаймні з одним інцидентом, пов’язаний із фішиногою спам-розсилкою.

Щодо фінансових витрат згідно з даними ФБР, у 2021 році жертви атак зазнали збитків на суму понад 54 мільярди доларів. Найбільша атака із використанням засобів соціальної інженерії, була здійснена громадянином Литви Евалдасом Римасаускасом проти двох найбільших веб-корпорацій світу: Google та Facebook. Римасаускас і його команда створили фальшиву компанію та видавали себе за виробника комп'ютерів, який співпрацював з Google та Facebook. Римасаускас також відкрив банківські рахунки на ім’я компанії. В результаті веб-гіганти зазнали сукупних збитків на суму понад 120 мільйонів доларів [19].

У січні 2022 року сталась масштабна фішингова атака з метою викрадення облікових даних з сервісу Office 365. Зловмисникам вдалося успішно імітувати повідомлення від Міністерства праці США (DoL). У даному випадку адреси з реальним доменом dol.gov підмінялися адресами з попередньо придбаних зловмисниками доменів dol-gov.com і dol-gov.us. При цьому фішингові електронні листи успішно проходили через шлюзи безпеки цільових організацій. У електронних листах використовувалися офіційні атрибути DoL, а самі листи

були написані професійно, запрошуючи отримувачів прийняти участь у торгах за державним проектом. Інструкції щодо торгів були включені в трьохсторінковий PDF-файл з вбудованою кнопкою “Прийняти участь”. При переході за посиланням жертви перенаправлялися на фішинговий сайт, який виглядав ідентично реальному сайту DoL. Сайт підроблених торгів пропонував користувачам ввести свої облікові дані Office 365 і навіть відображав повідомлення про помилку після першого введення. Таким чином, гарантувалося, що жертва введе свої облікові дані двічі, що зменшувало ймовірність помилкового введення [20].

Слід зазначити, що значна кількість спроб подібних атак блокується ще на етапі електронних повідомлень. За інформацією Google Gmail блокує більше 100 мільйонів спроб фішингу щодня [21], а також більше 100 рекламних повідомлень в секунду [22], що розміщені на сайтах, значна частина такої реклами містить шкідливе ПЗ. Попри це, Gmail (безкоштовний провайдер е-пошти) найчастіше використовується у BEC-атаках згідно щоквартальних звітів APWG (рис. 2.6). Антифішингова робоча група (APWG) - міжнародна коаліція фахівців по боротьбі з кіберзлочинністю, судових слідчих, правоохоронних органів, технологічних компаній, фірм, що надають фінансові послуги, університетських дослідників, неурядових організацій та багатосторонніх договірних організацій, що діють на некомерційній основі.

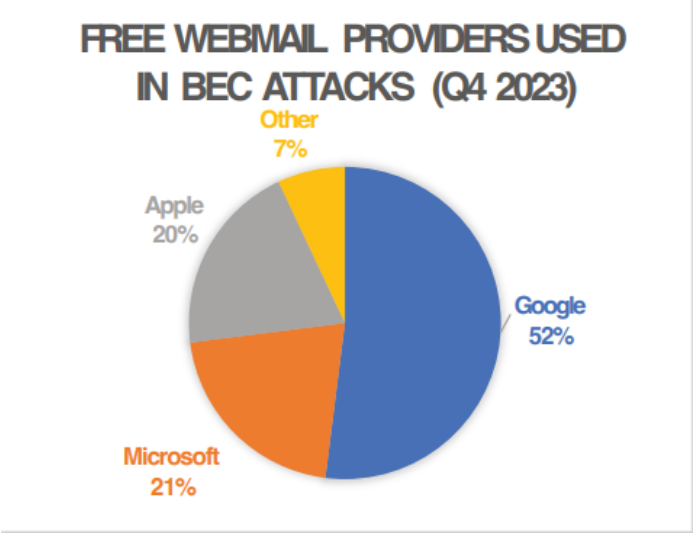

Рис. 2.6. Статистика використання поштових провайдерів у BEC-атаках

У звіті за останній квартал 2023 року [23] зазначено, що APWG виявило більше мільйону унікальних фішингових атак, з яких 42,8% - атаки через соціальні мережі. Також спостерігається зростання кількості гібридних атак:

8% BEC-атаки - це комбінація імперсонації, цільвого фішингу та фішингу через е-пошту;

6,1% поєднання голосового фішингу та фішингу через е-пошту, ціль таких атак обійти двофакторну автентифікацію;

також поєднання Ransomware та фішингу через е-пошту, за різними джерелами від 45% до 85% вірусів-вимагачів потрапляють на комп'ютери жертв за допогою е-пошти.

2.3 Роль соціальної інженерії в когнітивній війні

Такий термін як «війна світоглядів» (Weltanschauungskrieg) почав використовуватися ще у нацистській Німеччині, а в англійській мові його аналог з'явився у 1941 році - «психологічна війна» (Psychological warfare). Термін «когнітивна війна» (Cognitive warfare) у сучасному значенні почали використовувати у Сполучених Штатах у 2017 році для опису способів дій, доступних державі або впливовій групі, яка прагне «маніпулювати механізмами пізнання ворога або населення, щоб послабити, впливати підпорядкувати й зруйнувати його» [24].

У когнітивній війні людська свідомість стає полем бою, а основним інструментом є соціальна інженерія. По суті, у сучасному світі когнітивна війна - це масована фішингова атака через соціальні мережі та веб-сайти з новинами, яка націлена на населення усієї країни. Та її мета - вплив на індивідуальну і групову думку, поведінку на користь тактичних або стратегічних завдань агресора.

Хоча слід зазначити, що можуть використовуватись не тільки фейкові новини для досягнення цілей когнітивної війни, як стверджують науковці з університету Джонса Гопкінса та Імперського коледжа Лондона у свої статті на сайті НАТО [25]. Для провокування незгоди достатньо делікатного урядового

документа, викраденого з електронної пошти державної посадової особи, анонімно завантаженого на відкритий сайт соціальної мережі, або вибірково злитого опозиційним групам через соціальну мережу.

У розслідуванні The Washington Post 2023 року [26] представлені документи, які показують, як у січні 2023 року перший заступник глави адміністрації кремля Сергій Кирієнко доручив групі чиновників і політтехнологів забезпечити присутність в українських соціальних мережах для поширення дезінформації. Основним методом обрали розвиток "мережі Telegram-каналів у поєднанні з Twitter і Facebook/Instagram" як найефективніший спосіб проникнення в медіапростір України, але слід зазначити, що активно використовується і канали у Tik-Tok. Також Кирієнко сформулював чотири ключові завдання пропагандистської команди рф:

- дискредитація військового і політичного керівництва Києва;
- розкол української еліти;
- деморалізація українських військ;
- дезорієнтація українського населення.

Методи ведення когнітивної війни в рф ґрунтуються на підходах рефлексивного управління, започаткованого В. Лефевром (1936-2020), радянсько-американським психологом і математиком. Рефлексивне управління - це теорія та практика впливу на свідомість, емоції та поведінку противника або партнера за допомогою спеціально підготовленої інформації, яка спонукає його до прийняття бажаного рішення. Елементами такого підходу є:

- відволікання уваги (створення реальної чи уявної загрози життєво-важливим тиловим позиціям противника під час підготовчої стадії воєнних дій);
- перевантаження (за рахунок великої кількості суперечливої інформації);
- параліч (створення уявлення про загрози життєво-важливим інтересам чи найслабшим місцям);
- виснаження (примушення противника виконувати марні дії);
- обман (провокування противника передислокувати збройні сили до

“загрозливого” регіону);

•розкол (переконувати супротивника, що він має діяти всупереч інтересам коаліції);

•заспокоєння (примушення противника вважати, що здійснюється не підготовка до наступальних дій, а навчання або імітація);

•залякування (створення сприйняття непереборної переваги);

•провокація (нав'язування противнику вчинення дій, вигідних для вашої сторони);

•пропозиція (пропонування інформації, яка зачіпає супротивника юридично, морально, ідеологічно тощо);

•тиск (пропонування інформацію, що дискредитує уряд у власних очах населення).

Також у цьому розслідуванні [26] були представлені звіти пропагандистської команди рф щодо успішності кампанії саме за елементом “тиску”(рис. 2.7.).

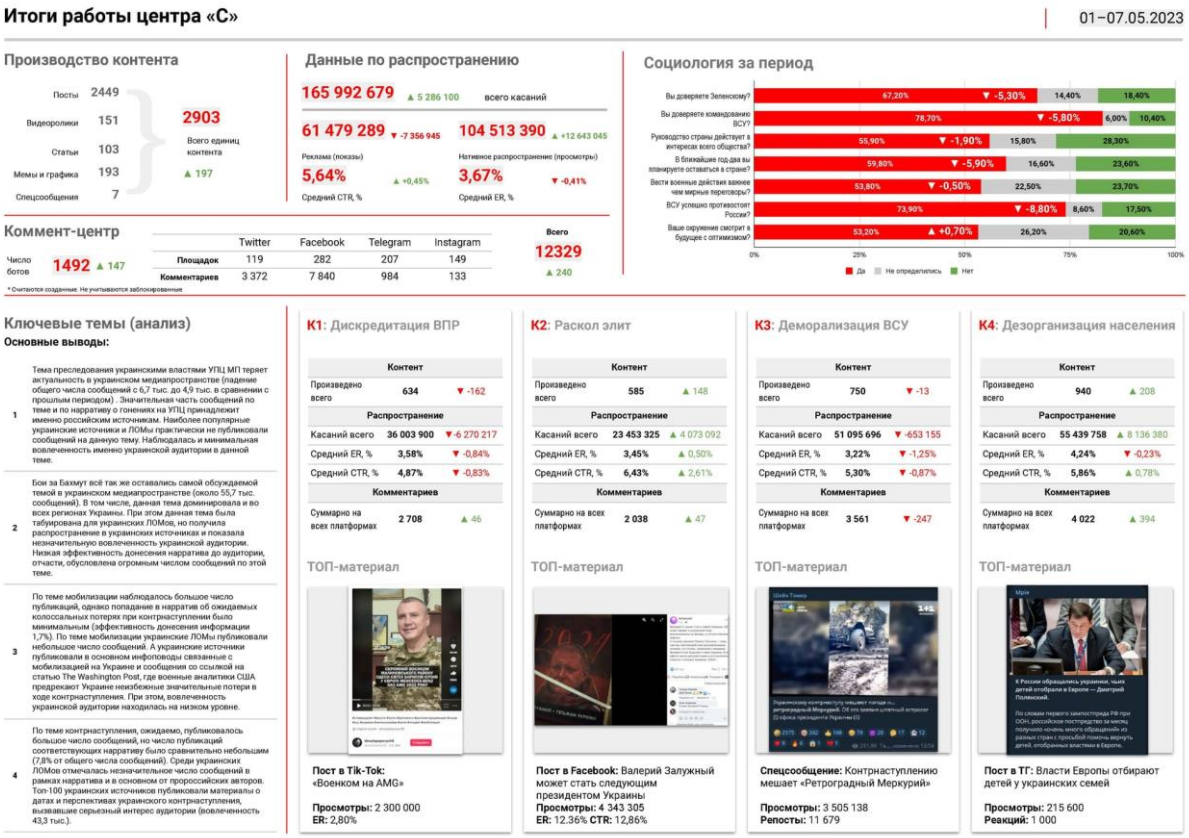

Рис. 2.7. Звіт пропагандистської команди рф

Паралельно пропагандистська команда рф вела кампанію в Західній Європі, для дезінформації населення держав-членів Європейського Союзу та подальшого використання її в Україні. Тактика європейської кампанії включала клонування й узурпацію засобів масової інформації та урядових веб-сайтів, таких як сайти Le Monde і Міністерства закордонних справ Франції, а потім розміщення на них фейкового контенту, що ганьбить український уряд, у рамках операції, названої чиновниками Європейського Союзу **Doppelgänger**. Вони також включали створення фейкових акаунтів політичних діячів у Twitter, зокрема міністра закордонних справ Німеччини Анналени Бербок. В подальшому повідомлення та пости з фейкових акаунтів і веб-сайтів поширювались в українському інформаційному просторі як справжні європейські репортажі. Після того, як у вересні 2023 року фейковий акаунт Baerbock у Twitter заявив, що “війна в Україні закінчиться за 3 місяці”, влада Німеччини почала розслідування і виявила більше ніж 50 000 акаунтів фейкових користувачів, які координували проросійську пропаганду, зокрема й тих, які просували твіт. Фейкові акаунти були продовженням кампанії Doppelgänger.

Слід зазначити важливу роль генеративного ШІ, так у своєму звіті [27] компанія Open AI повідомила, що за зірвали операції прихованого впливу, які намагалися використати моделі ШІ для низки завдань, таких як створення коротких коментарів і довгих статей різними мовами, вигадування імен і біографій для акаунтів у соціальних мережах, проведення досліджень з відкритих джерел, налагодження простого коду, а також переклад і вичитка текстів. А саме:

Операції пропагандистської команди рф, що відома під назвою **Doppelgänger**. Зловмисники використовували моделі ШІ для створення коментарів англійською, французькою, німецькою, італійською та польською мовами, які розміщувалися на Twittet і 9GAG, для перекладу та редагування статей англійською та французькою мовами, які розміщувалися на сайтах, пов'язаних з цією операцією, для створення заголовків і перетворення новинних статей на пости в Facebook.

Операції пропагандистської команди рф про яку раніше не повідомлялося, Bad Grammar, що діяла переважно в Telegram і була націлена на Україну, Молдову, країни Балтії та США. Зловмисники використовували моделі ШІ для створення та налагодження коду для запуску ботів в Telegram і створення коротких політичних коментарів російською та англійською мовами, які потім і публікувалися в Telegram.

Висновки до розділу 2

Соціальна інженерія охоплює широкий спектр атак, спрямованих на використання людського фактору для отримання доступу до конфіденційної інформації та фінансової вигоди. Найпоширенішою атакою соціальної інженерії є фішинг через електронну пошту. За даними з різних джерел, включаючи звіти Google, Microsoft, ENISA, APWG тощо, атаки соціальної інженерії становлять значну частину від усіх кібератак: до 85% випадків порушень безпеки компаній пов’язані з соціальною інженерією. Постійна еволюція атак соціальної інженерії та поява гібридних атак, таких як BEC-атаки, та доступність генеративного штучного інтелекту у сукупності призводить до зростання відсотку успішних атак. Навіть такі веб-гіганти як Google та Facebook зазнають фінансових збитків через атаки соціальної інженерії.

Також, соціальна інженерія відіграє ключову роль в когнітивній війні, оскільки вона використовується для маніпуляції переконань, зміни поведінки та контролю над інформацією. Це може включати дезінформацію, маніпулювання медіа, новинами, соціальними мережами, щоб вплинути на громадську думку та політичні процеси.

Отже, соціальна інженерія є вагомою складовою сучасних кіберзагроз, що вимагає комплексного підходу до захисту інформаційного простору. Кількість різновидів атак соціальної інженерних та їх поширеність підкреслюють необхідність постійного удосконалення заходів безпеки та освіти користувачів щодо виявлення та запобігання таким загрозами.

РОЗДІЛ 3 ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ В ОБЛАСТІ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

3.1 Методи захисту від атак соціальної інженерії

Захист від атак соціальної інженерії включає різноманітні заходи та стратегії, спрямовані на попередження маніпуляцій та забезпечення безпеки інформації. Методи захисту від атак соціальної інженерії можна поділити на 3 основні категорії: технічні, організаційні та освітні заходи (рис.3.1).

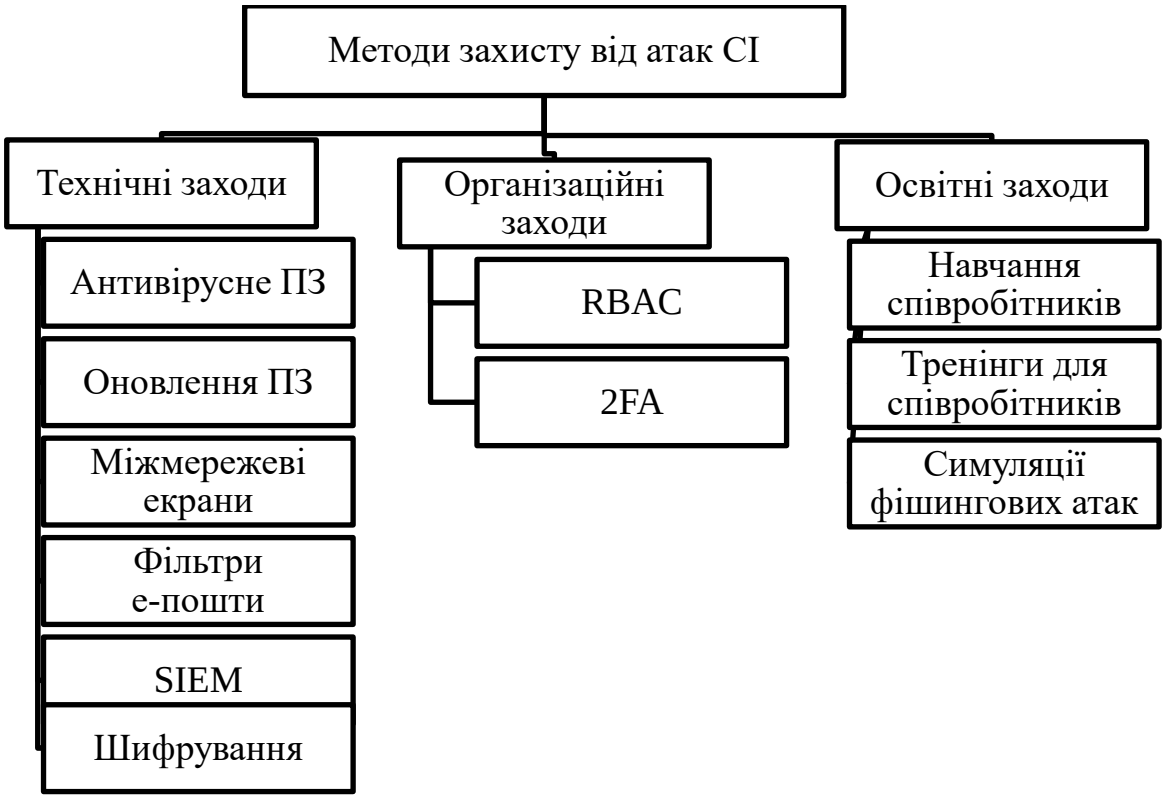

Рис. 3.1 Методи захисту від атак СІ

Технічні заходи - це комплекс програмних і апаратних заходів, які використовуються для захисту інформаційних систем і даних від несанкціонованого доступу, кібератак тощо. До таких заходів належить:

Використання антивірусного ПЗ. Це дозволяє виявляти та блокувати шкідливе програмне забезпечення, включаючи віруси, трояни, шпигунське ПЗ та інші загрози. Такий крок допоможе запобігти наслідків атак СІ, оскільки в разі

успішних атак СІ на комп’ютер жерти може бути встановлене шкідливе ПЗ. Наприклад, Eset, Avast, Comodo, Zillya, 360 Total.

Оновлення програмного забезпечення. Регулярне оновлення ПЗ та операційних систем допомагає усунути відомі вразливості та забезпечити актуальний захист, що зменшить ризик реалізації шкідливого ПЗ в разі успішної атаки СІ.

Використання міжмережевого екрану. Існують як програмні, так і апаратні рішення, що використовуються для контролю та фільтрації вхідного та вихідного мережевого трафіку. Перевірка всіх вхідних з’єднань і запитів забезпечить тільки легітимні з'єднання, а контроль вихідного трафіку використовується для запобігання несанкціонованому передаванню конфіденційної інформації.

Програмні: pfSense, TinyWall, Comodo Firewall, ZoneAlarm, iptables.

Апаратні: Cisco ASA (Adaptive Security Appliance), Palo Alto Networks Next-Generation Firewall, SonicWall Firewall, Fortinet FortiGate.

Використання фільтрів електронної пошти. Виявляють та блокують фішингові листи та спам, використовуючи алгоритми ШІ для аналізу вмісту листів, мають інструменти для автоматичного сортування, маркування, блокування або перенаправлення електронних листів на основі певних критеріїв. Вони можуть бути частиною клієнтських програм або серверних рішень для управління електронною поштою.

Наприклад, SpamAssassin, Postfix, MailScanner, Mozilla Thunderbird, Zoho Mail.

Впровадження SIEM. Security information and event management – це система управління подіями інформаційної безпеки, комбіноване рішення двох систем SIM (Security information management) і SEM (Security event management). Це велика система централізованої обробки даних, здатна аналізувати величезну кількість даних і знаходити інциденти серед великої кількості даних. Являє собою апаратно-програмні рішення. Таке рішення допоможе швидко реагувати на атаки СІ, навіть в разі успішної атаки буде можливість одразу заблокувати скомпроментовані акаунти або фіансові рахунки, що значно зменшить збитки від

атаки. Попри всі плюси, вартість таких систем дуже висока, тому таке рішення можливе не для всіх компаній.

Наприклад, Microsoft Sentinel, Splunk, LogRhythm, IBM QRadar, Google Chronicle, Graylog.

Шифрування фізичних носіїв інформації. Використовуються для шифрування конфіденційних даних шляхом перетворення їх у криптографічно безпечний формат, що значно зменшує ризик витоку інформації, якщо зловмисник в результаті успішної атаки СІ отримав фізичний доступ.

Наприклад, VeraCrypt, BitLocker, AES Crypt, Cryptomator.

Резервне копіювання даних. Регулярне створення резервних копій даних для відновлення у випадку втрати або пошкодження інформації буде ефективним, якщо в результаті успішної атак СІ було встановлено шкідливе ПЗ, яке видаляє або шифрує інформацію.

Наприклад, Redo Backup and Recovery, Cobian Backup, Aomei Backupper, Macrium Reflect Free, Paragon Backup & Recovery, BackUp Maker.

Контроль доступу в будівлю та відеоспостереження. Основні заходи для забезпечення захисту фізичного простору, що значно зменшать успіх атак імперсонації та допоможуть знайти зловмисника.

Організаційні заходи - комплекс управлінських та стратегічних заходів, спрямованих на підвищення свідомості персоналу, створення політик безпеки та впровадження стандартів ІБ.

Створення і впровадження політики безпеки. Це включає встановлення правил, процедур та стандартів спрямованих на попередження та виявлення спроб маніпулювання персоналом з метою отримання несанкціонованого доступу до конфіденційної інформації або систем. Перед створенням політики безпеки проводиться аналіз потенційних загроз та ризиків для інформаційної безпеки, завдяки цьому визначається найбільш вразлива інформація. Після аналізу ризиків створюються документовані правила і вимоги, які визначають, як інформація повинна бути захищена. Це включає в себе такі аспекти, як:

•Доступ. Встановлення правил доступу до інформації (наприклад, ролевий доступ до систем) та контроль доступу (наприклад, двофакторна автентифікація). Ролевий доступ до систем (RBAC - Role-Based Access Control) є однією з основних стратегій управління доступом до інформаційних ресурсів в компаніях або організаціях, він базується на принципі, що доступ до ресурсів повинен бути наданий користувачам на основі їхніх ролей в компаніях або організаціях і працює наступним чином:

Визначається набір ролей у організації, наприклад, адміністратор, начальник, користувач тощо. Кожна роль має свій набір дозволів.

Визначається перелік дій (дозволів), які можуть виконувати користувачі, котрі належать до певної ролі. Наприклад, адміністратор може мати дозвіл на створення, редагування та видалення користувачів, тоді як звичайний користувач може мати лише доступ до читання.

Визначаються правила доступу, деталізація того, які ролі мають доступ до конкретних ресурсів. Наприклад, правило може встановлювати, що тільки адміністратор може мати доступ до всіх ком’ютерів, а звичайні користувачі лише до свого робочого.

Асоціація ролей з користувачами - процес призначення користувачам однієї або декількох ролей. Це дозволяє керувати доступом на основі поточних обов’язків і функцій користувачів у організації.

Переваги використання RBAC включають покращену безпеку, зменшення ризиків людських помилок у керуванні доступом та спрощенну адміністрування ІКС.

Двофакторна автентифікація (2FA) передбачає використання двох різних способів підтвердження ідентичності користувача для доступу до облікового запису або фізичного доступу до системи. Зазвичай це комбінація чогось, що користувач знає (пароль, ПІН-код) і чогось, що він має (мобільний телефон, відбиток пальця, перепустка). Це допомагає у запобіганні атак соціальної інженерії, оскільки навіть якщо зловмисник дізнається пароль, то все одно не зможе отримати доступ без додаткового етапу автентифікації.

•Захист. Вимоги щодо захисту інформації від несанкціонованого доступу під час зберігання і передачі, тобто шифрування, захист мереж і контроль доступу.

•Зберігання. Правила і обмеження щодо зберігання інформації, визначення строків зберігання і процесу утилізації.

•Моніторинг і аудит. Моніторинг активності допомагає виявляти підозрілі дії та надавати швидку реакцію на потенційні загрози ІБ. Цей метод дозволяє системам кібербезпеки постійно моніторити та аналізувати активість користувачів та стан систем, що допомагає вчасно виявляти незвичайні патерни поведінки та попереджувати можливі атаки. Аудит безпеки також є ефективним інструментом захисту, який допомагає компанія або організаціям виявляти та виправляти слабкі місця у їх захисті інформації та систем. Ключові фактори аудиту безпеки як засобу захисту від атак соціальної інженерії:

•Оцінка систем безпеки. Аудитори проводять детальний аналіз систем безпеки, щоб виявити вразливості та можливі ризики.

•Аналіз політики безпеки.

•Перевірка відповідності. Аудит безпеки включає перевірку відповідності компанії або організації до стандартів безпеки та законодавчих вимог.

•Виявлення потенційних загроз. Під час аудиту безпеки виявляються потенційні загрози, пов’язані з соціально-інженерними атаками, такі як недостатня свідомість персоналу, слабкі паролі тощо.

•Рекомендації з покращення. Аудитори надають рекомендації з покращення безпеки, які допомагають зменшити ризики та забезпечити ефективний захист від атак соціальної інженерії.

Слід зазначити, що політика безпеки повинна регулярно оцінюватися і адаптуватися відповідно до внутрішніх процесів компанії або організації, нових загроз та технологій.

Освітні заходи - один з ключових аспектів реалізації захисту від атак соціальної інженерії, включає навчання, тренінги та проведення симуляцій атак з співробітниками.

Навчання співробітників. Регулярне навчання з інформаційної безпеки для усіх працівників компанії або організації значно знижує ризик успішних атак СІ, оскільки більшість методів соціальної інженерії розраховані на користувачів з низьким рівнем обізнаності в ІБ. Цей підхід передбачає систематичне навчання співробітників компанії за допомогою лекцій та відеоматеріалів за наступнимии темами: основи кібербезпеки, соціальна інженерія, фішинг та інші види атак, політика безпеки. Персонал повинен бути ознайомлений з правилами безпеки даних і заходами обережності, такими як не передавати конфіденційну інформацію по телефону або електронній пошті без перевірки автентичності отримувача, має розуміти методи атак, такі як фішинг, імперсонація, бейтінг та знати, як реагувати в разі підозри на такі атаки, повинен дотримуватися встановлених правил корпоративної безпеки, таких як обмеження доступу до конфіденційної інформації лише для авторизованих осіб та використання безпечних паролів. Інформаційні матеріали за цими темами можливо знайти у відкритому доступі, а сам процес навчання може проводитися співробітником компанії, що робить цей метод доступним і ефективним.

Тренінги для співробітників щодо виявлення та запобігання атакам соціальної інженерії. Більш складний і цікавий процес навчання, що має інтерактивну складову. Основними темами є: аналіз атак СІ, здобуття практичних навичок щодо розпізнавання атак СІ, процедури реагування на на підозрілі запити. Персонал повинен бути навчений розпізнавати ознаки можливих атак соціальної інженерії, такі як незвичайні запити на інформацію, неочікувані електронні повідомлення або телефонні дзвінки від невідомих джерел. Компанії можуть встановлювати системи повідомлень про безпеку, які надсилають співробітникам сповіщення про потенційні загрози або нові методи атак соціальної інженерії, щоб підвищити обізнаність персоналу. Після

проведення навчання та тренінгів співробітники повинні пройти тестування для визначення успішності процесу навчання.

Проведення симуляцій реальних атак.

Регулярні симуляції фішингових атак для підвищення обізнаності співробітників. По суті це може бути як внутрішній так і зовнішній аудит за результатами якого може буде визначити чи дійсно персонал компанії вміє застосовувати теоретичні знання на практиці та оцінити реальні ризики людського фактору. Процес симуляції атак має такі етапи:

Планування. Визначення цілей симуляції, вибір методів і сценаріїв, підготовка необхідних інструментів та матеріалів.

Проведення. Реалізація симуляційних атак відповідно до запланованих сценаріїв, моніторинг реакцій співробітників.

Аналіз та звітність. Оцінка результатів симуляцій, аналіз помилок і слабких місць, підготовка звіту з рекомендаціями щодо покращення безпеки.

Зворотний зв’язок та навчання. Обговорення результатів симуляцій зі співробітниками, проведення додаткових тренінгів для усунення виявлених проблем.

Правильно навчений персонал може бути ефективним бар’єром перед атаками соціальної інженерії, що загрожують безпеці даних та ресурсів компанії. Інвестування в навчання та освіту персоналу дозволяє підвищити рівень усвідомленості, покращити навички реагування та створити культуру безпеки всередині організації.

3.2 Огляд реалізації захисту від атак соціальної інженерії

Розглянемо реалізацію захисту від атак соціальної інженерії на прикладі типових поширених атак, будемо враховувати що компанія і її персонал впровадили заходи описані вище.

Impersonation

Атака: зловмисник представляється співробітником компанії та намагається

отримати доступ до приміщень та скопіювати конфіденційну інформацію собі на флешку.

Причини невдачі:

Освітні заходи. Співробітники навчені перевіряти посвідчення всіх осіб, що входять до приміщення, навіть якщо вони виглядають як співробітники.

Політики безпеки. Використання систем контролю доступу, які вимагають електронні картки або біометричні дані для входу в офіс.

Відеоспостереження. Постійний моніторинг входів та виходів з будівлі.

Результат: зловмисника зупинили на вході, і він не зміг отримати доступ до приміщень.

Piggyback

Атака. Зловмисник намагається проникнути в будівлю, слідуючи за справжнім співробітником.

Причини невдачі:

Освітні заходи. Співробітників навчають не пропускати за собою незнайомих людей і повідомляти про підозрілих осіб.

Системи контролю доступу. Вхідні двері оснащені системами, які дозволяють входити лише одному співробітнику за раз.

Результат: зловмисник не зміг проникнути в будівлю, оскільки співробітник дотримався правил безпеки.

RSE

Атака: зловмисник влаштовується на роботу прибиральником в охороняєму зону, на стіні з номером техпідтримки вказує власний контакт замість правильного номера, створює апаратну або програмну проблему потенційній жертві та очікує дзвінка від засмученого співробітника.

Причини невдачі:

Освітні заходи: співробітники навчені розпізнавати можливі ознаки зворотної соціальної інженерії та не повідомляють дані акаунту.

Антивірусне програмне забезпечення: використання антивірусного ПЗ, яке виявляє та блокує шкідливе ПЗ.

Відеоспостереження. Камери всередині офісу на випадок інцидентів.

Результат: зловмиснику не було надано конфіденційної інформаїї, ПЗ від “технічної підтримки” було заблоковано антивірусним ПЗ та зловмисник потрапив на камери при створенні “проблем”.

Spearphishing та Whale phishing

Атака: Цільова фішингова атака на системного адміністратора/директора з використанням персоналізованої інформації.

Причини невдачі:

Освітні заходи. Навчання співробітників розпізнавати персоналізовані атаки.

Фільтри електронної пошти. Використання сучасних фільтрів, що аналізують контекст повідомлень.

Політики безпеки. Впровадження правил щодо верифікації будь-яких незвичайних запитів.

Двофакторна автентифікація. Використання 2FA для додаткового захисту облікових записів.

Результат: атака не спрацювала, оскільки співробітник розпізнав її.

Smishing

Атака: зловмисник відправляє підроблене SMS повідомлення з підозрілого номер, що містять посилання на фішинговий веб-сайт.

Причини невдачі:

Освітні заходи. Співробітників навчено не довіряти SMS-повідомленням з номерів, що не відносяться до компанії. Також після аналізу посилання було виявлено різницу від легітимного джереда.

Фільтри SMS: Використання фільтрів, що блокують підозрілі SMS.

Результат: співробітники не натискали на фішингові посилання, а підозрілі повідомлення були заблоковані.

Vishing

Атака: зловмисник прикидається співробітником служби безпеки банку та намагається отримати інформацію від фінансових рахунків.

Причини невдачі:

Освітні заходи. Навчання співробітників виявляти телефонні шахрайства, не передавати дані від фінансових рахунків.

Політики безпеки. Заборона надавати конфіденційну інформацію по телефону без підтвердження особи.

SIEM. Блокування підозрілих телефонних дзвінків.

Результат: співробітники відмовились надавати інформацію та повідомили про підозрілі дзвінки.

E-mail phishing

Атака: багатьом співробітникам на електронну пошту надійшов фішинговий лист від начебто служби безпеки з вкладеним файлом, який мав інформація стосовно великої кількості входів в скриньку з різних ір-адрес та пропозицію змінити пароль.

Причини невдачі:

Освітні заходи. Співробітники розпізнали типову фішингову атаку і підроблений .pdf файл з посиланням на фішинговий сайт е-пошти.

Фільтри електронної пошти. Використання фільтрів для виявлення та блокування фішингових листів.

Двофакторна автентифікація (2FA). Додатковий рівень захисту.

Результат: атака не спрацювала, оскільки більшість співробітників розпізнала типовий фішинговий лист, а двофакторна автентифікація не дозволила зловмиснику отримати доступ до поштових скриньок.

BEC

Атака: зловмисник відправляє повідомлення на бізнес-електронну пошту зі схожого адресу з різним поштовим доменом від лиця компанії-партнера.

Причини невдачі:

Освітні заходи. Співробітник перевірив легітимність поштової адреси відправник та виявив невідповідність.

SIEM. Було швидко виявлено та заблоковане підозріле повідомлення.

Результат: атака не спрацювала, нелегітмнисть повідомлення було одразу

виявлено.

Social media phishing

Атака: фішинг через соціальні мережі, де зловмисник створив акаунт схожий на директора компанії та попросив надати йому конфіденційну інформацію

Причини невдачі:

Освітні заходи. Співробітників навчено перевіряти та розпізнавати підроблені профілі та повідомлення в соціальних мережах. Було перевірено переписку та знайдено офіційний акаунт.

Політика безпеки. Політика безпеки компанії забороняє ділитися конфіденційною інформацією через соціальні мережі.

Результат: Атака не спрацювала, оскільки співробітники не довіряли підозрілим повідомленням та дотримувались політики безпеки компанії.

Web-site phishing

Атака: зловмисник створює підроблений веб-сайт для перегляду фільмів, який часто відвідують співробітники компанії. Сайт виглядає як справжній, щоб зібрати логіни і паролі на випадок використання таких самих даних в корпоративних акаунтах.

Причини невдачі:

Освітні заходи. Співробітники побачили відсутність захищеного з’єднання з сайтом та розпізнали фейкову адресу.

Політики безпеки. Політика компанії передбачає перевірку веб-сайтів перед введенням будь-якої конфіденційної інформації та використання різних логінів і паролів.

Результат: більшість співробітників не вводили свої дані на підробленому веб-сайті, а отримані зловмисником дані не завдали шкоди компанії через використання різних паролів.

Baiting

Атака: зловмисник залишає заражений USB-накопичувач поряд з офісом

компанії, сподіваючись, що хтось підключить його до свого комп'ютера.

Причини невдачі:

Освітні заходи. Співробітників навчено не підключати знайдені USB-накопичувачі до своїх комп’ютерів.

Антивірусне програмне забезпечення. Використання антивірусного ПЗ, яке автоматично сканує та блокує підозрілі пристрої та шкідливе ПЗ.

Політики безпеки. В компанії діє політика, яка забороняє використовувати незареєстровані зовнішні носії даних.

Результат: жоден зі співробітників не підключив знайдений USB-накопичувач до свого компю’тера. Пристрій було передано до правоохоронних органів.

Scareware

Атака: зловмисник намагається залякати жертву, розмістивши на сайтах, які вона відвідує лякалки про зараження його комп’ютера вірусами.

Причини невдачі:

Освітні заходи. Співробітників навчено розпізнавати scareware і не реагувати на залякування, оскільки в них встановлене антивірусне ПЗ.

Антивірусне програмне забезпечення. Використання сучасного антивірусного ПЗ, яке захищає від лякалок при перегляду сайтів.

Політики безпеки. Політика компанії забороняє самостійно встановлювати ПЗ, цим займається тільки ІТ-відділ.

Результат: жоден зі співробітників не завантажив і не встановив шкідливе ПЗ, оскільки вони розпізнали атаку та дотримувались політики компанії.

Отже, більшості атак СІ можна запобігти завдяки навченості персоналу компанії, а використання технічних засобів захисту допомагає знизити ризик успішного результати атаку майже до 0.

3.3 Рекомендації з реалізації захисту від атак соціальної інженерії

Реалізація захисту від атак соціальної інженерії - це комплексний процес, який повинен мати початок на державному рівні, наприклад через впровадження і популярізацію культури ІБ. Це може включати інформування населення про можливі загрози СІ на державних телеканалах і веб-сайтах, на яких повинна розміщуватися інформація з прикладами атак СІ та способами їх розпізнати. Також можуть створюватися боти в мессенджерах та веб-портали з опитуванням.

Основні рекомендацій з реалізації захисту від атак СІ для компаній та організацій:

Займайтесь навчанням персоналу.

Проводьте регулярні навчальні сесії з питань кібербезпеки для всього персоналу. Ці сесії можуть включати лекції, тренінги, вебінари та інші форми навчання. Навчіть співробітників розпізнавати підозрілі повідомлення електронної пошти, соціальних мереж та інших каналів зв’язку, а також навчіть їх, як реагуванню на такі ситуації. Додайте у навчання реальні приклади атак соціальної інженерії, які сталися в інших компаніях. Це допоможе персоналу краще розуміти загрози та їхні наслідки. Також залучайте персонал до участі у симуляціях атак та інших практичних завданнях з кібербезпеки. Важливим моментом є те, що керівництво також має бути зацікавленим у цьому навчанні та займатись заохоченням співробітників до дотримання правил безпеки та активної участі у навчальних заходах. Проходження тестів щодо обізнаності в області захисту від атак СІ для нових співробітників.

Впровадьте та дотримуйтесь політики ІБ.

Для того, щоб вона працювала бездоганно потрібно перш за все провести аналіз ризиків та загроз пов’язаних з СІ. Це допоможе визначити потенційні сценарії атак і визначити найбільш вразливі місця. Не варто забувати ,що політика повинна бути сформована чітко та доступно для всіх співробітників організації. Вона повинна включати правила з обробки конфіденційної інформації, використання паролів, доступу до систем тощо. Працівники повинні бути ознайомлені з політикою безпеки та її важливістю. Треба переглядати та оновлювати політику ІБ, враховуючи зміни в технологіях, загрозах та вимогах

законодавства.

Регулярно проводьте аудит безпеки.

Його основна мета - забезпечити захист інформації та ресурсів організації шляхом виявлення і усунення слабких місць у системі. Аудит включає в себе аналіз і оцінку заходів безпеки, виявлення недоліків і розробку рекомендацій щодо їх виправлення. Атаки соціальної інженерії використовують маніпуляції та обман, щоб отримати доступ до конфіденційної інформації або фінансову вигоду. Під час аудиту безпеки важливо аналізувати не лише технічні аспекти захисту, а й людський фактор, котрий грає найважливішу роль в захисті від атак СІ. Це означає перевірку політик безпеки, проведення навчання персоналу з питань кібербезпеки, а також виявлення та усунення можливих слабкостей в системі, які можуть бути використані зловмисниками для здійснення атак соціальної інженерії.

Розгорніть спеціалізовані системи моніторингу, які можуть аналізувати активність користувачів у реальному часі. Це допомагає виявляти підозрілу, аномальну активність, яка може бути пов’язана з атаками соціальної інженерії. Проведення ретельного аналізу вхідних та вихідних даних з мережі для, такої як великий обсяг неправомірних запитів або спроби несанкціонованого доступу. Налаштуйте системи моніторингу для надсилання автоматичних повідомлень про будь-яку підозрілу активність, що може потребувати додаткового аналізу або реагування.

Не ігноруйте фізичний захист.

Дотримуйтесь пропускного режиму в офісні та серверні приміщення, створіть перепустки для додаткого захисту. Впровадьте відеоспостереження для запобігання несанкціонованого доступу до приміщень та можливості знайти зловмисника в разі успішної атаки.

Висновок до розділу 3

Захист від атак вимагає сукупність заходів, що охоплює як і технічні, так і організаційні моменти. Основними напрямками реалізації захисту включають аналіз систем комунікації, оцінку поведінки користувачів, регулярне навчання з кібербезпеки, моніторинг активності, створення політики безпеки та реагування на інциденти. Загалом, сукупність заходів до захисту від атак соціальної інженерії забезпечить безпеку даних і ресурсів, зменшить ризики кібербезпеки та допоможе підтримувати стабільну роботу.

Дослідження користувачів комп'ютерних систем та проведення аудиту безпеки для визначення актуальних загроз та вразливостей від атак методами СІ є надзвичайно сильним стимулом покращення кібербезпеки. Окрім цього, важливо зменшити вплив людського фактору. Сукупність аналізів щодо загроз та вразливостей та застосування заходів безпеки сильно підвищать рівень захисту комп'ютерних систем від атак методами соціальної інженерії.

Важливо підкреслити, що ефективний захист від атак це не тільки технічні моменти, а ще сукупність заходів стратегій. Навчання персоналу являється одним із ключових моментів в цьому етапі, оскільки досвідчені користувачі зможуть розпізнати підозрілі дії та вчасно на них зреагувати. Не менш важливим є те, що керівництво має активно брати участь у цих заходах та показати важливість цього навчання.

Політика безпеки відіграє не менш важливу роль в захисті від атак соціальної інженерії. Вона повинна бути чіткою, зрозумілою для всієї організації і відображати найновіші стандарти та кращі приклади в галузі кібербезпеки. Постійно оновлюючи політику безпеки з урахуванням нових загроз та технологій допоможе зробити захист ефективнішим.

Тільки застосування наведених методів у комплексі може створити достатньо міцний бар'єр, який захистить від атак соціальної інженерії.

Загальний висновок

Соціальна інженерія займає значне місце в сучасному житті, хоча ми можемо цього не усвідомлювати. Це мистецтво маніпулювання людьми, яке все частіше проявляється в нашому буденному житті. Важливо зрозуміти, що атаки соціальної інженерії працюють через психологічний вплив, тому замало лише технічного захисту. Головною проблемою в боротьбі з цими атаками є низька обізнаність нашого суспільства про методи та загрози соціальної інженерії. Атаки здійснюються поетапно, що ускладнює розпізнавання їх замислу жертвою. Все робиться максимально непомітно і без підозри, що значно підвищує шанси на успіх зловмисників.

Через недостатність інформації та навчання з кібербезпеки великий відсоток атак проходить успішно. Найпопулярнішим і найпоширенішим різновидом атак є фішинг, який має багато способів введення жертв в оману. Основним методом отримання конфіденційної інформації за допомогою фішингу є електронні листи. Зазвичай вони містять підроблені адреси та фальшиві сайти. За даними з різних джерел, таких як Google, Microsoft, ENISA та APWG, атаки соціальної інженерії складають до 85% від усіх видів кібератак. Через постійний розвиток методів атак, збитки зазнають не тільки малі компанії, але й великі корпорації, такі як Google та Facebook.

Соціальна інженерія відіграє важливу роль в інформаційній війні, проявляючись через маніпулювання новинами, медіа та соціальними мережами. Це ускладнює активний спротив суспільства проти таких атак. Атаки соціальної інженерії є значущою частиною кібератак, що спонукає до розробки комплексного захисту інформаційного простору. Кількість різновидів атак та їх постійний розвиток вказує на необхідність постійного вдосконалення захисту.

Захист має включати як технічні, так і організаційні аспекти. Основні методи реалізації захисту інформаційного простору включають аналіз комунікаційних систем, регулярне навчання персоналу, оцінку поведінки користувачів, моніторинг активності, реагування на інциденти та створення

політик безпеки. Ці заходи допоможуть зменшити вплив кібератак на безпеку даних та ресурсів.

Дослідження комп'ютерних систем та впровадження аудиту безпеки для визначення вразливостей є надзвичайно важливим стимулом для покращення кібербезпеки. Зменшення людського фактора також є важливим аспектом. Обов'язковим методом захисту від атак соціальної інженерії є навчання персоналу. Підвищення обізнаності персоналу автоматично підвищує рівень захисту. Співробітники, які добре ознайомлені з видами атак і знають, як на них правильно реагувати, зможуть вдало визначити підозрілі дії та швидко їх усунути.

Політика безпеки повинна постійно оновлюватися, щоб протидіяти новим методам атак. Вона повинна бути чіткою, зрозумілою і доступною для всього персоналу. Без цього працівники не зрозуміють суть методу захисту, що значно підвищить ризик успішного здійснення атаки.

Загалом, боротьба з атаками соціальної інженерії вимагає комплексного підходу, який включає технічні, організаційні та освітні заходи. Лише системний підхід дозволить зменшити ризики та захистити інформаційний простір від сучасних загроз. Кожен елемент захисту повинен працювати в тісній взаємодії з іншими, утворюючи багаторівневу систему безпеки, яка здатна ефективно протистояти атакам соціальної інженерії. Відповідальність за безпеку лежить на кожному працівникові, і лише спільними зусиллями можна досягти високого рівня захищеності.

Отже, через велику кількість атак соціальної інженерії важливо розуміти різновиди атак та способи протидії їм. Це актуально як для окремих осіб, так і для персоналу компаній та організацій. Обізнаність та навченість є головним методом захисту від атак, тому не слід нехтувати важливістю освітніх заходів. Регулярне проведення тренінгів та навчальних сесій, зокрема симуляцій реальних атак, значно підвищує рівень підготовленості співробітників. Працівники, які знають про можливі загрози та як на них реагувати, стають бар'єром на шляху зловмисників.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Митник К. Книга "The Art of Deception: Controlling the Human Element of Security" (Мистецтво обману: Контроль людського елементу безпеки), 2002.ст.278-279.

2. Баззела М. Книга "Open Source Intelligence Techniques",2012. ст 126.

3. Невідомий хакер продає дані 25 процентам користувачів WhatsApp. URL:https://24tv.ua/tech/ua/dannye-millionov-polzovatelej-whatsapp-vystavili-prodazhu_n2204999. (дата звернення:21.04.2024).

4. WhatsApp виклав у інтернет листування мільйонів людей. URL:https://gazeta.ua/articles/science/_whatsapp-vylozhil-v-internet-perepiski-millionov-chelovek/955235. (дата звернення:22.04.2024).

5. Бойман Г. Книга "Information and Communication Technologies in Organizations and Society", 2005. ст.79-81.

6. Про основні засади забезпечення кібербезпеки України Документ 2163-VIII, чинний, поточна редакція — Редакція від 04.04.2024.

7. Інформаційна безпека держави як елемент соціокультури. URL:https://aspects.org.ua/index.php/journal/article/view/720. (дата звернення:27.04.2024).

8. Поради (рекомендації) щодо створення КСЗІ в ІКС, які використовуються для надання послуг доступу до мережі Інтернет.

URL:https://cip.gov.ua/ua/news/poradi-rekomendaciyi-shodo-stvorennya-kszi-v-its-yaki-vikoristovuyutsya-dlya-nadannya-poslug-dostupu-do-merezhi-internet. (дата звернення:30.04.2024).

9. Що таке комплексна система захисту інформації (КСЗІ). URL:https://zahyst-ua.com/korisna-informaciya/shho-take-kompleksna-sistema-zahistu-informacii-kszi/. (дата звернення:30.04.2024).

10. Соціальна інженерія.Низка не технічних прийомів маніпулювання користувачами, які використовуються кіберзлочинцями під час атак. URL:https://www.eset.com/ua/support/information/entsiklopediya-ugroz/sotsialnaya-inzheneriya/. (дата звернення:01.05.2024).

11. Соціальна інженерія або маніпуляції свідомістю.URL: https://zillya.ua/sotsialna-inzheneriya-abo-manipulyatsi-svidomistyu. (дата звернення:01.05.2024).

12. Соціальна інженерія. URL:https://uk.wikipedia.org/wiki/. (дата звернення:01.05.2024).

13. Перелік категорій кіберінцидентів. URL:https://www.cip.gov.ua/ua/news/perelik-kategorii-kiberincidentiv. (дата звернення:01.05.2024).

14 . Дослідження методів соціальної інженерії та їх впливу на здоров'я людини. URL:https://card-file.ontu.edu.ua/items/363521b0-4d44-406c-85ad-472906b9b81d. (дата звернення:02.05.2024).

15. Публікація: Протидія методам та засобам соціальної інженерії. URL:https://openarchive.nure.ua/entities/publication/8c9c920b-4f74-460a-9e3c-bd50dcaa9654. (дата звернення:02.05.2024).

16. Що таке китобійний промисел? Пояснення китобійних електронних атак.URL:https://www.tessian.com/blog/whaling-phishing-attack/.(дата звернення:04.05.2024).

17. Останнє: ООН попереджає про зростання кіберзлочинності під час пандемії.URL: https://apnews.com/article/6ba6af57fd96e25334d8a06fcf999e7f. (дата звернення:07.05.2024).

18. Звіт ENISA (Агентства Європейського Союзу з питань мережевої та інформаційної безпеки) за період з січня 2019 року по квітень 2020 року щодо фішингових спам-розсилок.URL: https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/etl-review-folder/etl-2020-spam. (дата звернення:07.05.2024).

19. Литовця засуджено до 5 років ув'язнення за крадіжку понад 120 мільйонів доларів у шахрайській схемі компрометації бізнес-електронної пошти.URL: https://www.justice.gov/usao-sdny/pr/lithuanian-man-sentenced-5-years-prison-theft-over-120-million-fraudulent-business. (дата звернення:08.05.2024).

20. Свіжий фіш: фішери заманюють жертв фальшивими запрошеннями взяти участь у торгах на неіснуючі федеральні проекти.URL: https://www.inky.com/en/blog/fresh-phish-phishers-lure-victims-with-fake-invites-to-bid-on-nonexistent-federal-projects. (дата звернення:08.05.2024).

21. Gmail блокує понад 100 мільйонів спроб фішингу щодня.URL: https://safety.google/intl/ua_ua/.(дата звернення:09.05.2024).

22. Gmail блокує більше 100 рекламних повідомлень в секунду.URL: https://safety.google/intl/ua_ua/security/built-in-protection/.(дата звернення:09.05.2024).

23. Звіт про тенденцію фішмнгу APWG Q4 2023.URL: https://docs.apwg.org/reports/apwg_trends_report_q4_2023.pdf. (дата звернення:12.05.2024).

24. Ваш мозок під прицілом: український вимір когнітивної війни.URL: https://deepstateua.com/koghnitivni-viini-ukrayinskii-vimir/.(дата звернення:12.05.2024).

25. Протидія когнітивній війні: інформованість і стійкість.URL: https://www.nato.int/docu/review/uk/articles/2021/05/20/protidya-kogntivnj-vjn-nformovanst-stjkst/index.html. (дата звернення:12.05.2024).

26. Кремль проводить дезінформаційну кампанію, щоб підірвати Зеленського, про це свідчать документи.URL: https://www.washingtonpost.com/world/2024/02/16/russian-disinformation-zelensky-zaluzhny/.(дата звернення:13.05.2024).

27. Переривання оманливого використання штучного інтелекту шляхом таємних операцій впливу.URL: https://openai.com/index/disrupting-deceptive-uses-of-AI-by-covert-influence-operations/.(дата звернення:14.05.2024).