МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “МЕТОД ТЕСТУВАННЯ КОРИСТУВАЧІВ НА СТІЙКІСТЬ ДО СОЦІОІНЖЕНЕРНИХ МАНІПУЛЯЦІЙ ІЗ ВИКОРИСТАННЯМ ІМІТАЦІЙНИХ СЦЕНАРІЇВ”

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Управління інформаційною та кібернетичною безпекою

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

_____ Артем ЖУРБЕНКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ-61
Артем ЖУРБЕНКО

Керівник:
Доктор філософії з кібербезпеки
Михайло ЗАПОРОЖЧЕНКО

Рецензент:

_____ _____

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра Управління кібербезпекою та захистом інформації
Ступінь вищої освіти магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедрою УКБЗІ
_____ Світлана ЛЕГОМІНОВА
"____" _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Студенту Журбенко Артему Олеговичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: "Метод тестування користувачів на стійкість до соціоінженерних маніпуляцій із використанням імітаційних сценаріїв"

керівник кваліфікаційної роботи Михайло ЗАПОРОЖЧЕНКО, доктор філософії
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від "30" жовтня 2025 р. № 467
Строк подання кваліфікаційної роботи "11" грудня 2025 р.

2. Вихідні дані до кваліфікаційної роботи: *наукова література, стандарти з ІБ, аналітичні звіти, статистика інцидентів, корпоративні політики безпеки, кейси атак, типові вектори соціоінженерних впливів.*
3. Перелік питань, які потрібно розробити:
    1. Проаналізувати соціоінженерні загрози, їх класифікацію та методи впливу на користувачів.
    2. Дослідити існуючі підходи та методи оцінювання стійкості користувачів до соціоінженерних атак.
    3. Розробити метод імітаційного тестування користувачів на стійкість до соціоінженерних впливів, включно з побудовою сценаріїв і критеріями оцінки результатів.
    4. Сформувати практичні рекомендації щодо зниження ризику компрометації користувачів на основі результатів тестування.
4. Перелік ілюстративного матеріалу: *презентація*
5. Дата видачі завдання "02" жовтня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	11.10.2025	
2.	Збір та аналіз літератури.	20.10.2025	
3.	Дослідження теоретичних та методичних засад тестування користувачів на стійкість до соціоінженерних маніпуляцій	25.10.2025	
4.	Аналіз векторів тестування користувачів на стійкість до соціоінженерних маніпуляцій.	08.11.2025	
5.	Розробка методу тестування користувачів на стійкість до соціоінженерних маніпуляцій.	16.11.2025	
6.	Формулювання висновків за результатами дослідження.	24.11.2025	
7.	Оформлення роботи.	05.12.2025	
8.	Оформлення презентації.	16.12.2025	
9.	Отримання рецензії на роботу.	17.12.2025	
10.	Захист в ЕК.	__.01.2026	

Здобувач вищої освіти _____ Артем ЖУРБЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Михайло ЗАПОРОЖЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

Направляється здобувач Журбенко А.О. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека та захист інформації
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Метод тестування користувачів на стійкість до соціоінженерних маніпуляцій із використанням імітаційних сценаріїв"
Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач **ЖУРБЕНКО Артем** у кваліфікаційній роботі проаналізував теоретичні аспекти тестування користувачів на стійкість до соціоінженерних маніпуляцій, здійснив порівняльний аналіз існуючих підходів та дослідив практичне застовування імітаційних сценаріїв як елемента підвищення кіберстійкості організації в цілому.

ЖУРБЕНКО Артем показав високу теоретичну і практичну підготовку, володіння науково-дослідницькими методами, вміння самостійно знаходити шляхи вирішення проблеми дослідження. Результати дослідження апробовані на конференції "Стратегії кіберстійкості: управління ризиками та безперервність бізнесу" 27 лютого 2025 року.

Все це дозволяє оцінити кваліфікаційну роботу здобувача **ЖУРБЕНКА Артема** на оцінку "добре" та присвоїти йому кваліфікацію "Магістр з кібербезпеки та захисту інформації за освітньо-професійною програмою Управління інформаційною та кібернетичною безпекою".

Керівник кваліфікаційної роботи _____ Михайло ЗАПОРОЖЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Журбенко А.О. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою
Управління кібербезпекою та захистом
інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

здобувача вищої освіти Журбенка Артема Олеговича
на тему "Метод тестування користувачів на стійкість до соціоінженерних маніпуляцій із використанням імітаційних сценаріїв"

Актуальність За умов конкуренції компанії нерідко зустрічаються з нечесною боротьбою з використанням інформаційних технологій. Розвиток цифрових комунікацій робить бізнес вразливим до маніпуляцій. Атаки з використанням соціальної інженерії обходять технічні перешкоди, використовуючи людський фактор, тому потрібен комплексний підхід до інформаційної безпеки, що включає не тільки IT-захист, а й навчання та організаційні заходи. Дослідження методів протидії соціальним маніпуляціям та підвищення обізнаності користувачів є важливим завданням для розвитку галузі та підприємництва.

Позитивні сторони

1. У межах роботи здійснено всебічний аналіз теоретичних і методичних засад загроз соціальної інженерії, їх класифікації та ролі в сучасних інформаційно-комунікаційних системах. Проведено систематизацію векторів таких загроз, проаналізовано існуючі підходи до оцінювання стійкості користувачів та імітаційні методики тестування, що дозволило сформувати структуровану картину слабких місць у поведінці користувачів.
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді таблиць. Автор опрацював значну джерельну базу: близько 60 публікацій та електронних джерел, в тому числі англомовних.
3. За результатами дослідження запропоновано рекомендації щодо методики тестування стійкості до соціоінженерних впливів із використанням імітаційних сценаріїв.

Недоліки

1. В межах дослідження значну увагу було приділено теоретичному аналізу та розробці методики, проте для повного розкриття теми доцільно було б здійснити глибинне вивчення практичних аспектів.

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

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує позитивної оцінки, а здобувач Журбенко Артем Олегович заслуговує присвоєння кваліфікації "Магістр кібербезпеки за освітньо-професійною програмою "Управління інформаційною та кібернетичною безпекою".

Рецензент:
_____ _____ _____
підпис *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 80 стор., 6 рис., 7 табл., 61 джерел.

Мета роботи - розробка методу тестування користувачів на стійкість до соціоінженерних маніпуляцій на основі імітаційних сценаріїв, що забезпечує комплексне оцінювання поведінкових реакцій та визначення рівня вразливості до різних типів соціоінженерних впливів.

Об'єкт дослідження - процес взаємодії користувачів інформаційно-комунікаційних систем із соціоінженерними загрозами.

Предмет дослідження - методи та підходи до імітаційного моделювання соціоінженерних атак і процедур тестування користувачів з метою оцінювання їх стійкості до маніпуляцій.

Методи дослідження. Для розв'язання поставлених у роботі завдань застосовано комплекс теоретичних та емпіричних методів. Теоретичну основу становлять методи аналізу й синтезу для опрацювання наукових джерел, стандартів і нормативної документації; порівняльний аналіз для співставлення ефективності різних підходів до побудови імітаційних сценаріїв; методи систематизації та класифікації, що забезпечують впорядкування типів соціоінженерних атак і відповідних механізмів протидії. Емпіричний рівень дослідження представлений аналізом кейсів реальних соціоінженерних інцидентів та їх наслідків, контент-аналізом внутрішніх політик інформаційної безпеки й звітів про інциденти, а також моделюванням імітаційних сценаріїв соціоінженерних атак для оцінювання стійкості користувачів у контрольованих умовах.

Короткий зміст роботи. У роботі здійснено глибокий аналіз понять і механізмів, які характеризують соціальну інженерію як одну з ключових загроз інформаційній безпеці організацій. Теоретична частина охоплює сутність, класифікацію атак, еволюцію підходів до інформаційної безпеки та методи оцінки стійкості користувачів до маніпуляцій. В аналітичній частині проведено систематизацію векторів соціоінженерних загроз в сучасних ІКТ-середовищах,

досліджено існуючі підходи до тестування користувачів, а також оцінено ефективність навчальних і превентивних заходів. На основі отриманих результатів запропоновано методику тестування на стійкість до соціоінженерних атак за допомогою імітаційних сценаріїв та сформовано практичні рекомендації щодо підвищення рівня інформаційної безпеки.

***Галузь застосування*.** Розроблені підходи можуть використовуватися під час створення або вдосконалення систем управління інформаційною безпекою підприємств, зокрема в частині захисту від соціоінженерних загроз. Запропонована методика є корисною для організацій, які прагнуть реалізувати системний підхід до навчання персоналу, оцінки людського фактора, розробки політик реагування і превентивних заходів.

КЛЮЧОВІ СЛОВА : СОЦІАЛЬНА ІНЖЕНЕРІЯ, ІНФОРМАЦІЙНА БЕЗПЕКА, СТІЙКІСТЬ КОРИСТУВАЧІВ, ІМІТАЦІЙНІ СЦЕНАРІЇ, ТЕСТУВАННЯ НА ВРАЗЛИВІСТЬ, УПРАВЛІННЯ РИЗИКОМ, ЛЮДСЬКИЙ ФАКТОР.

ABSTRACT

The text part of the qualification work for obtaining a master's degree: 80 pages, 6 figure, 7 tables, 61 sources.

The purpose of the work is the development of a method for testing users' resistance to social engineering manipulations based on simulation scenarios, which provides a comprehensive assessment of behavioral responses and determines the level of vulnerability to various types of social engineering influences.

Object of research is the process of interaction between users of information and communication systems and social engineering threats.

Subject of research is methods and approaches to simulation modeling of social engineering attacks and user testing procedures to assess their resistance to manipulation.

Research methods. A set of theoretical and empirical methods was used to solve the tasks set in the work. The theoretical basis consists of methods of analysis and synthesis for processing scientific sources, standards, and regulatory documentation; comparative analysis for comparing the effectiveness of different approaches to building simulation scenarios; methods of systematization and classification that ensure the ordering of types of social engineering attacks and corresponding countermeasures. The empirical level of the study is represented by the analysis of cases of real social engineering incidents and their consequences, content analysis of internal information security policies and incident reports, as well as modeling of simulation scenarios of social engineering attacks to assess user resilience in controlled conditions.

Brief content of research. An in-depth analysis of the concepts and mechanisms that characterize social engineering as one of the key threats to the information security of organizations is carried out in this work. The theoretical part covers the essence, classification of attacks, evolution of approaches to information security, and methods for assessing user resistance to manipulation. The analytical part systematizes the vectors of social engineering threats in modern ICT environments, examines existing

approaches to user testing, and evaluates the effectiveness of training and preventive measures. Based on the results obtained, a methodology for testing resistance to social engineering attacks using simulation scenarios is proposed, and practical recommendations for improving information security are formulated.

Field of research. The developed approaches can be used when creating or improving enterprise information security management systems, in particular in terms of protection against social engineering threats. The proposed methodology is useful for organizations seeking to implement a systematic approach to staff training, human factor assessment, and the development of response policies and preventive measures.

KEYWORDS: SOCIAL ENGINEERING, INFORMATION SECURITY, USER RESILIENCE, SIMULATION SCENARIOS, VULNERABILITY TESTING, RISK MANAGEMENT, HUMAN FACTOR.

ЗМІСТ

ВСТУП 11

РОЗДІЛ 1 ТЕОРЕТИЧНІ ТА МЕТОДИЧНІ ЗАСАДИ ПРОТИДІЇ СОЦІАЛЬНІЙ ІНЖЕНЕРІЇ 14

1.1. Сутність та класифікація соціоінженерних атак: понятійний апарат, типологія, техніки впливу 14

1.2. Еволюція підходів до інформаційної безпеки: місце соціальної інженерії серед сучасних загроз 24

1.3. Методи та підходи до оцінювання стійкості користувачів до соціоінженерного впливу 31

Висновки до розділу 1 39

РОЗДІЛ 2 АНАЛІЗ ВЕКТОРІВ СОЦІОІНЖЕНЕРНИХ ЗАГРОЗ І ПІДХОДІВ ДО ЇХ ІМІТАЦІЇ 41

2.1. Ідентифікація основних напрямів реалізації соціоінженерних атак у контексті сучасних інформаційно-комунікаційних систем 41

2.2. Аналіз існуючих методів тестування користувачів на сприйнятливість до соціоінженерних впливів 47

2.3. Оцінювання ефективності заходів із підвищення обізнаності користувачів та формування стійкості до маніпуляцій 54

Висновки до розділу 2 59

РОЗДІЛ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ КОНТРЗАХОДІВ ІЗ ЗМЕНШЕННЯ РИЗИКУ КОМПРОМЕТАЦІЇ КОРИСТУВАЧІВ 61

3.1 Методика оцінки базового рівня стійкості до соціоінженерних маніпуляцій 61

3.2. Розробка методу тестування користувачів на стійкість до соціоінженерних маніпуляцій 71

3.3. Формування практичних рекомендацій щодо зниження ризику компрометації користувачів 79

Висновки до розділу 3 86

ВИСНОВКИ 88

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 90

ВСТУП

Актуальність теми. Соціальна інженерія на данний момент часу є найпоширенішим вектором початкового доступу для кіберзлочинців, більше половини атак щодо першого проникнення починаються з фішингу або інших прийомів маніпуляції людьми. Враховуючи поширеність і зростаючу ефективність таких атак, питання захисту інформації вже давно перестало бути виключно технічним, стало критично важливим увагу звертати на поведінковий аспект, наскільки співробітники можуть розпізнати спробу маніпуляції, утриматися від імпульсивної реакції, дотриматися внутрішніх процедур безпеки. Ці всі фактори разом формують фундамент для побудови стійкої системи інформаційної безпеки, де захищене середовище підтримується не лише технологіями, а й обізнаністю й відповідальністю людей.

З огляду на зазначене, обрана тема кваліфікаційної роботи має високу актуальність, оскільки результати дослідження дають змогу істотно підсилити захист організацій від соціоінженерних загроз.

Мета роботи - розробка методу тестування користувачів на стійкість до соціоінженерних маніпуляцій на основі імітаційних сценаріїв, що забезпечує комплексне оцінювання поведінкових реакцій та визначення рівня вразливості до різних типів соціоінженерних впливів.

Об'єкт дослідження - процес взаємодії користувачів інформаційно-комунікаційних систем із соціоінженерними загрозами.

Предмет дослідження - методи та підходи до імітаційного моделювання соціоінженерних атак і процедур тестування користувачів з метою оцінювання їх стійкості до маніпуляцій.

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

1. Проаналізувати соціоінженерні загрози, їх класифікацію та методи впливу на користувачів.

2. Дослідити існуючі підходи та методи оцінювання стійкості користувачів до соціоінженерних атак.

3. Розробити метод імітаційного тестування користувачів на стійкість до соціоінженерних впливів, включно з побудовою сценаріїв і критеріями оцінки результатів.

4. Сформувати практичні рекомендації щодо зниження ризику компрометації користувачів на основі результатів тестування.

Методи дослідження. Для розв'язання поставлених у роботі завдань застосовано комплекс теоретичних та емпіричних методів. Теоретичну основу становлять методи аналізу й синтезу для опрацювання наукових джерел, стандартів і нормативної документації; порівняльний аналіз для співставлення ефективності різних підходів до побудови імітаційних сценаріїв; методи систематизації та класифікації, що забезпечують впорядкування типів соціоінженерних атак і відповідних механізмів протидії. Емпіричний рівень дослідження представлений аналізом кейсів реальних соціоінженерних інцидентів та їх наслідків, контент-аналізом внутрішніх політик інформаційної безпеки й звітів про інциденти, а також моделюванням імітаційних сценаріїв соціоінженерних атак для оцінювання стійкості користувачів у контрольованих умовах.

Наукова новизна отриманих результатів полягає в тому, що в межах роботи пропонується комплексний підхід, а саме, побудова імітаційних сценаріїв із урахуванням контексту організації, психологічних і поведінкових параметрів, комбінована методика оцінювання, яка дозволяє не лише виявляти вразливості, а й прогнозувати ризики та ефективність заходів.

Практичне значення одержаних результатів цієї роботи полягає в отримані результатів та рекомендацій, які можуть бути використані організаціями (комерційними, державними), IT-відділами та службами безпеки для розробки політик, впровадження адаптивних тренінгів, оцінки ризиків і планування заходів безпеки.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції «Стратегії кіберстійкості: управління ризиками та безперервність бізнесу»:

Журбенко А. О. Використання хмарних технологій для забезпечення безперервності ітінфраструктури. Стратегії кіберстійкості: управління ризиками та безперервність бізнесу : матеріали всеукр. науково-практ. інтернет конф., м. Київ, 27 лют. 2025 р. С.177-181, URL: https://duikt.edu.ua/uploads/p_2779_46212583.pdf

РОЗДІЛ 1 ТЕОРЕТИЧНІ ТА МЕТОДИЧНІ ЗАСАДИ ПРОТИДІЇ СОЦІАЛЬНІЙ ІНЖЕНЕРІЇ

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

1.1. Сутність та класифікація соціоінженерних атак: понятійний апарат, типологія, техніки впливу

Соціальна інженерія - сукупність прийомів і методів впливу на людей з метою отримання несанкціонованого доступу до інформації, ресурсів або фізичних об’єктів. В основі соціальної інженерії лежить не уразливість програмного забезпечення чи криптографічні атаки, а використання психологічних, соціальних і процедурних слабкостей окремих осіб або організацій. Соціальна інженерія побудована на припущенні, що люди, їхні звички, очікування, емоції та організаційні процедури часто легше піддаються впливу, ніж складні технічні засоби захисту. Поняття «соціальна інженерія» охоплює широкий спектр операцій від простого масового фішингу електронною поштою до складних багатоетапних кампаній, що включають попередню розвідку OSINT, спірфішинг, вішинг, смішинг або фізичне вторгнення. [8]

Головними характеристиками соціальної інженерії є, насамперед, акцент на людському факторі. Серед найпоширеніших психологічних тригерів можна виділити довіру до авторитету, реакцію на терміновість, страх перед втратою вигод, бажання допомогти або бути корисним, ефект соціального доказу та схильність діяти за звичкою. [19] Такі механізми працюють без свідомого аналізу безпеки ситуації, особливо в умовах стресу або великого навантаження. Іншою важливою характеристикою є висока економічна ефективність для зловмисника: кампанії соціальної інженерії часто мають дуже низькі витрати на підготовку і,

водночас, високу віддачу у вигляді викрадених облікових даних, фінансових переказів або інформації для подальших атак. Завдяки цій економічній ефективності соціальна інженерія стала широко використовуваним інструментом для окремих кіберзлочинних угруповань, державних суб'єктів та шахрайських схем.

Соціальна інженерія, яка є загрозою для інформаційної безпеки організацій, дуже важко ідентифікувати та відстежити. Ця загроза набуває різних форм, що нагадують справжні операції або внутрішні процеси, і може залишатися прихованою протягом тривалого часу, виступаючи першим вектором для технологічної фази проникнення. Організаціям нелегко ідентифікувати наслідки атак соціальної інженерії. Це пов'язано з тим, що наслідки варіюються від витоку особистої та ділової інформації до економічних втрат, що включають шахрайство BEC (Business Email Compromise). Іноді наслідки атак соціального інжинірингу також призводять до втрати доступу до офісів, серверів або обладнання, зокрема в секторах, що мають справу з критичною інфраструктурою. Окрім прямих наслідків, атаки соціального інжинірингу також призводять до інших організаційних наслідків, які включають витрати на реагування, юридичні наслідки, втрату клієнтів та перегляд політик.

Для кращого розуміння вищезазначеної ідеї важливо також взяти до уваги поняття соціо-психологічної атаки, розвідки з відкритих джерел (OSINT), фішинг, вішинг та спуфінг.

Соціально-психологічна атака це атака, під час якої зловмисник, використовуючи психологічні прийоми, переконує жертву розкрити конфіденційну інформацію або зробити щось, що негативно впливає на оточення. Ця атака також не залежить від вразливостей і є переважно успішною, оскільки, як уже зазначалося, використовує емоційні тригери. Прикладами атак соціального інжинірингу є фішинг, вішинг та атаки в соціальних мережах.

OSINT (Open source intelligence) або ж соціально-психологічна розвідка або розвідка на основі відкритик джерел являє собою процес збору, аналізу та

використання загальнодоступної інформації з відкритих джерел задля отримання даних без порушення закону. Вона включає пошук у цифрових ресурсах, таких як соціальні мережі, ЗМІ, публічні бази даних та форуми, а також у традиційних джерелах, як приклад: газети, звіти різного типу або книги. [9]

Далі розглянуто фішинг та його найпоширеніші типи. Фішинг, це найпоширеніший на сьогодні тип соціальної інженерії, коли зловмисник прагне ввести в оману користувача, щоб він розкрив конфіденційну інформацію, таку як паролі, номери кредитних карток та особисті дані. [10] Це здійснюється за допомогою підроблених електронних листів, повідомлень або веб-сайтів, які схожі на справжню версію сайту, змушуючи цільову особу розкрити свої дані. Фішинг-атаки можна класифікувати на:

- класичний фішинг (email-фішинг) – це найпоширеніший вид фішингу, при якому зловмисник надсилає численні електронні листи, що нагадують повідомлення від надійних джерел (банків, компаній та урядових органів), в яких просить надати конфіденційну інформацію або перейти за посиланням;
- цільовий фішинг (Spear phishing) – це цільовий вид фішингу, при якому зловмисник націлюється на одну особу або групу осіб. Повідомлення надсилається безпосередньо адресату, що підвищує ймовірність успіху шахрайства;
- вішинг (Vishing) – шахрайство, що здійснюється по телефону. Шахрай стверджує, що працює в банку, службі IT-підтримки або поліції. Він використовує свої навички соціальної інженерії, щоб викрасти дані споживачів; [12]
- смішинг (Smishing) – фішинг за допомогою SMS-повідомлень. Як і у випадку з вішингом, повідомлення розроблені так, щоб нагадувати типові повідомлення, що надсилаються банками або поштовою службою, і часто містять посилання, яке веде на фішинговий сайт;
- фармінг (перенаправлення на підроблені сайти) – це фішинг, який передбачає перенаправлення осіб на фішингові веб-сайти, що виглядають як

справжні. Це робиться з метою введення в оману користувача, щоб він надав конфіденційні дані на фішинговому веб-сайті для доступу до даних;

- спуфінг (Spoofing) – це техніка фішингу, яка передбачає, що зловмисник видає себе за надійну сторону, змінюючи дані відправника повідомлення, які можуть складатися з адреси електронної пошти, IP-адреси та номера телефону. На відміну від фішингу, який не гарантує автентичність повідомлення, техніка спуфінгу це забезпечує. Наприклад, у фішинговому повідомленні використовується спуфінг електронної пошти, щоб повідомлення виглядало так, ніби воно було надіслане справжнім банком, а в техніці «китобійного полювання» використовується техніка спуфінгу ідентифікатора дзвінка, щоб дзвінок виглядав так, ніби він надходить зі справжнього номера;
- вейлінг (Whaling або CEO fraud) – у цьому випадку шахраї вирішують видати себе за генерального директора компанії. Вони використовують веб-сайти компаній, соціальні мережі та інші джерела для збору даних про генерального директора або інших керівників вищої ланки. Вони видають себе за керівника вищої ланки, використовуючи подібну ділову електронну адресу. Це шахрайство має набагато складнішу форму, оскільки є цілеспрямованим, але я впевнений, що ви розумієте, скільки даних про будь-яку людину можна зібрати, використовуючи відкриті джерела. [11]

Розповсюдженність та кількість фіксації випадків схематично зображено в рис. 1.1.

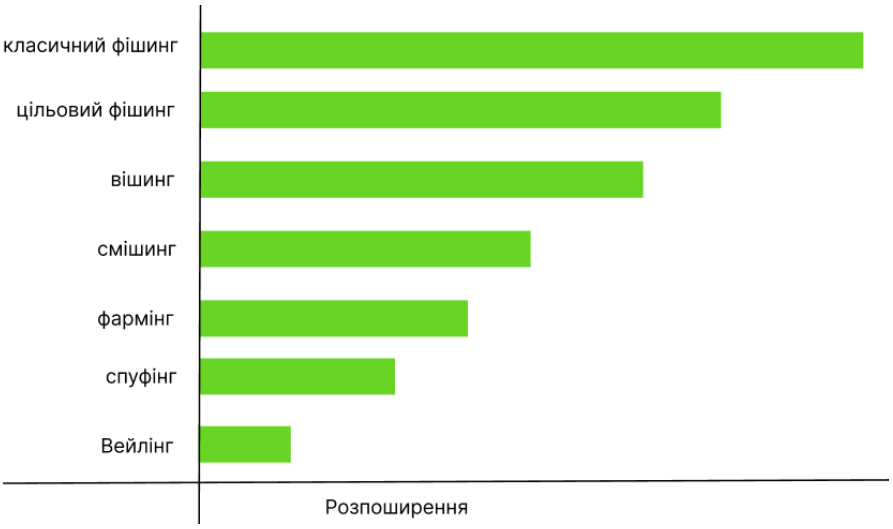

Рис. 1.1. Частота фіксації випадків різних типів фішингу

Соціоінженерні атаки можна класифікувати за трьома різними ознаками, за типом цілі, каналом впливу і мотивом атакуючого. Тип цілі, тобто, що саме хоче отримати або досягти зловмисник. Це може бути незаконне отримання конфіденційної інформації (логіни, паролі, банківські дані, персональні дані), доступ до захищених систем або ресурсів, виконання певних дій (перерахунок коштів, передача даних, зміна налаштувань), або компрометація організаційних процедур (внутрішніх політик, процедур підтвердження, прав доступу). Іноді ціль - просто отримати довіру або внутрішню інформацію для подальших більш складних атак. Зловмисник – не звертає увагу на технічні слабкості системи, він використовує психологічні чи поведінкові вразливості людини, щоб обійти захист і досягти своїх цілей.

Крім того, за способом реалізації атаки їх можна розділити на «соціальні / людські» (social-based), «технічні/комп'ютерні» (technical/computer-based) та «фізичні» (physical-based). Соціальні атаки передбачають психологічний вплив через комунікацію, соціальні відносини, маніпуляції, як приклад: дзвінки, переконання, вмовляння або створення довіри. Технічні - використовують цифрові засоби: листи, сайти, шкідливі вкладення, зловмисні програми. Фізичні ж, передбачають безпосередню фізичну взаємодію або проникнення, доступ до приміщень чи носіїв, спостереження чи крадіжку документів. Така тривимірна класифікація допомагає зрозуміти, яким шляхом може піти атака, і які засоби захисту треба застосовувати. (рис. 1.2) [15]

Рис. 1.2. Соціоінженерні атаки за різними ознаками

Зловмисники з різними мотивами створюють спроби соціальної інженерії, які відрізняються за характером, але мають одну спільну рису: використання людського фактору. Деякі з них прагнуть отримати гроші, здійснити шахрайство або викрасти фінансові дані, а інші прагнуть отримати доступ до конфіденційної інформації, комерційної або державної. Інші хочуть зруйнувати довіру або репутацію та підірвати авторитет, посіявши сумніви серед тих, хто стоїть за організацією. У деяких випадках метою є розширення контролю, захоплення ресурсів або послаблення безпеки, щоб залишити двері відкритими для наступного етапу атаки. Звичайно, є й ті, хто керується мотивами соціальної або політичної маніпуляції, намагаючись ввести в оману, дестабілізувати або змінити поведінку певних людей або груп. Класичні прийоми дезінформації, маніпуляції особистими даними та підриву довіри. [20]

Що стосується здійснення такої атаки, канал впливу визначає як метод, так і класифікацію, що слідує за ним. До поширених каналів, через які здійснюються ці атаки, належать електронна пошта або інші онлайн-повідомлення, фішинг,

SMS-повідомлення, смфішинг, телефонні дзвінки, вішинг, корпоративні чат-інструменти або месенджери, і навіть зовнішні носії, такі як USB-накопичувачі, «залишені» на робочому місці, байтинг, або поєднання цифрових і фізичних технік

Нижче розглянуто найпростіші способи протидії таким атакам. (табл. 1.1)

Таблиця 1.1

Протидія атакам на основі соціальної інженерії

Назва атаки	**Протидія**
Класичний Фішинг	Перевірка відправника: обов'язкова перевірка повної адреси електронної пошти (не лише ім'я). Уникнення переходу за посиланням, наведення курсору на посилання, щоб побачити справжню URL-адресу. Користувач повинен перевіряти кому він відправляє конфіденційні дані через email. Жодна поважна установа (банк, державний орган) не вимагатиме паролі, PIN-коди чи CVV-коди електронною поштою. Багатофакторна автентифікація (MFA). Увімкнення MFA (навіть якщо пароль скомпрометовано, доступ без другого фактора буде майже неможливим).
Цільовий Фішинг	Перевірка «петлею зворотного зв'язку»: Якщо лист від колеги чи керівника здається дивним або вимагає термінових дій, потрібно надіслати новий лист по іншим перевіреним контактним даним або зателефонувати особі-відправнику, щоб підтвердити запит, не використовуючи функцію «Відповісти» на підозрілому листі.
Вейлінг	Протоколи фінансових операцій: Впровадження суворих внутрішніх правил, які вимагають двох підписів (two-person rule) або вербального підтвердження великих фінансових переказів, навіть якщо запит надійшов від керівника вищої ланки. Обмеження даних в OSINT: Обмеження публічної інформації про ролі та внутрішню ієрархію компанії, щоб ускладнити зловмисникам імітацію керівництва.
Вішинг	Завершення дзвінка та повторний виклик: Якщо несподівано дзвонять, видаючи себе за банк чи техпідтримку, потрібно перервати розмову, якщо хоча б якась інформація здається дивною. Самостійно знайти офіційний номер організації (на звороті картки або на офіційному сайті) і передзвонити їм, щоб перевірити інформацію.
Смішинг	Не відкривати посилання: Користувач ніколи не має переходити за посиланнями у несподіваних SMS-повідомленнях. Перед цим потрібно ввести URL-адресу банку/поштової служби вручну у браузері.
Спуфінг	Ігнорування ідентифікатора: Користувач повинен пам'ятати, що номер, або іншу інформацію яка відображається на екрані, можна підробити. Потрібно використовувати протидію, як при вішингу: перервати розмову та передзвонити або написати на офіційний номер чи пошту.

Продовження табл. 1.1

Назва атаки	Протидія
Фармінг	Перевірка URL-адреси та HTTPS: Завжди потрібно перевірятт, що адреса сайту в адресному рядку правильна, а з'єднання захищене (наявність символу замка та префіксу https://). Використання надійних DNS-серверів: Використання захищених або відомих DNS-провайдерів (наприклад, Google DNS, Cloudflare), оскільки фармінг часто передбачає компрометацію локальних DNS-налаштувань. Антивірусне ПЗ та мережеві фільтри: Використання актуальних антивірусних програм (наприклад стандартний Windows Defender), які можуть виявляти та блокувати шкідливі зміни у файлі hosts комп'ютера.

Також важливо згадати зворотну соціальну інженерію (Reverse Social Engineering (RSE)), вона має ту саму мету, що й типова атака соціальної інженерії, але з повністю іншим підходом. Це атака person-to-person, де зловмисник встановлює прямий контакт з ціллю, щоб змусити її розкрити конфіденційну інформацію. У більшості випадків хакер встановлює контакт з ціллю за допомогою електронної пошти та соціальних мереж, використовуючи різні схеми та видаючи себе за благодійника або кваліфікованого фахівця з безпеки, щоб переконати її надати доступ до своєї системи або мережі. [7]

Зловмисник може використовувати ці техніки як окремо так і комбінуючи їх, для початку розглянемо техніку при якій давить на авторитет. В цій техніці зловмисник видає себе за керівника, співробітника техпідтримки або представника влади, зазвичай використовуючи спуфінг, для того щоб викликати у жертви довіру до своїх слів. Метод зазначений вище частіше за все комбінують з техніками терміновості та залякування. При використанні методу терміновості частіше за все створюється відчуття критичної, обмеженої в часі ситуації для того, щоб жертва діяла ірраціонально і не встигла критично оцінити ситуацію. Тим часом при методі залякування використовують загрози, наприклад: розголошення конфіденційної інформації, погроза судовим позовом або блокуванням рахунків, щоб змусити жертву діяти необачливо під впливом емоцій.

Техніка жадібності використовується зловмисниками, щоб спокусити жертву обіцянкою великої вигоди за мінімальні зусилля, що притупляє

пильність. Зловмисник створює привабливу ілюзію, наприклад, виграш у лотерею або великий спадок, яка потребує від жертви невеликих дій: ввести особисті дані, паролі, номери банківських карток для підтвердження або сплатити невелику комісію чи податок. Цей метод часто використовують у фішингових кампаніях, де обіцянка великої винагороди стає потужним емоційним стимулом, змушуючи жертву ігнорувати очевидні ознаки шахрайства та діяти поспішно.

Методи соціальної інженерії рідко існують окремо. Через це вони майже завжди поєднуються з технічними векторами атаки. Таке поєднання збільшує шанси зловмисника на успіх, оскільки, з одного боку, використовує психологію, маніпулювання та довіру людей, а з іншого - технічні недоліки в системах або шкідливе програмне забезпечення.

Соціальна інженерія як психологічна маніпуляція є першою ланкою в ланцюжку атаки: зловмисник може зв'язатися зі співробітником електронною поштою, телефоном або іншим каналом, видаючи себе за довірену особу або представника служби, і попросити виконати дію, яка на перший погляд здається обґрунтованою. Наприклад, це може бути прохання терміново оновити пароль, перевірити документ, завантажити нову версію програми або підключитися до VPN/мережі для перевірки. У таких випадках психологічний тиск, створення довіри, терміновість або авторитет спонукають жертву до негайних дій без ретельної перевірки.

Якщо в технічному середовищі є вразливість, наприклад, відсутність багатофакторної автентифікації (MFA), слабкий контроль над встановленням програмного забезпечення, недостатня фільтрація шкідливих вкладень, погана політика перевірки запитів на доступ або платежів – соціальний тригер може активувати саме те, що дає зловмиснику технічний міст для вторгнення. Наприклад, співробітник отримує електронний лист із підробленим, але правдоподібним дизайном від IT-адміністратора, переходить за посиланням і відкриває фішингову сторінку, або завантажує шкідливий файл. Якщо на комп'ютері немає обмежень, зловмисник отримує логіни/паролі, запускає

шкідливе ПЗ і бере під контроль обліковий запис або систему. Це приклад роботи соціальної інженерії та технічних атак як одного ланцюга.

Більш складні, гібридні або багатоетапні атаки, де соціальні методи та технічні вектори змінюються або поєднуються. Наприклад, спочатку жертві надіслано лист-фішинг із вкладенням, потім йде телефонний дзвінок, щоб переконати відкрити вкладення або зателефонувати у «службу підтримки» і ввести дані вручну. Така тактика, соціо-технічна атака, часто ефективніша, ніж просто фішинг, оскільки чергування каналів і підходів розмиває увагу, створює більшу правдоподібність і знижує шанси, що жертва запідозрить шахрайство.

Ще один варіант взаємодії - коли соціальна інженерія використовується для отримання «технічної інформації» або підготовки технічного вектору атаки. Такі як телефонний дзвінок або лист, зловмисник дізнається, яка саме версія програмного забезпечення використовується, чи є доступ через віддалений комп’ютер, які процедури перевірки діють у компанії. Після цього йде цілеспрямована технічна атака через експлойти, brute-force або доступ через незахищену мережу. Тобто соціальна інженерія «відкриває двері», дає інсайдерську інформацію, знижує бар’єри, а технічні методи вже «пробивають» захист.

В контексті великих організацій або корпорацій таке поєднання соціальної інженерії з технічними векторами атак є особливо небезпечним, бо внутрішні процедури, такі як перевірки, політики чи багаторівневі дозволи, часто покликані захищати від зовнішніх атак, але не враховують людський фактор. Якщо співробітник під тиском виконує нестандартну дію (наприклад, додає нового користувача, змінює реквізити, дає доступ комусь на стороні), технічні системи можуть цього не помітити, оскільки формально все буде в рамках політики. Саме тому поєднання соціальних і технічних векторів робить атакуючих набагато сильнішими, вони використовують природну довіру, обмеження систем і людські процедури, які складно перевірити автоматично. [16]

1.2. Еволюція підходів до інформаційної безпеки: місце соціальної інженерії серед сучасних загроз

За останні два десятиліття пріоритети інформаційної безпеки трансформувалися, перейшовши від суто технічного фокусу до більш складних, людино- та процесоорієнтованих моделей, що враховують управління ризиками, архітектуру, операційну готовність, управління ланцюгами постачання та культуру безпеки. У перші дні існування корпоративних мереж із чіткими межами захист зосереджувався на точках входу, де брандмауери, системи виявлення та запобігання вторгненням (IDS/IPS), антивірусне програмне забезпечення та шифрування відігравали головну роль, а людський фактор часто ігнорувався або зводився до потреби в навчанні. Однак із поширенням мобільності, віддаленої роботи та хмарних технологій ці межі розмилися, ресурси та користувачі опинилися за межами традиційного периметра, що зробило неефективною модель безпеки, засновану на довірі до внутрішньої мережі та блокуванні зовнішніх загроз. Це спричинило переосмислення архітектури безпеки та призвело до появи концепції Zero Trust, яка наголошує на безперервній перевірці та контролі доступу на рівнях користувачів, пристроїв і сервісів. [55] Типова схема мережевого захисту організації зображено на рис. 1.3.

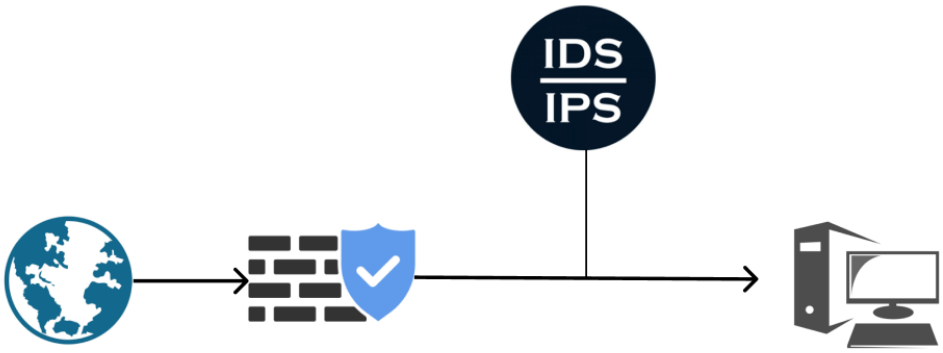

Рис. 1.3. Класична схема мережевого захисту організації

Водночас стало зрозуміло, що належний захист неможливий без урахування людського фактора. Реальні інциденти показали, що соціальна

інженерія та людські помилки залишаються значними векторами атак. Це спонукало організації інвестувати в розвиток кіберкультури, навчання на основі поведінкових даних, регулярні симуляції фішингових атак та валідаційні кампанії. Отже, політики, процеси, роль HR і лідерство стали невід'ємною частиною стратегій кібербезпеки.

Масштабні інциденти, зокрема атаки на ланцюги постачання (наприклад, SolarWinds), засвідчили, що навіть добре захищена внутрішня інфраструктура може бути вразливою через скомпрометоване стороннє ПЗ. Це привернуло увагу до безпечного життєвого циклу розробки ПЗ, вимог прозорості поставок (SBOM), управління третіми сторонами та безперервного моніторингу ланцюгів постачання, що призвело до посилення управління ризиками постачальників, впровадження вимог перевірок і акцентування на архітектурах, які зводять до мінімуму довіру до зовнішніх компонентів. [5]

Поряд із цим, розвиток технологій сприяв появі рішень для безперервного моніторингу та аналізу (SIEM, SOAR), захисту кінцевих точок (EDR/XDR), поведінкової аналітики (UEBA), хмарної безпеки (CASB, CSPM, CWPP) і конвергентних архітектур (SASE), які забезпечують гнучкий захист у різнорідних середовищах. Однак ці інструменти розглядаються не як самодостатні, а як елементи, що мають бути інтегровані з процесами реагування, обміном даними про загрози, реагуванням на інциденти та продуманими політиками управління ідентифікацією та доступом (MFA, найменші привілеї, управління ідентифікацією).

Регуляторні й організаційні чинники також підпали під плин часу, з’явилися вимоги GDPR, національні директиви з кібербезпеки, ініціативи щодо забезпечення безпеки ланцюгів постачання та стандарти управління ризиками (ISO/IEC 27001, NIST Cybersecurity Framework) стимулюють підхід, орієнтований на управління ризиками та доведеннями про відповідність, а не лише на набір технічних продуктів Зв'язок технічних, управлінських і правових вимог зробив пріоритети багатовимірними, тому організації повинні демонструвати не лише наявність інструментів, а й системне управління

ризиками, процедури реагування та відновлення, а також дієве навчання персоналу.

Ці зміни пріоритетів вплинули на організаційну структуру та практику, внаслідок чого безпека перестала бути суто IT-завданням, а стала частиною управління бізнес-ризиками. Керівники з інформаційної безпеки (CISO) відіграють роль стратегічних менеджерів ризиків, а інвестиції спрямовуються не лише на інструменти, а й на процеси, людський капітал, інтеграцію DevSecOps та розширення інформаційної видимості за допомогою телеметрії. Зважаючи на важливість стійкості та відновлення, планування має враховувати не лише запобігання, а й сценарії швидкого відновлення після порушень.

Наукові підходи до оцінки загроз також зазнали розвитку, перейшовши від технічно орієнтованих моделей до комплексних, мультидисциплінарних та емпірично-орієнтованих підходів, що поєднують кіберрозвідку, поведінкову науку, моделювання загроз і машинне навчання. Раніше оцінка загроз зосереджувалася на виявленні та класифікації технічних векторів, таких як вразливості ПЗ, експлойти, мережеві аномалії, з використанням сканування вразливостей, SIEM-логіки та сигнатурних детекторів. Однак із поширенням соціальної інженерії стало очевидно, що технічні системи, навіть добре налаштовані, не можуть захистити від маніпуляцій, спрямованих безпосередньо на людину, її довіру та процес прийняття рішень. Тому наукові моделі почали враховувати людський фактор як рівноправний елемент загрози.

Ця трансформація виражається в декількох важливих напрямках методологічного розвитку. Спочатку з’явилися стандартизовані інструменти для кількісної оцінки «важкості» соціальних атак для людини-спостерігача. Прикладом служить NIST Phish Scale, який дозволяє ранжувати фішингові листи за складністю їх виявлення людиною і вводить стандартизовані для досліджень і симуляцій. [6] Це дало змогу перейти від суто якісних описів атак до експериментальних дизайнів і статистичної інтерпретації результатів симуляцій awareness-кампаній. Такі підходи дозволяють порівняти результати між організаціями і корелювати поведенкові метрики з рівнем ризику.

У науковому інструментарії з'явилися поведінкові моделі та експериментальні протоколи, запозичені з психології та соціології. Прості лекції або одноразові тренінги часто не дають тривалого ефекту або взагалі не впливають на поведінку в складніших, реалістичних сценаріях. Тому оцінка загроз має включати не лише разові показники, а й показники стійкості в часі, частоту повідомлень про інциденти, час до повідомлення та інші поведінкові індикатори.

Розвиток машинного навчання та аналітики дозволив поєднати автоматичне виявлення та прогнозування з поведінковою аналітикою. Моделі машинного навчання можуть ефективно фільтрувати та ранжувати шкідливі повідомлення за ознаками технічної підробки, такий комбінований підхід дає кращі результати, ніж будь-який з компонентів окремо. Сучасні наукові підходи часто включають імітаційні моделі, що поєднують автоматичні детектори та поведінкові індикатори.

Наукові підходи підкреслюють необхідність системного, міждисциплінарного аналізу загроз, де технічна аналітика поєднується з соціальною наукою, правовими аспектами та управлінськими практиками. Це включає розробку методик для етичних симуляцій, стандартизацію показників, моделі ROI/ROSI для обґрунтування інвестицій у програми підвищення обізнаності, а також рекомендації щодо інституційної організації. Міжнародні агенції, такі як ф, розробляють методології оцінки ландшафту загроз та настанови, які стимулюють перехід від фрагментарних тестів до впровадження систем управління кібербезпекою з урахуванням людського фактора. Сучасна наука з оцінки загроз рухається від реактивного, вузько-технічного підходу до проактивного, соціотехнічного та емпірично валідованого підходу. [14]

Соціальна інженерія ж дедалі сильніше займає центральне, часто вирішальне місце в сучасному наборі кіберзагроз як для корпоративних, так і для персональних ІТ-систем, тому що вона дозволяє атакуючим обійти технічні бар’єри, використовуючи людський фактор. Аналітичні звіти великого масштабу та практичні розслідування демонструють, що фішинг, пре-текстинг і інші

соціально-інженерні підходи залишаються одними з найпоширеніших початкових векторів компрометації. [24]

Існує декілька взаємопов'язаних причин такого становища. По-перше, соціальна інженерія ефективно використовує базові психологічні механізми, такі як довіра, підкорення авторитету, страх пропустити щось важливе, бажання допомогти або швидко отримати вигоду. По-друге, атаки, засновані на маніпуляціях, легко масштабуються і таргетуються. Сучасні OSINT-інструменти, відкриті джерела даних і автоматизація, включно зі штучним інтелектом, дозволяють створювати правдоподібні, персоналізовані повідомлення для великих груп або таргетованих кампаній (spear-phishing, whaling). Поєднання персоналізації та масовості робить ці атаки дешевими для зловмисника і складними для виявлення для служб безпеки.

У корпоративних IT-системах соціальна інженерія часто є початковою фазою складніших ланцюгових атак. Отримавши облікові дані, доступ до пошти або допомогу в обході процедур, зловмисник переходить до технічного етапу, розгортаючи програми-вимагачі (ransomware), викрадаючи дані або порушуючи доступність. У багатьох серйозних інцидентах саме вдалий фішинговий лист або відповідь на дзвінок від імені адміністратора стає помилкою, що відкриває шлях до масштабних збитків. У бізнес-контексті соціальну інженерію часто пов'язують зі схемами BEC, витоком облікових записів і першим кроком у ланцюгу, що завершується ransomware-атаками або витоком інтелектуальної власності.

На персональному рівні соціальна інженерія загрожує приватності, фінансовій безпеці та цифровій ідентичності людини. Фішингові посилання, смішингові повідомлення, шахрайські дзвінки та deepfake можуть ввести в оману навіть технічно підковану людину, особливо коли атака націлена на емоційні чи соціальні тригери, що веде до компрометації особистих облікових записів, крадіжки коштів або використання скомпрометованих акаунтів для подальшого розповсюдження шкідливих повідомлень.

Зважаючи на свою природу, соціальна інженерія вимагає змін у пріоритетах захисту. Традиційні заходи залишаються необхідними, але недостатніми, оскільки не впливають безпосередньо на поведінковий фактор. Сучасні підходи до безпеки поєднують технічні контрзаходи з організаційними та поведінковими. Багатофакторна автентифікація (MFA), політики підтвердження фінансових операцій поза основним каналом зв'язку, фільтрація фішингу, інтеграція кампаній з підвищення обізнаності з регулярними симуляціями, швидка кореляція інцидентів через SIEM та навчання персоналу з обговоренням помилок і їх виправленням - усе це необхідно, оскільки саме комбінація технічних бар'єрів і культури безпеки знижує ймовірність успіху комбінованих соціотехнічних атак.

Ефективність соціальної інженерії залежить від поєднання технологічних, соціальних та психологічних факторів, які взаємопідсилюють один одного. Технологічні фактори посилюють соціоінженерні атаки, послаблюючи або усуваючи технічні бар'єри для нападника і надаючи можливості масштабувати й персоналізувати атаки. Ключовими технічними факторами є широкодоступні OSINT-джерела та платформи, що дозволяють швидко збирати персональні та корпоративні дані, масове використання хмарних сервісів, BYOD та мобільних додатків, які змінюють межі довіри, слабкі налаштування автентифікації, недостатнє використання багатофакторної аутентифікації, а також поява і застосування генеративного штучного інтелекту, що дозволяє створювати високоякісний, цільовий контент. У сукупності ці технології роблять атаки правдоподібнішими і дешевшими в реалізації, дозволяють одночасно атакувати багато цілей і швидко адаптуватися до реакцій жертв.

Соціальні чинники формують середовище, в якому соціоінженерні прийоми знаходять точки опори. Поширення дистанційної та гібридної роботи змінює звички спілкування: співробітники звикли до миттєвих повідомлень, push-сповіщень та підтверджень по телефону, що відкриває більше каналів для атак. У поєднанні з доступністю даних про співробітників у відкритих мережах, ці обставини підвищують точність і правдоподібність соціальної інженерії.

Психологічні фактори є серцем успіху соціальної інженерії, пояснюючи, як атаки долають критичне мислення і викликають бажану дію. Основними психологічними рушіями є вбудовані когнітивні евристики та упередження, такі як автоматичні реакції на авторитет, терміновість чи дефіцит, вигоду або жадібність, соціальний доказ і симпатію. Інші психологічні фактори, такі як втома уваги, емоційні стани, бажання допомогти або сором зізнатися у помилці, також значно підсилюють ймовірність успіху маніпуляції. [13]

В таблиці нижче показано як ці чинники працюють та що їм можна протиставити. (табл. 1.2)

Таблиця 1.2

Фактори ефективності соціоінженерних атак

Категорія фактору	**Що саме посилює атаку**	**Який результат для зловмисника**	**Приклади протидії**
Технологічні: AI контент, PhaaS, OSINT, BYOD, слабка MFA.	Автоматизація, персоналізація, масштабування, багато каналів входу	Висока швидкість і якість фішингу, велика кількість цілей, швидка адаптація сценаріїв	Впровадження MFA, фільтрація доменів, моніторинг і блокування PhaaS-інструментів.
Соціальні: віддалена робота, культура організації, час/навантаження.	Більше точок контакту, слабші процеси перевірки, низька звітність	Підвищена ймовірність успішних pretext-атак і BEC	Політики out-of-band, аудит постачальників, регулярні симуляції для різних ролей.
Психологічні: авторитет, терміновість, жадібність, соціальний доказ, втому уваги.	Спрацьовування евристиків, імпульсивні рішення	Жертва виконує дію (клік, введення даних, переказ коштів) без перевірки	Навчання, зворотний зв'язок, дизайн інтерфейсів з підказками

Розвиток технологій, розгалуженість соціальної інфраструктури та психологія суттєво впливають на дієвість соціоінженерних атак. Традиційні методи захисту інформації, такі як антивіруси чи міжмережеві екрани, мають обмеження у протидії соціальній інженерії. Вони добре працюють проти технічних загроз (віруси, вразливості ПЗ), але не враховують людський фактор, схильність до обману та маніпуляцій.

Навіть налаштовані системи захисту (багатофакторна автентифікація, моніторинг мережі) можуть бути обійдені через фішинг або підроблені повідомлення. Соціальна інженерія не завжди потребує використання вразливостей, тому технічні засоби часто неефективні. Крім того, традиційні методи не завжди встигають за швидкою зміною тактик атак, персоналізацією та націленням на конкретних людей.

Технічні засоби не можуть контролювати дії користувачів. Захист може блокувати шкідливі файли, але не може змусити людину не переходити за підозрілими посиланнями або не довіряти неправдивим повідомленням. Людська необережність залишається слабким місцем, яке неможливо захистити лише технічними засобами. Статистика свідчить, що більшість успішних атак відбувається через помилки користувачів.

Часто в організаціях відсутні політики, що враховують соціальні загрози, такі як перевірка запитів, навчання персоналу та культура безпеки. Технічні рішення не завжди покривають ситуації, коли зловмисник маскується під іншу особу. Традиційні методи потребують гнучкості та адаптації до нових реалій, оскільки вони орієнтовані на відомі атаки та неефективні проти нових технік, таких як цільовий фішинг або багатоетапні атаки з психологічним впливом. Регулярний перегляд політик, навчання та моніторинг необхідні для підтримки ефективності захисту.

1.3. Методи та підходи до оцінювання стійкості користувачів до соціоінженерного впливу

Оцінка людського фактору є пріоритетною задачею, що поєднує методи поведінкових наук, інженерії ризику, прикладної статистики. Сучасні підходи до неї розвинулися від простих опитувань і переліків до складних комбінованих методів. Це дозволяє виміряти не лише знання, а й поведінку, приховані упередження, реакцію на тиск і стійкість користувачів. На практиці підходи до оцінки людського чинника - це спектр методів: інструменти самооцінки,

стандартизовані опитувальники для виявлення знань і ставлення, контрольовані експерименти, симуляції, методи аналізу надійності людини (HRA), агент-орієнтоване моделювання поведінки, машинне навчання для прогнозування ризиків. Ці підходи часто комбінують у гібридні оцінки, щоб компенсувати недоліки кожного окремого інструменту. Далі розглянуто деякі підходи для оцінки впливу людського фактору.

Опитування, анкети, інтерв'ю, фокус-групи - це класичні соціологічні та психологічні інструменти для оцінки користувачів. Вони є основою для отримання даних про знання, установки, самовідчуття користувачів щодо загроз і процедур, корпоративну культуру. Ці інструменти корисні для попередньої діагностики, сегментації аудиторій і формування навчальних програм. Однак вони мають упередження самооцінки та соціально бажаної відповіді. Тому сучасні програми оцінки поєднують опитування з поведінковими тестами, щоб зіставити знання з діями.

Поведінкові симуляції (контрольовані фішингові кампанії, сценарії vishing/smishing, baiting або багатоканальні атаки) - це основний інструмент оцінки, оскільки вони вимірюють реакцію користувача в умовах, наближених до реальних. Такі симуляції дозволяють будувати базові лінії, проводити A/B-експерименти різних форматів навчання, а також виявляти підрозділи або ролі з підвищеним ризиком. Важливо розробляти валідні, етичні та контекстно-релевантні сценарії для коректного вимірювання та інтерпретації метрик.

Формалізовані підходи Human Reliability Analysis (HRA), запозичені з галузей з високим рівнем ризику (енергетика, авіація, хімічні процеси) застосовують у кібербезпеці для оцінки ймовірності людських помилок і їхнього внеску в інциденти. HRA-методики дозволяють розкласти завдання, визначити чинники впливу, оцінити частоту помилок і змоделювати ефект контрзаходів. Щоб перенести HRA в інформаційну безпеку, потрібно адаптувати його до цифрового контексту. Це дозволить інтегрувати людський фактор у загальні моделі ризику.

Теорії прийняття рішень (адаптована теорія сигнал-детекції (SDT) або модель сприйнятливості до фішингу (PSM)) потрібні для інтерпретації того, як користувачі відокремлюють реальні повідомлення від фішингових. SDT дозволяє розрізняти чутливість до шахрайства та схильність до помилкових спрацьовувань, а PSM структурує стадії атаки та чинники вразливості.

Агент-орієнтовані моделі та методи машинного навчання дозволяють змоделювати взаємодію індивідів у мережі, перевірити, як правила поведінки або зміни в політиках вплинуть на ризик. ML-моделі можуть прогнозувати групи високого ризику на основі історичних патернів поведінки. Це дозволяє пріоритезувати втручання та ресурси, але потребує якісних даних, етичних гарантій і зрозумілих моделей для прийняття рішень.

Якісні методи (кореневий аналіз причин, інтерв'ю після інцидентів, розбори сценаріїв) важливі для розуміння мотивацій і контексту: чому користувач клікнув, не скористався процедурою перевірки, які чинники сприяли помилковій дії. Поєднання якісних і кількісних даних дозволяє створювати профілі вразливості та персоналізовані траєкторії, що підвищує ефективність програм обізнаності. Важливо вимірювати динаміку: повторні симуляції, відстеження ефекту, оцінка втоми від тестів і виявлення побічних ефектів.

Сучасні підходи мають обмеження: опитування можуть містити упередження, симуляції впливати на моральний стан співробітників і викликати етичні питання, HRA вимагає детального опису завдань і не завжди враховує мінливий цифровий контекст, ML-моделі залежать від якості даних і можуть відтворювати упередження. Тому потрібно поєднувати методи, дотримуватися етичних правил, забезпечувати репрезентативну вибірку і статистичну коректність.

У науковій літературі описано багато методик тестування користувачів: опитування, лабораторні експерименти, польові симуляції, червоне командування й інтегровані соціально-технічні оцінки. Логіка таких досліджень - відтворити або змоделювати сценарій маніпуляції, отримати дані про реакції людей, виміряти поведінкові індикатори (кліки, час реакції, повідомлення про

підозри) і зробити висновки про вразливість і ефективність контрзаходів. Виділяють три методологічні групи: опитувальні дослідження, лабораторні експерименти та польові симуляції. Кожна з них дає різні знання та має свої сильні сторони. Наприклад, опитування корисні для виявлення чинників ризику, лабораторні дослідження дозволяють контролювати змінні, а польові симуляції дають дані про поведінку людей у реальному робочому середовищі.

Опитування застосовуються для визначення чинників, пов'язаних із вразливістю: рівень цифрової грамотності, довіра до джерел інформації, особистісні характеристики, навантаження і участь у тренінгах. Такі методи часто поєднують з експериментами, наприклад, тест-листами або віртуальними завданнями, щоб пов’язати самооцінку з поведінкою. Лабораторні експерименти дозволяють тестувати механіки соціальної інженерії, наприклад, порівнювати реакцію на масові фішингові листи та таргетовані spear-phishing-повідомлення, перевіряти налаштування повідомлення під контекст жертви або визначати, чи зменшує критичний текст кількість кліків. Такі есперименти забезпечують причинно-наслідкові інтерпретації, але їхня зовнішня валідність може бути обмеженою через штучність умов. Польові симуляції (розсилки фіктивних фішинг-листів, red-team сценарії з телефонними дзвінками, фізичними проникненнями і багатоетапними атаками) дають дані, які інформують політику організацій і стратегії навчання. Однак ці підходи потребують етичного й юридичного супроводу, щоб не завдати шкоди персоналу і зберегти довіру.[17]

У наукових роботах описані методи: OSINT-підготовка і персоналізація сценаріїв, симулятори spear-phishing, think-aloud і інтерв’ю після інциденту для розбору мотивацій і ментальних моделей користувачів, а також User/Entity Behavior Analytics (UEBA)-підходи, які поєднують технічний логінг з моделями поведінки для виявлення аномалій, що можуть свідчити про успішну компрометацію. Комбінація кількісних і якісних методів дає можливість виявити не лише тих, хто попався, а й зрозуміти чому. Це важливо для розробки курсів і змін у процесах. Мета методик зміщується від простого «виявити вразливих» до «вбудувати навчання й оцінку у процеси організації». Це означає, що популярні

підходи включають програми з симуляціями, автоматичне надсилання навчальних модулів тим, хто провалив тест, A/B-тести для оптимізації навчання та моніторинг впливу на інциденти. Тренінги підвищують стійкість користувачів, проте стандартизовані, персоналізовані й повторювані втручання дають найкращий ефект.

При аналізі вразливості людини до соціальної інженерії, часто орієнтуються на низку показників, які умовно можна поділити на поведінкові реакції та суб'єктивне сприйняття чи оцінку ризику. Нижче наведено таблицю з найбільш вживаними показниками. (табл. 1.3)

Таблиця 1.3

Показники сприйнятливості користувачів

Показник	Що фіксує	Обмеження
Click-rate (Коефіцієнт кліків)	Частка користувачів, які перейшли за підозрілим посиланням або виконали дію після отримання «приманки» (лист з повідомлення тощо)	Не показує кількість користувачів які майже натиснули, не враховує тих, хто відкрив лист, але не натиснув.
Конверсія (подальші дії) – введення даних, підтвердження, завантаження (наприклад, логін/пароль, завантаження вкладення тощо)	Наскільки далеко пішла атака чи лише був клік, чи користувач перейшов до критичного кроку.	Часто технічно або етично важко виміряти, не завжди можна перевірити, чи користувач дійсно передав дані.
Час реакції / час перевірки / time-to-click або time-to-decision	Як швидко користувач приймає рішення після отримання листа, чи дає собі час на обдумування	Швидкий клік не означає однозначну вразливість, можливо, користувач був упевнений, можливо, під тиском. Потрібен контекст ситуації.
Увага, перегляд елементів листа, візуально-когнітивні метрики (eye-tracking - fixations, dwell time, areas of interest)	Наскільки уважно користувач аналізує лист, чи звертає увагу на такі червоні прапорці, як адресу, заголовки, посилання, сигнали ризику	Не завжди корелює з правильним виявленням.

Продовження табл 1.3

Показник	Що фіксує	Обмеження
Self-report / оцінка ризику, сприйняття підозрілості	Наскільки користувач відчуває, що повідомлення може бути шахрайським, наскільки він довіряє чи не довіряє листу	Суб'єктивність, соціально-бажана відповідь, якщо люди знають, що проходять тест на фішинг, можуть відповідати адекватно, але на практиці діяти інакше.
Повторюваність / "resilience over time" / temporal метрики	Чи змінюється поведінка після навчання, чи користувачі стають менш сприйнятливими згодом.	Результати часто показують, що класичні тренінги не дають значного довготривалого ефекту, також зміни можуть бути зумовлені іншими факторами
Reporting-rate	Наскільки часто користувачі повідомляють про підозрілі повідомлення замість просто ігнорувати	Не всі звіти повідомляють про зловмисні дії: може бути надмірне повідомлення, або навпаки, користувачі могли просто ігнорувати лист, а не перевіряти. Трудно передбачити мотивацію повідомлення.

Формалізовані показники дозволяють кількісно оцінювати вразливість, здійснювати порівняння між групами або після навчальних заходів, відстежувати зміни, генерувати статистичні дані та створювати звіти для керівництва чи політики безпеки. Крім того, вони дають змогу проводити дослідження, що базуються на емпіричних даних, таких як поведінкові, когнітивні та міжособистісні аспекти, а не на інтуїції чи експертних судженнях.

Проте існують певні обмеження. Не всі показники однаково точно відображають реальну сприйнятливість, і деякі з них надмірно залежать від контексту. Наприклад, відстеження погляду показує, куди дивився користувач, однак не гарантує правильне розуміння отриманих ним сигналів. Показник кліків є простим, але загальним інструментом, що не надає інформації про причини кліків. Звітність, зі свого боку, залежить від організаційної культури, мотивації повідомляти та уникнення небажаної уваги.

При оцінці стійкості користувачів до соціоінженерних впливів коли говорять про людський фактор, мають на увазі, що користувач, це не просто «слабка ланка», а активний суб'єкт з власними психологічними, когнітивними, емоційними, соціальними та поведінковими характеристиками. Ці

характеристики можуть робити людину більш або менш стійкою до соціоінженерних атак.

На психологічному рівні важливу роль відіграє довіра. Особи, схильні довіряти іншим, особливо керівництву, колегам, технічній підтримці або службі безпеки, можуть бути більш уразливими до атак, де зловмисник видає себе за довірену особу. У таких випадках навіть сумнівні сигнали, такі як підозрілі адреси або нетипові запити, можуть ігноруватися, якщо джерело вважається надійним. Довірливість, як риса особистості або соціальна установка, стає основою для успішних атак з використанням соціальної інженерії. Сприйнятливість користувача до швидкої реакції під впливом часу чи емоцій, без перевірки деталей, значно підвищує ризик успішної атаки. Когнітивні властивості, такі як оцінка ризику, схильність до сумнівів і критичне мислення, також мають велике значення. Чим вища здатність людини розпізнавати нетипові ситуації, перевіряти інформацію та аналізувати деталі, тим нижча ймовірність успішної атаки.

Соціальні та ситуаційні чинники теж мають значення, наприклад, становище в організації, роль, рівень навантаження, кількість обов’язків, доступ до інформації, організаційні процедури, корпоративна культура безпеки. Працівники із великою зайнятістю, стресом, браком часу або з великою кількістю повідомлень, можуть бути уразливішими, адже менше часу на аналіз та більше імпульсивності. Емоційні стани, такі як, страх, тривога, спантеличення, стрес, втому, перевантаженн роблять людину психологічно вразливішою. Зловмисники часто створюють контекст тиску, терміновості, загрози або нагороди, усе, щоб викликати емоційну реакцію й обмежити раціональний аналіз. Більш того, під час особистих криз, війни, нестабільності, зміни умов, психологічна вразливість зростає, і саме такі періоди часто стають сприятливими для складних маніпуляцій.

При оцінці стійкості користувачів до атак, що використовують методи соціальної інженерії, слід враховувати широкий спектр факторів, включно з психологічними рисами, когнітивними здібностями, емоційним і соціальним

станом, досвідом, обізнаністю, поведінковою культурою та контекстом. Саме комбінація цих факторів визначає стійкість або вразливість людини чи групи до маніпуляцій.

Оцінка стійкості спирається на різні способи з різними перевагами та недоліками - від експертних оцінок і анкетування до поведінкових експериментів, симуляцій та автоматизованої аналітики. Ці підходи часто поєднуються, оскільки жоден окремий метод не забезпечує повного розуміння людського фактора. Експертні оцінки корисні для швидкого збору інформації за відсутності даних, анкетування дає змогу виявити рівень знань і установок у великих групах, поведінкові тести та симуляції відтворюють реальні дії в умовах, які максимально наближені до робочих, технічна аналітика (UBA/UEBA, логування) дає змогу виявити тривалі закономірності аномальної поведінки, а лабораторні методи використовуються для вивчення когнітивних процесів. [18]

Нижче приведено порівняння типових індикаторів і ключових обмежень. (табл. 1.4)

Таблиця 1.4

Переваги і обмеження методів оцінювання

Метод	**Типові індикатори**	**Переваги**	**Обмеження**
Експертне оцінювання	Рейтинги ризиків, ймовірностей, пріоритетів заходів	Швидко дає контекстні оцінки. Корисна при дефіциті даних	Суб'єктивність, упередження, важко валідувати
Анкетування / опитування	Рівень знань, самооцінка, готовність звітувати	Масштабованість, простота збору	Соцбажаність, розрив між заявами й поведінкою
Симуляції (phishing campaigns)	Click-rate, conversion, reporting-rate, time-to-click	Пряма поведінкова інформація, тест інтервенцій	Етичні/юридичні питання, варіативність складності
Лабораторні методи	Fixations, dwell time, нейрофізіологічні реакції	Глибоке розуміння уваги й процесів ухвалення рішень	Висока вартість, низька зовнішня валідність
UBA / UEBA аналітика	Аномалії в логах, відхилення патернів	Моніторинг у реальному часі, масштаб	Хибні спрацьовування, потреба в baseline і налаштуванні

Продовження табл. 1.4

Метод	Типові індикатори	Переваги	Обмеження
Експериментальні дизайни (A/B, контрольні групи)	До/після показники, статистична значущість	Оцінка причинності, перевірка інтервенцій	Потреба у ресурсах, плануванні, етичні обмеження

Висновки до розділу 1

У розділі розглянуто теоретичні засади протидії соціоінженерним загрозам в контексті забезпечення інформаційної безпеки організацій. Особливу увагу приділено систематизації підходів до розуміння сутності соціальної інженерії, що дозволило надати формалізоване визначення цього поняття як цілеспрямованого використання маніпулятивних технік для отримання несанкціонованого доступу до інформаційних активів через вплив на поведінку співробітників.

Проведена класифікація методів реалізації соціоінженерних атак, що охоплює як традиційні інструменти (фішинг, SMS-фішинг, вішинг), так і сучасні гібридні підходи, які поєднують технічні та психологічні засоби, зокрема із використанням штучного інтелекту, соціальних мереж та deepfake. Це дозволяє глибше зрозуміти динаміку еволюції загроз та адаптивність методів атак.

На основі аналізу сучасних підходів, що застосовуються в організаціях для запобігання соціоінженерним атакам, виявлено, що більшість практик залишаються фрагментованими, орієнтованими переважно на формальне навчання або використання окремих технічних засобів. Водночас недостатньо уваги приділяється інтеграції навчальних, організаційних та поведінкових заходів у єдину систему управління інформаційною безпекою.

Оцінка впливу соціоінженерних атак на концепцію управління інформаційною безпекою організацій показала, що ці атаки не лише створюють ризики витоку інформації, а й підривають довіру до засобів безпеки, викликають порушення регламентів, впливають на репутацію та можуть мати юридичні наслідки. Узагальнення чинників сприйнятливості працівників до

маніпулятивного впливу засвідчило, що критичними є не лише рівень обізнаності, а й організаційний контекст: культура безпеки, соціальна динаміка в колективі, управління стресовими станами та цифрова поведінка працівників.

Загалом, результати першого розділу сформували комплексне уявлення про соціальну інженерію як багатовимірну загрозу, що вимагає міждисциплінарного підходу до протидії. Теоретичне підґрунтя, викладене у розділі, забезпечує основу для розроблення методологічних і практичних рішень, які будуть розглянуті у наступних частинах дослідження.

РОЗДІЛ 2 АНАЛІЗ ВЕКТОРІВ СОЦІОІНЖЕНЕРНИХ ЗАГРОЗ І ПІДХОДІВ ДО ЇХ ІМІТАЦІЇ

Цей розділ закладає основу для переходу від теоретичного розуміння загроз соціоінженерії до практичних інструментів, від класифікації загроз і аналізу каналів атаки, до вибору і розробки сценаріїв для оцінювання стійкості персоналу та інформаційних систем. Такий підхід дозволяє побудувати комплексну, адаптивну систему кібербезпеки з урахуванням людського фактора і динамічних ІТ-середовищ.

2.1. Ідентифікація основних напрямів реалізації соціоінженерних атак у контексті сучасних інформаційно-комунікаційних систем

Соціальна інженерія в сучасних інформаційних системах реалізується різними способами, і її методи стали набагато ширшими, ніж раніше. Зараз зловмисники використовують як звичайні засоби, як-от електронна пошта, телефон і фізичний доступ, так і нові технології, як-от месенджери, мобільні пристрої, хмарні сервіси та штучний інтелект. Вони пристосовують свої дії до конкретної ситуації жертви та її інфраструктури, що збільшує їхні шанси на успіх. Ці дії можна поділити на кілька схожих, але різних за технікою та психологічним впливом категорій.

Фішинг електронною поштою є одним з найпоширеніших методів. Зловмисники надсилають електронні листи, які виглядають як офіційні повідомлення від банків, служб підтримки, партнерів або знайомих. У цих листах містяться підроблені посилання або вкладення, які перенаправляють на фальшиві сайти або завантажують шкідливі програми для крадіжки логінів, паролів, фінансових або особистих даних. Цей спосіб є масовим, його легко розширити, і навіть досвідчені користувачі можуть стати його жертвами, особливо якщо повідомлення викликає сильні емоції.

Spear phishing (цільовий фішинг) застосовується, коли атака спрямована на конкретну людину або організацію. У цьому випадку зловмисники спочатку аналізують жертву: її посаду, коло спілкування, проєкти, стиль роботи та внутрішні правила. Це робиться для того, щоб створити лист або повідомлення, яке максимально відповідає професійному чи соціальному контексту жертви та викликає довіру. Персоналізація, увага до деталей і знання внутрішніх процесів роблять такі атаки набагато небезпечнішими, ніж звичайний масовий фішинг.

Соціальна інженерія активно використовує телефонні дзвінки та SMS, що відомі як вішинг і смішинг. Зловмисники телефоном або SMS можуть представлятися службою підтримки, банком або іншою організацією, якій довіряють. Вони створюють ситуацію терміновості або пропонують допомогу, щоб змусити жертву надати особисту інформацію або виконати дії, які дають доступ до систем. Оскільки люди звикли швидко відповідати на дзвінки або повідомлення, такі атаки можуть обійти технічні засоби захисту, особливо якщо вони подаються як термінові.

Окрім цифрових-каналів, важливі також фізичні або комбіновані методи. Один з них - baiting, коли зловмисник залишає заражений USB-накопичувач або інший носій у громадському місці або на території компанії, сподіваючись, що хтось підключить його до комп'ютера. Також можливі спроби проникнення в будівлі або підробка посвідчень, щоб отримати доступ до обладнання або систем. Ці методи поєднують психологічні маніпуляції та використання людського фактора, що робить їх серйозною загрозою, особливо в компаніях із комбінованою IT/офлайн інфраструктурою або слабким фізичним контролем.

Ще варто виділити два види напрямів реалізації соціоінженерних атак, які тісно інтегруються в інформаційно-комунікаційні системи й посилюють загальну небезпеку, а саме, атаки на хмарні облікові записи (cloud credential harvesting) та QR-код фішинг (quishing). Атаки на хмарні облікові записи часто починаються з класичних соціально-інженерних прийомів - фішинг-кампаній, цілеспрямованих повідомлень або spear-phishing операцій, але, при цьому, їхня кінцева мета відрізняється: зловмисники прагнуть «збирати» облікові дані,

одноразові токени або сесійні ключі, які дають безпосередній доступ до хмарних сервісів, корпоративної пошти, сховищ документів і систем управління профілями. Після отримання таких даних атакуючі виконують takeover (захоплення облікового запису), що дозволяє їм читати кореспонденцію, ініціювати платіжні операції, змінювати налаштування автентифікації, розповсюджувати шкідливі посилання від імені легітимного користувача або рухатися латерально в екосистемі постачальників і партнерів. В деяких випадках атака на один хмарний акаунт стає стартовою точкою для масштабних компрометацій у ланцюгу поставок. З огляду на те, що корпоративні та персональні дані дедалі частіше зберігаються й використовуються в хмарі, кампанії, спрямовані на збір облікових даних, стали одним із головних векторів порушень безпеки - їх підсилюють як традиційними методами, такими як злами, витоки паролів, так і нові тактики з підробкою повідомлень від служб підтримки хмарних сервісів або імітацією систем багатофакторної автентифікації з метою збору OTP/токенів. [22]

QR-код фішинг (quishing), являє собою інший сучасний напрямок, що використовує особливості комунікації, такі як, масове поширення QR-кодів у рекламі, наклейках, меню ресторанів, документах PDF та у внутрішніх розсилках робить цей канал привабливим для зловмисників. Замість класичного кліку на URL у листі жертві пропонують відсканувати код - дія, яка зазвичай виконується на мобільному пристрої, поза традиційними email-фільтрами та без можливості переглянути посилання перед переходом. Після сканування користувача спрямовують на підроблений сайт для збору логінів або платіжних даних, або запускають завантаження шкідливого мобільного додатка. Інший варіант має на увазі розміщення QR-коду всередині PDF-документа або електронного листа, який обходить сканери посилань, бо посилання зашифровано в зображенні. Через легкість розповсюдження QR-кодів і те, що люди часто довіряють коду на друкованому носії або в офіційному листі, quishing став популярним інструментом як проти споживачів (фінансові шахрайства, підроблені платіжні

сторінки), так і проти співробітників організацій (введення облікових даних у фейкові форми для доступу до корпоративних сервісів).

Ці методи поєднують технічні інструменти та соціальні маніпуляції. Cloud credential harvesting часто вимагає попереднього збору інформації про організацію, її постачальників і співробітників, а також психологічного впливу, щоб завоювати довіру жертви або змусити її виконати потрібну дію. Quishing використовує звичку довіряти графічним знакам і сканувати QR-коди у громадських місцях або в документах, обходячи звичайні фільтри. Обидва ці підходи особливо небезпечні під час віддаленої роботи та в гібридних інфраструктурах, де користувачі працюють із хмарними сервісами з особистих або корпоративних пристроїв, часто поза контролем корпоративних мереж.

Далі буде розглянуто нові види соціоінженерних атак, які з'явилися завдяки розвитку штучного інтелекту. ШІ є ключовим інструментом, що дозволяє автоматизувати масові розсилки та робити їх більш персоналізованими. Завдяки високій правдоподібності, яку забезпечує штучний інтелект, зловмисники можуть успішно впливати на велику кількість людей, докладаючи менше зусиль та збільшуючи свої шанси на успіх. [46]

Найпростішим прикладом можливостей генеративного ШІ є створення реалістичного контенту. Наприклад, у випадку фішингу, штучний інтелект може швидко клонувати справжні вебсайти та змінювати їх, щоб обманути жертв, створюючи більш переконливі фішингові сторінки. Ще більше занепокоєння викликає здатність генеративного штучного інтелекту створювати різні види текстів і медіа:

- текст: створює переконливі електронні листи, текстові повідомлення або дописи в соціальних мережах, які виглядають як написані людьми. Ці повідомлення можуть бути налаштовані для конкретних людей або організацій;
- зображення: створює реалістичні зображення, як-от підроблені посвідчення, офіційні логотипи або відредаговані фотографії, щоб фішингові або соціально-інженерні атаки виглядали більш правдоподібно;

- голос: створює реалістичні голосові записи або здійснює вішинг, представляючись довіреними особами або організаціями по телефону;
- відео: створює дуже реалістичні відео з використанням технології діпфейків, які змінюють зовнішність і голос реальних людей. Такі відео можуть використовуватися для поширення неправдивої інформації, видавання себе за керівників або відомих людей, а також для введення цілей в оману, щоб змусити їх до певних дій.

Ці маніпулятивні медіа виглядають дуже реалістично і можуть ввести людей в оману, змушуючи їх вірити в неправдиві історії або події. Діпфейки викликають велике занепокоєння через їхню здатність поширювати неправдиву інформацію та руйнувати довіру до візуальних і аудіальних доказів. У контексті соціальної інженерії та фішингу, діпфейки можуть бути створені на основі особистої візуальної та аудіоінформації. [52] Ця інформація може бути зібрана з відкритих джерел, закритих джерел або надана іншими зловмисниками. Поєднання все більшої кількості особистої інформації та вдосконалених можливостей діпфейків може бути використано для наступних цілей:

- видавання себе за іншу людину: створюючи майже ідеальну візуальну та аудіо імітацію довіреної особи, як-от колеги, друзі або члени сім'ї, зловмисники можуть переконати жертв виконати завдання або надати особисту інформацію;
- обхід біометричних систем: деякі системи безпеки, які використовують розпізнавання обличчя або голосу, можуть бути обмануті за допомогою діпфейків, що надає несанкціонований доступ;
- вимагання викупу: зловмисники можуть створювати скандальні або компрометуючі діпфейки людей, а потім погрожувати їх оприлюднити, якщо не буде сплачено викуп;
- дезінформація: діпфейки можуть поширювати неправдиву інформацію або пропаганду, яка виглядає правдивою, що може викликати паніку, впливати на громадську думку або навіть впливати на поведінку фондового ринку.

Розвиток ШІ не обмежується лише візуальними маніпуляціями. Нещодавнє впровадження великих мовних моделей (LLM), як-от ChatGPT або Bard, відкрило нові можливості для зловживань у соціальній інженерії та фішингу. LLM можуть створювати дуже переконливі та персоналізовані фішингові електронні листи, які відповідають контексту жертви, що значно підвищує ефективність таких атак. Це також стосується всіх інших текстових каналів комунікації, як-от SMS або чати в соціальних мережах. Замість звичайних фішингових повідомлень, зловмисники можуть використовувати LLM для спілкування з жертвами в режимі реального часу, змінюючи розмову, щоб ефективніше маніпулювати ціллю. Крім того, ці моделі швидко розвиваються і набувають нових можливостей, що виходять за межі створення тексту (наприклад, ChatGPT Code Interpreter). Новою проблемою, пов'язаною з просунутими системами ШІ, є можливість обходу встановлених обмежень або правил використання (jailbreaking). Зловмисники, знаходячи вразливості в інтерфейсах або системах контролю доступу, можуть використовувати можливості ШІ не за призначенням. У контексті соціальної інженерії та фішингу такий необмежений доступ може зробити шахрайські кампанії набагато складнішими для виявлення. [1]

Важливо зазначити, що атаки із застосуванням соціальної інженерії часто використовують декілька методів одночасно. Зловмисники можуть почати з фішингового листа, потім здійснити телефонний дзвінок, використати фальшивий сайт або завантажити шкідливе ПЗ через USB, і завершити атаку через внутрішні системи або мережу партнера. Така комбінація технічних, психологічних і фізичних методів дозволяє обійти багато рівнів захисту й ускладнює виявлення атаки на ранніх стадіях.

У сучасних інформаційних системах, де користувачі працюють через email, месенджери, телефон, мобільні пристрої, хмарні сервіси, VPN або віддалені робочі середовища, соціальна інженерія має велику перевагу над технічним зламом. Вона використовує слабкості в поведінці людей, організаційних процедурах, корпоративних процесах, комунікаційних каналах і

довірі. У таких умовах, навіть якщо технічний захист є надійним, атака через маніпуляцію людиною або процесами може бути більш результативною і складною для виявлення та запобігання.

Соціоінженерні атаки зазвичай націлені на отримання особистої інформації, як-от внутрішня документація, дані співробітників і клієнтів, комерційні таємниці або технологічні розробки, оскільки ця інформація є цінною для конкурентів або зловмисників. Важливою метою є також отримання доступу до корпоративних систем і ресурсів, наприклад, контроль над обліковими записами, внутрішніми серверами, мережевими сегментами або адміністративними панелями, що дозволяє зловмисникам розширювати свої права, закріплюватися в інфраструктурі або запускати технічні атаки. Також метою є фінансові активи, як-от грошові перекази, компрометація платіжних систем, вимагання або шахрайські операції, спрямовані на отримання прибутку за рахунок організації. Ці цілі часто поєднуються: доступ до інформації дозволяє створювати більш переконливі сценарії обману, контроль над системами полегшує виведення грошей, а фінансова вигода стимулює створення складних схем впливу на персонал.

2.2. Аналіз існуючих методів тестування користувачів на сприйнятливість до соціоінженерних впливів

Аналіз наявних методів тестування користувачів на вразливість до соціальної інженерії показує використання різноманітних підходів: від опитувань до складних симуляцій, збору даних про поведінку та їх інтеграції в програми безпеки. Опитування (анкети, тести, запитання) оцінюють знання користувачів про загрози, наприклад - знання про фішинг, розпізнавання підозрілих листів, правила поводження з паролями. Такий підхід є первинною діагностикою, що дозволяє охопити багато людей, оцінити базові знання та виявити їх прогалини.

Продовжуючи тему тестування користувачів до соціальної інженерії сьогодні дедалі більше спирається на академічні дослідження та емпіричні експерименти - це дає змогу не лише перевірити, чи «натиснуть» на фішингове посилання, а й зрозуміти, чому людина це зробила, за яких умов, з якими психологічними, контекстуальними й організаційними тригерами. Одним із таких підходів є багатовимірне моделювання схильності до фішингу. Наприклад, у дослідженні Predicting User Susceptibility to Phishing Based on Multidimensional Features (2022) автори запропонували модель, яка на основі низки ознак, демографічних, поведінкових, психологічних, історії користувача, прогнозує ймовірність того, що конкретна особа стане жертвою фішингу. Це означає, що тестування може бути не лише постфактум, а превентивним - оцінити схильність до ризику ще до того, як атака буде зроблена.

Для більш практичної перевірки і значно глибшої діагностики, застосовують симуляції соціоінженерних атак, зокрема симуляцію фішингу. Під час її проведення організація створює контрольоване «тренувальне середовище», яке імітує реальні умови роботи: поштовий клієнт, веб-браузер, корпоративні комунікації. У такому середовищі відправляють фішингові, смішингові чи інші типи повідомлень, або створюють фейкові сайти, запити на введення даних, щоб перевірити, чи користувачі натиснуть на підозрілі посилання, спробують ввести свої паролі або нададуть іншу конфіденційну інформацію. Після того, як співробітники або користувачі отримали такі листи, аналізують, скільки з них натиснули на посилання, відкрили вкладення, ввели дані, чи повідомили про підозру - таким чином оцінюється реальна сприйнятливість.

Однак в аналізі сучасної практики тестування видно і суттєві проблеми. Наприклад, в дослідженні «Anti-Phishing Training (Still) Does Not Work: A Large-Scale Reproduction of Phishing Training Inefficacy Grounded in the NIST Phish Scale» було показано, що стандартні тренінги з підвищення обізнаності не дають суттєвого зниження кількості кліків на фішинг-листи або підвищення частоти повідомлень про підозріле. [2] Це означає, що навіть якщо організація проводить регулярно навчання, без системного підходу та оновлення підходів, ефективність

може бути низькою. При цьому в дослідженні показано, що шкала складності фішингових листів корелює з поведінкою, а саме чим ретельніше підготований лист - тим більша ймовірність, що користувач зробить те що зловмисник просить зробити в листі.

Ще один підхід - застосування даних поведінки користувачів у поєднанні з технічними та аналітичними засобами, як приклад дослідження «ADVERT: An Adaptive and Data-Driven Attention Enhancement Mechanism for Phishing Prevention» використовує eye-tracking, щоб аналізувати, на які елементи листа користувач дивиться: чи звертає увагу на URL, домен, підказки, невідповідності, орфографію тощо. Також система ADVERT, використовує таку методологію: під час взаємодії з листом відстежується, на що саме користувач дивиться, як розподілено його увагу, і на цій основі оцінюється, чи потенційна атака буде помічена, чи пройде непомітно. В експериментах це підвищувало точність розпізнавання фішингу порівняно з контрольним рівнем. [3]

Доповнюючи сказане вище можна сказати, що багато досліджень і симуляцій робляться у контрольованому середовищі, яке не повторює реального навантаження, емоційного стану, багатозадачності, часу, відволікань. Відповідно результати можуть бути не об’єктивними, тобто реальна сприйнятливість користувачів може бути значно вищою, ніж було показано при проведенні тестування. Це ставить питання про валідність і репрезентативність таких тестів.

Ще можна виділити дослідження «Sustaining Cyber Awareness: The Long-Term Impact of Continuous Phishing Training and Emotional Triggers» в якому було проаналізовано ефект безперервних симуляцій фішингу з урахуванням емоційних, контекстуальних тригерів протягом 12 місяців у реальних організаціях. [4] Це дозволяє оцінити не просто один інцидент, а динаміку, чи зменшується сприйнятливість, чи зростає здатність розпізнавати шахрайство з часом, чи повертаються помилки, наприклад, через зміну складу співробітників, стресове навантаження або втому. Такий підхід набагато ближчий до реального життя організацій, ніж класичні короткострокові експерименти, і дає більш цінну інформацію для формування політики безпеки.

У науковій та корпоративній практиці часто поєднують симуляції з навчанням (тренінгами) та подальшим перевірочним тестуванням - тобто моделюють атаку, дають користувачам фідбек або освіту, а потім знову тестують, щоб перевірити, чи змінилася поведінка. Це дозволяє не просто діагностувати вразливість, а й оцінити ефективність заходів безпеки, змін у культурі компанії, здатність персоналу реагувати правильно. Такий підхід розглядається як одна з ключових стратегій підвищення стійкості до соціальної інженерії.

Окремо використовуються методи соціо-технічного тестування, інтегровані в загальний процес оцінки безпеки - наприклад, в рамках комплексних тестів на проникнення (pentesting), коли крім технічної перевірки вразливостей мереж і програм, тестується людський фактор, а саме, чи може співробітник опинитися мішенню, чи реагує на фішинг, чи дотримується політик безпеки. Такі методи включають емульовані атаки, аналіз поведінки, повідомлень, реакцій, а також перевірку фізичного доступу, верифікації запитів, перевірок ідентичності. У таких тестах важливо аналізувати не лише кількість вдалих/невдалих спроб атаки, а й які саме умови, комбінації факторів (текст листа, контекст, психологічний тиск, зовнішні стимули) призводили до успіху.

Додатковими методами тестування є інтеграція технологій штучного інтелекту та машинного навчання для генерації тестових сценаріїв (AI-driven simulations). Сталі методи симуляції часто страждають від шаблонності: зловмисники постійно вдосконалюють свої тактики, тоді як навчальні кампанії із аналізу соціального сприйняття часто використовують статичні бібліотеки листів завдяки яким співробітники швидко вчаться розпізнавати за формальними ознаками, а не за суттю загрози. Натомість, оновлені підходи передбачають використання великих мовних моделей (LLM) для створення персоналізованих сценаріїв атак (spear-phishing), які базуються на відкритих даних про співробітника (OSINT). Такі системи здатні автоматично генерувати контент, що враховує посадові обов'язки, стиль комунікації та навіть поточні проєкти жертви, що значно підвищує валідність тестування. Дослідження показують, що тести,

згенеровані штучним інтелектом, мають значно вищий показник успішності проникнення («click rate»), ніж створені людиною шаблони, що змушує організації переглядати свої оцінки вразливості персоналу в бік погіршення прогнозів.

Моделі тестування, залежно від типу атаки, відрізняються за цілями, реалізацією, метриками оцінки та обмеженнями. Для email-фішингу використовують автоматизовані кампанії з шаблонами листів різного ступеня персоналізації, класифікованими за складністю. Збираються дані про доставку, відкриття, перехід за посиланням, конверсію, повідомлення про підозру та час до кліку. Це дозволяє проводити A/B-експерименти та оцінювати ефект навчання. Для коректного дизайну симуляцій рекомендують оцінювати складність листа за інструментами на кшталт NIST Phish Scale та пов’язувати кожну пастку з навчальним зворотним зв’язком.

Тестування вішінгу відрізняється орієнтацією на сценарний, ручний і якісний компонент, замість масових автоматизованих розсилок в цьому методі зазвичай застосовують підготовлені сценарії дзвінків з імпровізованими скриптами та ролями, тренованими операторами або використанням технологій синтезу голосу для підвищення правдоподібності. Оцінюють не лише те, чи жертва надала інформацію під час дзвінка, а й проміжні сигнали, чи запросив користувач підтвердження, чи виконав дії після дзвінка. Через це вішинг-тести зазвичай дорожчі у виконанні і вимагають ретельної координації з HR і юриспруденцією, а також заздалегідь прописаних аварійних сценаріїв (щоб миттєво зупинити симуляцію, якщо вона може спричинити реальну шкоду). Реалістичність вишукує баланс між соціальним інженерним талантом оператора та контролем, і багато провайдерів радять комбінувати дзвінки з попередньою емейл-розвідкою для підвищення правдоподібності сценарію

Моделі для SMS-фішингу поєднують характеристики обох попередніх підходів, але мають власні технічні і поведінкові нюанси, а саме, симуляції здійснюються через масові або таргетовані SMS або месенджери з короткими повідомленнями, посиланнями або кодами і оцінюються за click-, conversion-rate,

reporting і часом реакції. Смс-канал - обмежений за простором для пояснення і сильно оперує на швидкій реакції та мобільній поведінці користувачів, тому в тестах зазвичай аналізують контекст, наскільки повідомлення виглядає «особистим», чи використовує воно OTP-провокації, посилання на клон-сторінки або QR-коди. Через особливості мобільних інтерфейсів деякі симуляції додають елементи, які імітують push-повідомлення або автоматизовані сервіси . Смс-симуляції зазвичай менш автоматизовані, ніж емейл-кампанії, і вимагають тестування на реальних мобільних середовищах.

Моделі тестування розрізняються за підходом до зворотного зв'язку. Для емейл-кампаній використовують миттєвий зворотний зв'язок та автоматичну прив'язку до мікро-курсів. Для вішингу проводять індивідуальний аналіз помилок або групові сесії. Всі моделі мають відповідати етичним вимогам: узгодження із зацікавленими сторонами, обмеження тем, конфіденційність результатів та підтримка учасників, щоб уникнути шкоди репутації або психологічних наслідків.

Продовжуючи тему про наслідки при проведенні тестів на реальних користувачах потрібно враховувати цілий спектр етичних та правових аспектів, інакше такі тести можуть призвести не до підвищення безпеки, а до порушень прав людей, етичних дилем та юридичних проблем. [29]

Важливо гарантувати конфіденційність і захист персональних даних, бо тестування передбачає збір інформації про дії користувачів, їхню поведінку, реакції, можливо навіть часові відмітки, введені дані, сторінки, які вони відвідували, тощо. Такі дані мають розглядатися як персональні або чутливі, і їх обробка повинна відповідати нормам, які регулюють приватність, захист даних і digital-права. Невиконання цього може призвести до порушення права на приватність та до юридичної відповідальності. Необхідна прозорість та обґрунтованість тестів. Організація, яка проводить симуляції, має мати чітку політику, документовані правила, які регламентують, коли і як такі тести проводяться, для яких цілей і як обробляються отримані дані. Це важливо, щоб користувачі не відчували себе під таємним наглядом чи маніпуляціями без їхньої

згоди, навіть якщо письмова згода не видається перед кожним тестом. Етичне ставлення передбачає, що люди мають право знати, що система може проводити тестування, і що їхні дані не будуть використані проти них лише в навчальних або оцінювальних цілях.

Також потрібно уникати каральних або стигматизуючих наслідків для учасників. Результати тестів не мають використовуватися для покарання, звільнення, приниження чи дискримінації, мета таких тестів має бути навчально-діагностичною, а не репресивною. Використання даних для дисциплінарних заходів підриває довіру співробітників до політики безпеки, породжує страх та опір, що може обернутися навпаки зниженням безпеки.

Не менш важливим є психологічний комфорт і безпека учасників. Симуляції соціоінженерних атак можуть викликати стрес, тривогу, відчуття, що їхню довіру зрадили, або почуття небезпеки, особливо якщо сценарій занадто реалістичний або включає емоційний тиск. Організатори мають передбачити підтримку, пояснення після тесту, забезпечувати, щоб учасники не переживали за свою безпеку, не відчували сорому чи страху за провал, а сприймали це як навчання. [37]

Юридично слід передбачити правову основу для обробки та зберігання даних, їхнім використанням, обмеженням доступу, знищенням після завершення тестів, а також відповідальністю за витоки або зловживання. Якщо збору даних не було погоджено або обробка відбувається без необхідних гарантій, це може суперечити закону про захист персональних даних або іншому релевантному регулюванню.

Етичність проведення передбачає, що мета таких тестів, це підвищення безпеки і обізнаності, а не експериментальна маніпуляція людьми без їхнього розуміння чи згоди. Симуляції мають бути спланованими, пропорційними, з урахуванням ризиків для психологічного та правового стану учасників. Тільки за таких умов тестування може вважатися етично виправданим і правомірним.

2.3. Оцінювання ефективності заходів із підвищення обізнаності користувачів та формування стійкості до маніпуляцій

В багатьох установах безпека вже не зводиться до технічних засобів, натомість фокусується на навчанні, психології та поведінці. Базовим заходом є систематичні програми навчання, які мають на меті ознайомити співробітників з типами небезпек (фішинг, соціальна інженерія, шахрайство, важливість безпечної поведінки) та виробити навички розпізнавання і реагування. Зазвичай навчання ділиться на основні курси для всіх і спеціалізовані модулі для різних груп залежно від ролі, рівня доступу чи діяльності. Такий підхід допомагає адаптувати контент, наприклад, для менеджерів, фінансистів, IT-фахівців, HR або віддалених працівників можуть бути різні сценарії, враховуючи їхні ризики.

Більш сучасні методи включають імітації атак і соціоінженерні тести, які дозволяють перевірити реакцію працівників на реалістичні ситуації. Це не просто навчання, а перевірка поведінки під впливом приманки. Після імітацій аналізують, хто клікнув, хто повідомив про підозріле, як швидко реагували, і на основі цього будують програми навчання.

Важливо регулярно оновлювати знання і повторювати тренінги. Оскільки способи соціальної інженерії постійно змінюються, одного разу навчити недостатньо, потрібна систематична, періодична освіта, яка пристосовується до нових ризиків, оновлює контент і нагадує про правила безпеки. Крім того, організації часто поєднують навчання, імітації, політики безпеки та технічні засоби для забезпечення багаторівневого захисту. У таких програмах важливо не тільки передати знання, а й сформувати культуру безпеки: звичку перевіряти листи, сумніватися у дивних запитах, повідомляти про підозрілі речі та дотримуватися процедур.

Для дієвої оцінки заходів з підвищення обізнаності потрібне поєднання чітких цілей, різних показників (click rate, reporting rate, time-to-report, knowledge scores, MFA adoption тощо), правильного експериментального дизайну (контрольні групи, A/B-тести, довготривалі дослідження), якісного аналізу

мотивів і контексту, технічної аналітики та інтерпретації результатів з точки зору бізнесу. Безперервність, адаптивність, персоналізація навчання і злагоджена робота з технічними засобами - запорука стійкості організації перед загрозами соціальної інженерії в довгостроковій перспективі. Для реалістичних очікувань і рішень рекомендується поєднання наукових методів і практичних показників з прозорою звітністю перед керівництвом.(табл. 2.1)

Таблиця 2.1

Оцінювання заходів з підвищення обізнаності

Напрям оцінювання	**Сутність**	**Типові показники/Метрики**	**Що дозволяє визначити**
Результати фішинг-симуляцій	Аналіз реакції користувачів на контрольовані імітації атак	Click-through rate, repeat offenders, reporting rate	Поточний рівень вразливості, динаміку покращення, здатність розпізнавати загрози
Довгостроковий моніторинг реальних інцидентів	Спостереження за поведінкою користувачів у реальних робочих умовах	Зменшення інцидентів, кількість повідомлень про підозріле, успішні/запобіглі атаки	Реальну ефективність навчання у робочих ситуаціях
Оцінка результатів навчальних модулів	Перевірка знань після тренінгів	Результати тестів, вікторин, виконання завдань	Рівень теоретичної підготовки та розуміння загроз
Аналіз поведінкових звичок та культури безпеки	Визначення того, як користувачі виконують правила у щоденній роботі	Дотримання політик, кількість “near miss”, відповідність процедурі	Реальну сформованість стійкої поведінки до атак
Аудит процедур і політик безпеки	Перевірка, наскільки заходи інтегровані в управлінські процеси	Compliance rate, результати перевірок	Якість внутрішньої інфраструктури підтримки безпеки
Психологічні й соціальні оцінки	Аналіз факторів довіри, схильності до ризику, впевненості користувачів	Опитування, самооцінювання впевненості, інтерв’ю	Бар’єри, що впливають на сприйнятливість до атак
Аналіз динаміки ефекту у часі	Вивчення, як змінюється стійкість через місяці/роки	Порівняння періодичних симуляцій, повторні вимірювання метрик	Стійкість навчального ефекту, ризик «втоми від безпеки»

Продовження табл. 2.1

Напрям оцінювання	**Сутність**	**Типові показники/Метрики**	**Що дозволяє визначити**
Оцінювання загальної кіберстійкості	Вплив навчання на системну безпеку	Зниження ризику, зменшення втрат, зростання рівня захищеності	Загальну користь навчання для організації

Оцінювання стійкості персоналу до методів соціальної інженерії - це не лише фіксація інцидентів чи підрахунок переходів за сумнівними посиланнями. Це складне аналітичне завдання, яке вимагає поєднання психологічних підходів, знань з теорії інформаційної безпеки та методів стохастичного моделювання. Діагностика захищеності системи передбачає перехід від виявлення вразливостей до з'ясування причин поведінкових відхилень, що потребує комплексної методології.

Імітаційне моделювання атак залишається основним способом перевірки теоретичних моделей загроз. Активні симуляції, такі як фішингові кампанії, дозволяють отримати реальну картину поведінки користувачів в умовах, наближених до реальних. Проте, просте вимірювання кількості кліків може дати неточну інформацію, якщо не враховувати контекст атаки. Тому сучасні тестування все частіше включають елементи фізичного проникнення або маніпуляції через корпоративні месенджери, формуючи гібридні вектори. Це дозволяє виявити не лише індивідуальні помилки, а й недоліки в процедурах реагування на інциденти.

Критичним недоліком багатьох симуляцій є суб’єктивність в оцінці складності тестових сценаріїв. Для об’єктивізації даних доцільно використовувати метрику NIST Phish Scale. Її цінність полягає в розділенні двох параметрів: видимих ознак атаки (cues) та контекстуальної відповідності (alignment). Практичне застосування цієї шкали дозволяє диференціювати результати: ігнорування користувачем примітивного спаму не є доказом його компетентності, тоді як помилка при обробці висококонтекстуального спір-фішингу (spear-phishing), адаптованого під специфіку посадових обов'язків,

свідчить про необхідність перегляду технічних, а не лише освітніх заходів захисту.

Поглиблений аналіз вимагає структурування сценаріїв за допомогою спеціалізованих фреймворків, наприклад, FIST (Fraud Incident Structured Threat Framework). На відміну від класичного Cyber Kill Chain, який фокусується на технічних етапах, FIST декомпозує інцидент через призму маніпулятивних технік на кожному етапі взаємодії з жертвою. Це дає змогу досліднику документувати не просто факт атаки, а конкретні психологічні важелі (претексти), що спрацювали. Такий підхід трансформує розрізнені дані логів у структуровану базу знань (Threat Intelligence), необхідну для прогнозування майбутніх векторів атак.

В основі оцінювання лежать моделі прогнозування, приклад такої Phishing Susceptibility Model (PSM). Вона розглядає вразливість як залежність від когнітивних процесів, емоційного стану, робочого контексту та організаційної культури. Використання PSM дозволяє визначати, чи пов'язаний успіх атак з часом доби, завантаженістю підрозділу або типом пристрою. Це зміщує фокус з пошуку винних користувачів на умови, що провокують помилки. [49]

Аналіз відмінностей у самооцінці та фактичній поведінці є важливим напрямом. Опитування часто показують, що люди з низькою кваліфікацією переоцінюють свою здатність захищатися (ефект Даннінга-Крюгера). Якісні методи, зокрема поглиблені інтерв'ю після інцидентів, допомагають зрозуміти, чому люди роблять неправильний вибір..

Для обробки результатів експериментів корисно застосовувати теорію виявлення сигналів. Вона дозволяє обчислити індекс чутливості та критерії прийняття рішень. Це допомагає визначити, наскільки добре працівники відрізняють безпечні листи від шкідливих, враховуючи інформаційний шум, і чи схильні вони до надмірної обережності чи недбалості. Такий аналіз дає більше інформації ніж звичайні відсотки.

Важливо враховувати психологічні фактори. Тому що, соціальна інженерія частіше спрацьовує, коли використовуються принципи впливу, такі як авторитет,

терміновість і дефіцит. Тому оцінювання включає аналіз профілів користувачів для визначення груп ризику. Люди з високою товариськістю можуть бути більш вразливими через соціальні зв'язки, що вимагає спеціальних заходів захисту для них.

Ключові показники ефективності (KPI) системи оцінювання також зазнають змін. Акцент зміщується з Click Rate на метрики резистентності, таких як Time to Report (час від отримання листа до повідомлення в SOC) та Reporting Rate (частка виявлених атак). Зростання Reporting Rate є індикатором зрілості культури безпеки, тоді як просто низький Click Rate може бути наслідком технічної фільтрації, а не обізнаності. Аналіз динаміки цих показників дозволяє будувати криві навчання та ідентифікувати «хронічно вразливих» користувачів.

Для аналізу складних систем доцільно використовувати нечітку логіку і теорію графів. Представлення організації у вигляді графа, де працівники та ресурси є вузлами, а зв'язки між ними - довірою, дозволяє виявити критичні шляхи поширення атаки. Нечітка логіка допомагає враховувати невизначеність при оцінці ймовірності атак, що неможливо зробити звичайними способами.

Тривала дія заходів щодо підвищення обізнаності про атаки залежить від технічних, організаційних, педагогічних і поведінкових факторів. Окремі заходи не дають стабільного ефекту, потрібна система, яка постійно підтримується і змінюється. Важливо, щоб керівництво підтримувало безпеку, виділяло кошти на навчання і власним прикладом показувало важливість повідомлень про проблеми. Це створює культуру, де навчання сприймається серйозно, інакше ініціативи швидко втрачають ефективність.

Частота і структура курсів є важливими, оскільки одноразові лекції дають короткий ефект. Розбиття інформації на невеликі частини з регулярним повторенням допомагає закріпити знання і зменшити забування. Програми, які поєднують короткі уроки, вправи та симуляції, краще зберігають ефект з часом, ніж звичайні лекції. Актуальність і персоналізація матеріалу ж, впливає на те, наскільки добре знання перетворюються на дії. Сценарії навчання повинні бути пов'язані з реальними ризиками і процесами в компанії, враховувати робочі

умови і змінюватися відповідно до нових видів атак. Якщо матеріал неактуальний або занадто загальний, працівники перестають звертати на нього увагу і повертаються до старих звичок.

Практичні методи, а саме симуляції з миттєвим зворотним зв'язком, покращують стійкість краще, ніж просто інформаційні модулі. Поєднання тестів з моментальною оцінкою змушує працівника відпрацьовувати потрібні дії. Важливо проектувати такі симуляції етично, щоб не навчити працівників неправильним реакціям (наприклад, автоматично натискати «повідомити» без аналізу) або не викликати втому від тестів.

Для тривалої роботи потрібно постійно оновлювати і навчати на основі даних. Збір відгуків, зміна матеріалу відповідно до нових технік атак, перевірка програми й підтримка знань викладачів перетворюють разову ініціативу на систему підвищення стійкості.

Висновки до розділу 2

У цьому розділі здійснено дослідження актуальних напрямів реалізації соціоінженерних атак у сучасних інформаційно-комунікаційних системах, а також методів їх імітації та перевірки стійкості користувачів. Проаналізовано широкий спектр технік соціального впливу від традиційних, таких як фішинг, pretexting, smishing, vishing, baiting, до новітніх гібридних тактик, у яких використовуються можливості штучного інтелекту, соціальних мереж та технологій deepfake для підвищення переконливості атак. Така класифікація дозволяє краще зрозуміти динаміку еволюції загроз і демонструє, наскільки сучасні атаки можуть бути багатоканальними та адаптивними.

Було проведено огляд існуючих методів тестування користувачів на сприйнятливість до соціоінженерних впливів який показав, що практики в організаціях часто залишаються фрагментованими, так як переважно застосовується формальне навчання або періодичні awareness-тренінги, поодинокі симуляції або тестування на фішинг, без системної інтеграції з

загальною політикою безпеки. У багатьох випадках імітації атаки виконуються як окремі «разові» заходи без подальшого аналізу, сегментації ризиків чи розвитку системи захисту. Це створює вразливість перед складнішими, багатоканальними атаками, особливо з урахуванням появи AI-підсилених схем.

Аналіз ефективності заходів із підвищення обізнаності показує, що без інтеграції навчальних, організаційних та поведінкових практик важко досягти сталого зниження ризиків. Навчальні програми лише тоді мають сенс, коли вони поєднані з регулярними перевірками, симуляціями, аналізом результатів і подальшими коригувальними заходами.

Крім технічних і процедурних ризиків, соціоінженерні атаки серйозно впливають на довіру до систем безпеки, корпоративну культуру, репутацію компаній, а також можуть мати реальні юридичні та фінансові наслідки у разі компрометації. Вразливість користувачів це не лише питання недостатньої обізнаності, але і соціального, організаційного контексту такого як відсутність культури безпеки, незрозумілі процедури, тиск, дефіцит уваги і навантаження.

Результати цього розділу довели, що соціоінженерні загрози сьогодні є комплексними й постійно розвиваючимися, а захист від них вимагає не лише технічних засобів, але й системного підходу, організаційних політик, регулярного тестування, навчань, аналізу поведінки та культури безпеки. Без такої комплексної стратегії організація залишається вразливою навіть при наявності сучасних технологічних систем захисту. Цей розділ сформував методологічну основу для розробки власного методу - більш адаптивного, поведінково орієнтованого, що буде представлений у наступному розділі.

РОЗДІЛ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ КОНТРЗАХОДІВ ІЗ ЗМЕНШЕННЯ РИЗИКУ КОМПРОМЕТАЦІЇ КОРИСТУВАЧІВ

Цей розділ присвячено практичній реалізації розроблених у роботі підходів до протидії соціоінженерним загрозам та оцінюванню їх ефективності. У межах розділу здійснюється перехід від методологічного обґрунтування імітаційного тестування до впровадження конкретних контрзаходів, спрямованих на зниження ризику компрометації користувачів. Особливу увагу приділено аналізу результатів застосування навчальних, організаційних і технологічних заходів, а також оцінці їх впливу на поведінкові показники та рівень інформаційної безпеки, що дозволяє обґрунтувати доцільність і практичну результативність запропонованих рішень

3.1 Методика оцінки базового рівня стійкості до соціоінженерних маніпуляцій

Оцінка базового рівня стійкості користувачів є фундаментальним етапом у процесі управління ризиками, пов'язаними із соціоінженерними загрозами. Цей етап необхідний для встановлення об’єктивної "точки відліку" (Baseline), від якої буде вимірюватися ефективність усіх подальших контрзаходів та тренінгових програм. Без кількісного розуміння початкового рівня вразливості, будь-які твердження про зменшення ризику будуть мати суто гіпотетичний характер, позбавлений емпіричного підґрунтя. Завданням цього розділу є деталізація методики, яка дозволяє не лише якісно описати стан обізнаності користувачів, але й перевести потенційні загрози у вимірні фінансові показники.

Першим кроком у цій методиці є визначення ключових показників вразливості (Metrics Definition). Недостатньо просто фіксувати факт кліку чи введення даних; необхідно розрізняти різні рівні компрометації та пильності. Для цілей дослідження було обрано чотири основні метрики, що забезпечують комплексний аналіз. Головною метрикою, що відображає ступінь вразливості, є

Phish-prone Percentage (PPP). Цей показник обчислюється як відношення кількості користувачів, які вчинили критичну дію (наприклад, перехід за шкідливим посиланням або введення облікових даних), до загальної кількості користувачів, що брали участь в імітації, помножене на сто. Високий показник PPP прямо корелює з високим ризиком успішної соціоінженерної атаки. Другою, не менш важливою метрикою, є Report Rate (коефіцієнт повідомлень), який відображає рівень пильності та проактивної поведінки співробітників. Це відсоток користувачів, які повідомили службу безпеки про підозрілий лист чи інший вид маніпуляції. Високий Report Rate є позитивним індикатором, оскільки дозволяє службі безпеки оперативно реагувати та блокувати загрозу до того, як вона спричинить значну шкоду. Додаткові метрики включають Open Rate (відсоток відкритих листів) та Click Rate (відсоток переходів за посиланнями), які допомагають діагностувати проміжні стадії реакції користувачів.

Для переходу від суто технічних показників вразливості до економічно обґрунтованої оцінки ризику використовується розрахунок гіпотетичних фінансових втрат (Baseline ALE). Цей підхід дозволяє керівництву оцінити інвестиції у контрзаходи не як витрати, а як запобігання збиткам. У сфері інформаційної безпеки для цього застосовується формула Annualized Loss Expectancy (ALE): ALE = ARO x SLE; де SLE - це оцінка фінансових втрат від одного успішного інциденту, спричиненого соціальною інженерією (включаючи витрати на відновлення систем, розслідування, юридичні послуги та репутаційні збитки); а ARO - прогнозована річна частота успішних інцидентів. В контексті оцінки базового рівня, ARO може бути прямо скоригована на основі початкового показника PPP. Наприклад, якщо PPP високий, це означає високу ймовірність того, що соціоінженерна атака буде успішною протягом року. Таким чином, Baseline ALE є фінансовим виразом поточного, незменшеного ризику, який компанія несе через людський фактор. Обґрунтування значень SLE та ARO у цьому випадку базується на галузевих звітах Verison Data Breach Investigations Report (DBIR), які надають середні показники витрат на інциденти, а також на внутрішньому досвіді та аналізі попередніх інцидентів, якщо такі мали місце.

Імітація соціоінженерних атак є найбільш об'єктивним методом для отримання емпіричних даних для розрахунку PPP та Report Rate. Це має бути контрольована, етична кампанія, розроблена для точного відтворення реальних загроз, з якими стикаються користувачі. Сценарії імітації повинні бути максимально реалістичними, використовуючи принципи маніпуляції, такі як терміновість, авторитет чи цікавість. Важливо забезпечити, щоб тестові сценарії не завдали реальної шкоди інфраструктурі або даним. Після проведення первинної кампанії, отримані дані використовуються для розрахунку початкових метрик. Наприклад, якщо з 500 співробітників 150 ввели свої облікові дані на фіктивній сторінці, то PPP становить $\frac{150}{500} * 100\% = 30\%$ Цей показник 30% стає базовим рівнем, з яким будуть порівнюватися результати після навчання. Параметри щодо оцінки базового рівня вразливості користувачів наведено в табл. 3.1.

Таблиця 3.1

Параметри оцінки базового рівня вразливості користувачів

Показник	**Одиниця виміру**	**Формула**	**Значення**	**Призначення**
Кількість протестованих користувачів	особа	Фактична кількість співробітників, які отримали імітацію	500	Визначає загальну вибірку.
Phish-prone Percentage (PPP)	%	Кількість компрометацій/загальну кількість * 100%	30%	Ключовий показник початкової вразливості (Baseline).
Report Rate	%	Кількість повідомлень/загальну кількість * 100%	5%	Показник початкової пильності.
Single Loss Expectancy (SLE)	Грошовий еквівалент (USD/UAH)	Оцінка середньої вартості одного інциденту (відновлення, простій, репутація)	$50,000	Фінансова вартість одного випадку компрометації.
Annual Rate of Occurrence (ARO)	Коефіцієнт (0 до 1)	На основі PPP, скоригований з урахуванням частоти атак	0.8	Оцінка річної ймовірності успішної компрометації.
Annualized Loss Expectancy (ALE)	Грошовий еквівалент (USD/UAH)	ARO x SLE	$40,000	Базовий рівень фінансового ризику через соцінженерію.

Для забезпечення повноти аналізу проведення сегментації користувачів перед початком імітаційного тестування. Не всі співробітники мають однаковий профіль ризику. Користувачі відділів, що працюють з фінансовою інформацією (бухгалтерія) або конфіденційними даними (HR), можуть бути більш привабливими цілями для зловмисників. Відповідно, їхній показник PPP може мати вищий вплив на загальний ALE. Сегментація дозволяє виявити зони підвищеного ризику (Risk Hotspots), для яких будуть розроблятися найбільш цільові та інтенсивні контрзаходи. Наприклад, якщо PPP для фінансового відділу становить 45%, а для адміністративного – 15%, це вказує на необхідність негайного пріоритетного навчання першої групи.

Крім того, необхідно фіксувати не лише кількісні, але й якісні характеристики успішних атак. Це включає тип спрацювавшої маніпуляції (наприклад, використання фальшивого авторитету керівництва, фішинг з проханням оновити корпоративне ПЗ, або використання емоційного шантажу). Аналіз якісних даних дозволяє калібрувати тренінгові програми, фокусуючи їх на тих векторах атаки, які є найбільш ефективними проти даної групи користувачів, тим самим підвищуючи ефективність впроваджуваних контрзаходів. Результати якісного аналізу є невід'ємною частиною звіту про базовий рівень вразливості та є прямим вхідним параметром для етапу розробки навчальних матеріалів.

Встановлення початкового рівня ALE є важливим для розрахунку повернення інвестицій (ROI) в безпеку, оскільки зменшення ALE після впровадження контрзаходів є прямою економічною вигодою. Якщо, наприклад, базовий ALE становить $40 000, а після навчання він знизиться до $10 000, це означає, що програма запобігла $30 000 потенційних річних втрат, обґрунтовуючи всі витрати на проведення імітацій та навчання. Таким чином, цей етап є підготовчою основою для доказової безпеки (Evidence-Based Security).

Важливо також забезпечувати дотримання етичних норм та внутрішніх політик компанії під час навчання. Імітація не повинна викликати паніку, підривати довіру до внутрішніх комунікацій чи призводити до дисциплінарних

стягнень щодо співробітників, які "провалили" тест. Метою є не покарання, а навчання. Тому комунікація результатів має бути прозорою, а процес імітації повинен включати елемент миттєвого навчання (Teachable Moment): користувач, який клікнув, має одразу отримати інформативне повідомлення про те, що це був тест, та короткі інструкції, як діяти наступного разу.

Оцінка базового рівня - це лише половина процесу. Для кількісного обґрунтування зменшення ризику необхідно заздалегідь спланувати етап повторного тестування (Retest). Повторний тест має проводитися через достатній проміжок часу після завершення програми навчання, щоб дати змогу користувачам засвоїти матеріал та змінити свою поведінку. Сценарій повторного тестування повинен бути відмінним від базового, щоб уникнути ефекту "запам'ятовування", але мати співставну складність, аби забезпечити об'єктивне порівняння $PPP_{baseline}$ та PPP_{retest}. Успішне зниження PPP у повторному тесті є прямим, вимірним доказом того, що впроваджені контрзаходи ефективно знизили ризик.

Практична реалізація імітаційного тестування є логічним продовженням етапу оцінки базового рівня, перетворюючи теоретичні моделі загроз на контрольований експеримент у реальному середовищі організації. Цей етап є критичним для збору емпіричних даних, які слугують фундаментом для об'єктивної оцінки вразливості та подальшого кількісного вимірювання ефективності впроваджених контрзаходів. Без проведення фактичного тестування будь-які припущення щодо обізнаності персоналу залишаються суб'єктивними, а інвестиції в навчання - неоптимізованими. Процес розпочався з ретельної підготовки, що включала сегментацію користувачів та розробку специфічних векторів атак, адаптованих до реалій діяльності компанії.

Оскільки профіль ризику співробітника є функцією від його доступу до критичних систем та ролі в організації, було виділено декілька цільових груп для проведення тестування. До ключових сегментів увійшли Фінансовий відділ, Відділ кадрів (HR), IT-департамент та загальний персонал. Фінансовий відділ і HR були класифіковані як пріоритетні цілі (High-Value Targets) через їхню

постійну взаємодію з конфіденційною фінансовою та персональною інформацією відповідно, що робить їх найбільш привабливими мішенями для реальних зловмисників. Така сегментація дозволила не лише отримати усереднений показник вразливості по компанії, але й виявити конкретні зони підвищеного ризику (Risk Hotspots), які потребують посиленого контролю.

Для забезпечення високої реалістичності та охоплення різних психологічних тригерів було розроблено та впроваджено три ключові імітаційні сценарії, що базуються на принципах соціальної інженерії: авторитеті, страху та цікавості.

Перший сценарій, Сценарій А, був орієнтований на маніпуляцію авторитетом та терміновістю. Він імітував офіційний лист від імені вищого керівництва компанії або директора IT-департаменту. У повідомленні йшлося про "критичну загрозу безпеці" або "спробу злому облікового запису", що вимагало від користувача негайних дій. Лист містив категоричну вимогу перейти за наданим посиланням протягом обмеженого часу (наприклад, 30 хвилин) для зміни корпоративного пароля. Цей сценарій був розроблений для фіксації найвищого рівня компрометації - введення діючих облікових даних на підробленій сторінці авторизації. Успішність такої атаки є прямим індикатором високого показника PPP (Phish-prone Percentage) та свідчить про нездатність персоналу критично оцінювати запити, навіть якщо вони надходять від "керівництва". Схематичне зображення порядку проведення тестування виконано в рис. 3.1.

Рис. 3.1. Маніпуляція авторитетом та терміновістю

Підготовка сценарію має на увазі вибір тригерів, завдяки яким користувачі будуть введені в оману. Це включає в себе персону, від імені якої буде написане письмо та переважно апеляція до авторитету та терміновості.

У випадку, коли користувач ігнорує повідомлення, відповідно фіксується що об’єкт не відреагував на появу повідомлення, тому враховується що інцидент не має продовження. Коли користувач перевірив повідомлення і виявив що воно фальшиме, інцидент не мав продовження і навчання пройшло успішно. З іншої сторони, коли користувач перевіряв, але все рівно перейшов за фішинговим посиланням та ввів свої облікові дані в підроблений сайт, PPP фіксується. Так само і з користувачами, які без роздумів перейшли за посиланням.

Другий сценарій використовував емоційний тиск та елементи фінансового шахрайства. Цільовій аудиторії надсилалися повідомлення, що імітували листи від банку-партнера, податкової служби або важливого контрагента. Зміст листа

попереджав про "несанкціоновану транзакцію великого обсягу" або "прострочений платіж, що призведе до штрафних санкцій". Користувачам пропонувалося терміново завантажити "рахунок-фактуру" або перейти за посиланням для скасування операції. Метою цього сценарію була перевірка здатності співробітників зберігати спокій та верифікувати джерело інформації в умовах штучно створеного стресу. Високий відсоток кліків у цьому сценарії вказує на вразливість до атак типу Business Email Compromise (BEC). Схематичне зображення порядку проведення тестування для фінансового відділу виконано в рис. 3.2.

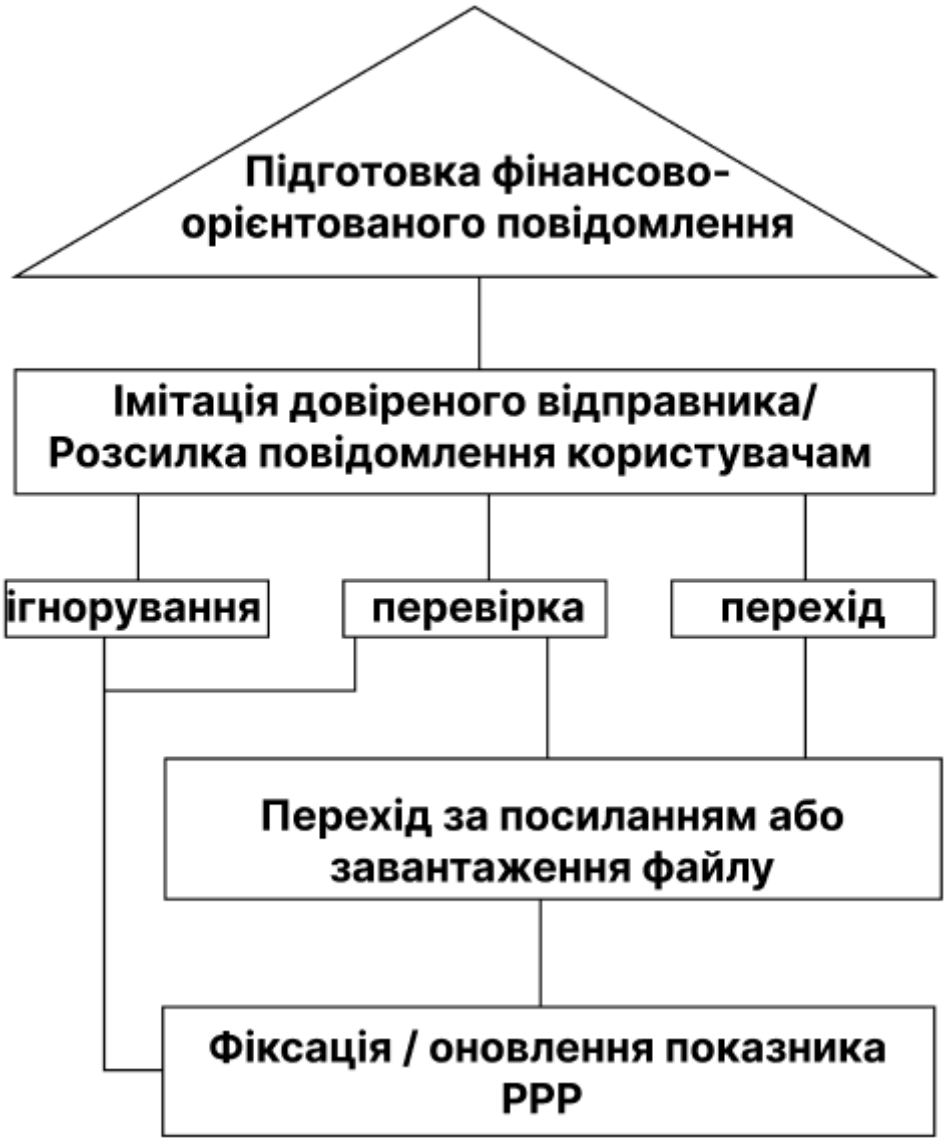

Рис. 3.2. Схема використання емоційного тиску та фінансового шахрайства

На першому етапі формується повідомлення, зміст якого імітує фінансово критичну ситуацію. У тексті використовуються тригерні формулювання, зокрема повідомлення про несанкціоновані транзакції, прострочені платежі, можливі штрафні санкції або блокування рахунків. Основною метою цього етапу є створення штучного стресового контексту, який знижує рівень раціонального аналізу з боку отримувача. Далі здійснюється імітація авторитетного або довіреного джерела (банк-партнер, податкова служба, контрагент, фінансовий відділ організації). Повідомлення надсилається цільовій групі користувачів з використанням візуальних і текстових елементів, характерних для офіційної ділової комунікації. Цей етап спрямований на перевірку здатності користувачів верифікувати джерело інформації. Після отримання повідомлення можливі три основні типи поведінки користувачів:

1. Ігнорування - користувач не взаємодіє з повідомленням, що свідчить про базову обережність або сформовані навички кібергігієни;
2. Перевірка - користувач намагається перевірити достовірність повідомлення шляхом звернення до альтернативних джерел або внутрішніх процедур;
3. Перехід - користувач переходить за посиланням або завантажує вкладений файл без попередньої верифікації, що є потенційно небезпечною дією;
4. Перехід за посиланням або завантаження файлу.

У разі вибору небезпечної дії користувач здійснює перехід за вбудованим посиланням або завантажує файл, який імітує рахунок-фактуру чи фінансовий документ. Цей етап дозволяє зафіксувати рівень довіри до повідомлень, що апелюють до фінансових втрат та терміновості. Завершальним етапом є фіксація результатів та оновлення показника PPP (Phishing Proneness Percentage), який відображає частку користувачів, схильних до фішингових та BEC-атак. Аналіз цього показника дає змогу оцінити загальний рівень вразливості персоналу до сценаріїв фінансового шахрайства та емоційного тиску.

Третій сценарій, Сценарій В, був спрямований на експлуатацію людської цікавості та бажання отримати вигоду. Легенда атаки будувалася навколо

повідомлення від HR-відділу з темою "Нова політика преміювання" або "Зміни у соціальному пакеті". Лист закликав співробітників ознайомитися з деталями, які нібито містилися у прикріпленому файлі (наприклад, документ Word з макросами або архів). Хоча в рамках тестування файл був безпечним, його завантаження та спроба відкриття імітували розповсюдження шкідливого програмного забезпечення або програм-вимагачів. Цей вектор дозволив оцінити готовність користувачів ігнорувати правила безпеки щодо роботи з вкладеннями заради задоволення особистого інтересу.

Проведення кампанії здійснювалося за допомогою спеціалізованого програмного забезпечення, що забезпечило автоматичну фіксацію дій користувачів на кожному етапі взаємодії з фішинговим листом. Система відстежувала чотири ключові метрики: Open Rate (відсоток відкритих листів), Click Rate (відсоток переходів за посиланням), PPP (відсоток компрометації даних) та Report Rate (відсоток повідомлень про інцидент). Важливо зазначити, що процес тестування супроводжувався механізмом "миттєвого навчання" (Teachable Moment). Якщо користувач припускався помилки і переходив за посиланням або вводив дані, він автоматично перенаправлявся на спеціальну навчальну сторінку. Там йому повідомляли, що це була навчальна перевірка, і одразу вказували на "червоні прапорці" (індикатори фішингу) у листі, які він пропустив. Такий підхід дозволив трансформувати потенційно негативний досвід помилки у конструктивний навчальний момент без створення атмосфери страху.

Аналіз результатів первинного тестування підтвердив гіпотезу про високий рівень вразливості персоналу до методів соціальної інженерії. Загальноорганізаційний показник PPP на рівні 30%, зафіксований у Таблиці 3.1, свідчить про значні прогалини в системі захисту. Однак детальний розгляд даних виявив тривожну диспропорцію: співробітники фінансового відділу показали рівень компрометації 45% у сценарії з "несанкціонованою транзакцією", що є критичним ризиком для організації. Водночас, загальний показник Report Rate склав лише 5%, що вказує на пасивність персоналу: навіть ті, хто розпізнав

загрозу, переважно просто видаляли лист, не повідомляючи службу безпеки, залишаючи організацію "сліпою" до атаки. Отримані емпіричні дані стали основою для розробки диференційованої програми контрзаходів, яка буде детально описана в наступному підрозділі.

3.2. Розробка методу тестування користувачів на стійкість до соціоінженерних маніпуляцій

Метод тестування користувачів на основі імітаційних сценаріїв, реалізується як послідовний багатоетапний процес, спрямований на отримання об’єктивних, вимірюваних і економічно інтерпретованих даних щодо стійкості персоналу до соціоінженерних маніпуляцій.

Початковим етапом є визначення базового рівня стійккості (Baseline Assessment), який слугує відправною точкою для всього подальшого аналізу. На цьому етапі формується кількісне уявлення про поточну вразливість персоналу без впливу навчальних чи коригувальних заходів. Для цього визначаються ключові метрики поведінкової реакції користувачів, зокрема Phish-prone Percentage (PPP) як основний індикатор схильності до компрометації, Report Rate як показник пильності та проактивної поведінки, а також допоміжні метрики Open Rate і Click Rate, що дозволяють простежити ланцюг реакцій користувача від отримання повідомлення до потенційно небезпечної дії.

Наступним етапом є сегментація користувачів за профілем ризику, яка базується на ролях, рівнях доступу та типах інформації, з якою працюють співробітники. У документі показано, що відділи з доступом до фінансових або персональних даних (фінансовий відділ, HR) розглядаються як пріоритетні цілі через підвищену привабливість для зловмисників. Така сегментація дозволяє не лише отримати усереднений показник вразливості, а й виявити локальні «зони ризику», де наслідки успішної атаки є найбільш критичними.

Після цього здійснюється проєктування імітаційних сценаріїв атак, яке передбачає вибір психологічних тригерів, каналу доставки та легенди атаки. У

межах методу розробляються сценарії, що апелюють до авторитету і терміновості, емоційного тиску та фінансового страху, а також до цікавості й очікуваної вигоди. Кожен сценарій адаптується до конкретної цільової групи та моделює реалістичні умови, з якими користувачі можуть зіткнутися у повсякденній діяльності, що забезпечує високу валідність отриманих результатів.

Далі йде проведення контрольованої імітаційної кампанії, під час якої сценарії реалізуються у реальному інформаційному середовищі організації з використанням спеціалізованого програмного забезпечення. Система автоматично фіксує всі дії користувачів - відкриття повідомлень, переходи за посиланнями, введення даних або повідомлення службі безпеки. Важливою складовою цього етапу є дотримання етичних принципів і відсутність реальної шкоди для інфраструктури та даних.

Паралельно з фіксацією поведінкових реакцій реалізується механізм миттєвого навчання (Teachable Moment). У разі помилкових дій користувач одразу отримує пояснення, що подія була навчальною імітацією, та інформацію про ознаки шахрайства, які він не розпізнав. Це дозволяє перетворити сам процес тестування на елемент навчання без створення атмосфери покарання або страху.

Наступний етап полягає в кількісному та якісному аналізі результатів, де розраховуються значення PPP, Report Rate та інших метрик як у цілому по організації, так і в розрізі окремих підрозділів і сценаріїв. Отримані показники використовуються для оцінки ймовірності успішних атак та для фінансової інтерпретації ризиків шляхом розрахунку Annualized Loss Expectancy (ALE), що дозволяє пов’язати поведінкові вразливості з потенційними економічними втратами.

Завершальним етапом є планування та проведення повторного тестування (Retest) після впровадження навчальних і організаційних контрзаходів. Повторні сценарії відрізняються за змістом, але зберігають порівнювану складність, що дає змогу коректно оцінити динаміку змін показника PPP і підтвердити ефективність вжитих заходів. Зменшення базового рівня PPP та відповідного

ALE розглядається як кількісно доведений результат підвищення стійкості персоналу до соціоінженерних впливів. Всі ці етапи зображені нижче. (рис. 3.3)

Рис. 3.3. Етапи проведення методу тестування користувачів на стійкість до соціоінженерних маніпуляцій

Проведення тестування потребує використання сукупності програмних інструментів і технологій, які забезпечують повний цикл імітаційного моделювання, збору поведінкових даних, їх аналітичної обробки та подальшої інтеграції результатів у систему управління інформаційною безпекою. До них входять: спеціалізовані платформи для симуляції соціоінженерних атак, технічні засоби створення артефактів атак, модулі логування та аналітики, аналітичні інструменти та платформи навчання та управління знаннями. [25]

Спеціалізовані платформи для симуляції соціоінженерних атак дозволяють реалізовувати фішингові, SMS-, vishing- та комбіновані сценарії у контрольованому середовищі. Такі платформи забезпечують централізоване керування кампаніями, автоматизоване надсилання повідомлень, персоналізацію контенту, а також фіксацію дій користувачів у режимі реального часу. Використання автоматизованих симуляційних систем дає змогу отримати репрезентативні статистичні дані та уникнути суб'єктивності оцінювання, характерної для опитувальних методів.

Для реалізації імітаційних сценаріїв необхідними є технічні засоби створення артефактів атак, зокрема інструменти для формування фішингових повідомлень, тестових веб-сторінок і форм введення даних, а також сценарії телефонних або текстових комунікацій. Усі ці елементи використовуються

виключно в навчальному режимі й не передбачають реального збирання конфіденційної інформації. Важливою вимогою, зазначеною в документі, є ізоляція таких артефактів від продуктивних систем підприємства з метою запобігання технічним інцидентам.

Збір і фіксація результатів тестування здійснюється за допомогою модулів логування та аналітики, які реєструють поведінкові реакції користувачів: відкриття повідомлень, переходи за посиланнями, спроби введення даних, а також факти повідомлення службі безпеки. На основі цих даних автоматично розраховуються показники Phish-prone Percentage (PPP), Click Rate, Report Rate та інші метрики, що є базою для кількісного аналізу рівня вразливості персоналу.

Для подальшої інтерпретації результатів застосовуються аналітичні інструменти оцінювання ризиків, які дозволяють пов’язати поведінкові показники з економічними наслідками. Використання підходів до розрахунку очікуваних річних втрат (Annualized Loss Expectancy, ALE), також потребує спеціалізованих програмних засобів для обробки статистичних даних, побудови звітів і порівняння результатів між різними циклами тестування.

Окрему категорію становлять платформи навчання та управління знаннями (LMS), які інтегруються з системами симуляції. Вони використовуються для реалізації механізму миттєвого навчального зворотного зв’язку, коли після помилкової дії користувач автоматично отримує навчальні матеріали, пояснення ознак шахрайства та рекомендації щодо правильної поведінки. Така інтеграція дозволяє перетворити процес тестування на елемент безперервного навчання персоналу.

Для оцінки тестування критерії формуються окремо для кожного типу імітаційного сценарію з урахуванням каналу атаки, очікуваної поведінкової реакції та потенційних наслідків компрометації. Такий підхід дозволяє забезпечити адекватність оцінювання та уникнути спрощеного трактування результатів, коли різні за складністю й небезпекою сценарії аналізуються за однаковими показниками.

Базою для формування критеріїв є визначення цільової дії користувача, яка в межах конкретного сценарію вважається критичною з погляду інформаційної безпеки. Для фішингових та smishing-сценаріїв такою дією зазвичай є перехід за посиланням або введення облікових даних на підробленій сторінці, тоді як для vishing-сценаріїв - передача конфіденційної інформації, одноразових кодів або підтвердження небезпечної операції під час телефонної розмови. Саме ця очікувана дія визначає, які поведінкові показники будуть ключовими при оцінці результатів тестування.

Для кожного типу сценарію використовується набір кількісних метрик, що відображають послідовні етапи взаємодії користувача з атакуючим повідомленням. До них належать показники відкриття повідомлень, коефіцієнти кліків або відповіді, частка користувачів, які виконали небезпечну дію, а також частка тих, хто ідентифікував загрозу і повідомив службу безпеки. Центральним інтегральним показником виступає Phish-prone Percentage (PPP), який інтерпретується як імовірність компрометації користувача у межах заданого сценарію та дозволяє порівнювати результати між різними кампаніями тестування.

Важливою особливістю формування критеріїв є урахування складності сценарію та його правдоподібності. Результати сценаріїв з високим рівнем персоналізації та психологічного тиску не можуть безпосередньо порівнюватися з простими навчальними сценаріями. Тому оцінювання здійснюється з поправкою на тип сценарію, використані психологічні тригери та цільову аудиторію, що забезпечує коректну інтерпретацію рівня вразливості користувачів.

Окрім кількісних показників, критерії оцінки включають якісний аналіз причин успіху або невдачі сценарію. Для цього досліджується, які елементи повідомлення або взаємодії вплинули на рішення користувача: авторитет джерела, терміновість запиту, страх фінансових втрат чи використання внутрішньої термінології організації. Такий аналіз дозволяє не лише зафіксувати факт уразливості, а й зрозуміти її поведінкові та організаційні передумови.

Фінальним етапом формування критеріїв є їх прив’язка до ризик-орієнтованої моделі оцінювання. Результати тестування можуть бути використані для розрахунку очікуваних річних втрат (ALE), де значення PPP виступає ймовірнісною складовою ризику. Таким чином, критерії оцінки перестають бути суто навчальними показниками і трансформуються в інструмент управління інформаційною безпекою, який дозволяє приймати обґрунтовані управлінські рішення щодо пріоритетів навчання та захисних заходів.

Для етичного проведення тестів потребується формальне організаційне погодження. Ініціація імітаційних кампаній має здійснюватися виключно за згодою керівництва організації та відповідальних підрозділів з інформаційної безпеки, HR і, за потреби, юридичної служби. Таке погодження фіксує допустимі межі тестування, цілі проведення кампаній і виключає використання результатів у дисциплінарних або каральних цілях.

Ключовою процедурою захисту конфіденційності при проведені тестів є обмеження збору та обробки персональних даних. Під час тестування не здійснюється збирання реальних облікових даних, паролів чи іншої чутливої інформації. Усі імітаційні форми введення даних працюють у навчальному режимі та фіксують лише факт взаємодії користувача зі сценарієм без збереження введеного вмісту. Це мінімізує ризик порушення вимог законодавства у сфері захисту персональних даних.

Для забезпечення інформаційної безпеки інфраструктури застосовується ізоляція середовища тестування. Усі фішингові сторінки, тестові сервіси та системи збору даних розміщуються в окремому контрольованому середовищі, яке не має доступу до продуктивних інформаційних систем підприємства. Такий підхід унеможливлює випадкове порушення працездатності бізнес-процесів або компрометацію реальних інформаційних активів.

Важливою процедурою є анонімізація та агрегування результатів. Підсумкові звіти формуються на рівні груп, підрозділів або ролей, без персоналізованого зазначення імен користувачів. Індивідуальні результати

можуть використовуватися лише для адресного навчального зворотного зв’язку та не підлягають публічному розголошенню. Це дозволяє зберегти довіру персоналу до процесу тестування і запобігти стигматизації окремих співробітників. Також тестування розглядається як інструмент навчання і підвищення обізнаності, а не як засіб контролю або покарання. Усі виявлені помилки інтерпретуються в контексті вдосконалення процедур, навчальних програм і захисних механізмів, а не як індивідуальні порушення дисципліни.

Для зниження психологічного навантаження та запобігання негативним наслідкам застосовується контроль змісту сценаріїв. Також передбачаються обмеження на використання тем, які можуть викликати сильний стрес, паніку або моральний дискомфорт, зокрема пов’язаних із загрозами здоров’ю, безпеці близьких або фінансовою катастрофою. Це дозволяє зберегти навчальний характер тестування і уникнути етичних порушень.

Наступною процедурою є інформування та навчальний зворотний зв’язок. Після завершення кампанії користувачам пояснюється навчальний характер подій, надається інформація про типові ознаки соціоінженерних атак і правильні моделі поведінки. Такий підхід підсилює сприйняття тестування як елементу корпоративної культури безпеки, а не прихованого контролю.

Після проведення тестування користувачів потрібно інтегрувати його результати у систему навчання та підвищення обізнаності користувачів не як окремий звітний продукт, а як безперервний елемент циклу управління інформаційною безпекою.

Насамперед отримані результати використовуються для формування адресного навчального зворотного зв’язку. Кожна зафіксована помилкова дія користувача має супроводжуватися негайним поясненням навчального характеру події та коротким роз’ясненням ознак соціоінженерної атаки, які не були розпізнані. Такий підхід, дозволяє закріпити правильні моделі поведінки безпосередньо в момент помилки, коли користувач найбільш сприйнятливий до навчальної інформації.

На основі агрегованих метрик тестування, зокрема Phish-prone Percentage, Report Rate та інших поведінкових показників, здійснюється сегментація користувачів за рівнем стійкості та профілем ризику. Навчальні заходи мають бути диференційованими: для груп із підвищеною вразливістю доцільно застосовувати поглиблені або повторні тренінги, тоді як для користувачів із високим рівнем обізнаності достатніми є підтримувальні інформаційні матеріали. Це дозволяє уникнути формального «однакового для всіх» навчання та підвищує ефективність використання ресурсів.

Важливим напрямом інтеграції результатів є адаптація змісту навчальних програм до виявлених типових помилок і поведінкових патернів. Якщо аналіз тестування показує, що користувачі найчастіше реагують на сценарії, пов’язані з авторитетом керівництва або терміновими фінансовими запитами, відповідні приклади, кейси та вправи мають бути включені до навчальних матеріалів. Таким чином, навчання базується не на абстрактних загрозах, а на реальних сценаріях, з якими стикається конкретна організація.

Також необхідна інтеграція результатів тестування з платформами навчання та управління знаннями (LMS). Це дає змогу автоматизувати призначення навчальних модулів за результатами тестування, відстежувати проходження курсів і корелювати навчальну активність із подальшою динамікою показників стійкості. Така інтеграція забезпечує замкнений цикл «тестування - навчання - повторне тестування», що є основою для доказового підходу до підвищення обізнаності персоналу.

Окремо важливо виділити ролі групового аналізу результатів у формуванні культури безпеки. Узагальнені результати кампаній можуть використовуватися під час внутрішніх семінарів, інформаційних розсилок або нарад з безпеки для демонстрації типових загроз і колективних помилок без персоналізації даних. Це сприяє підвищенню усвідомлення ризиків і формуванню спільної відповідальності за інформаційну безпеку.

Завершальним елементом інтеграції є використання результатів тестування для планування наступних навчальних імітаційних заходів. Сценарії

повторного тестування мають коригуватися з урахуванням попередніх результатів, поступово підвищуючи складність атак і охоплюючи нові вектори впливу. Таким чином, навчання і тестування формують єдиний адаптивний процес, спрямований на довгострокове зниження сприйнятливості користувачів до соціоінженерних маніпуляцій. Виходячи з всього вищеперерахованого можна почати формування практичних рекомендацій що будуть описані в наступному підрозділі.

3.3. Формування практичних рекомендацій щодо зниження ризику компрометації користувачів

Результати проведеного дослідження базового рівня вразливості персоналу підтвердили гіпотезу про те, що людський фактор залишається найбільш критичною ланкою в системі забезпечення інформаційної безпеки організації. Зафіксований показник Phish-prone Percentage (PPP) на рівні 30% та низький коефіцієнт звітування (Report Rate 5%) вказують на необхідність впровадження комплексної стратегії протидії соціоінженерним загрозам. На основі отриманих емпіричних даних та розрахованих показників очікуваних річних втрат (ALE), нижче сформовано систему практичних рекомендацій, що охоплюють технічний, організаційний та методологічний рівні.

Першочерговим є відмова від уніфікованого підходу «один тренінг для всіх» на користь диференційованої моделі навчання. Сегментація користувачів, проведена на етапі оцінки базового рівня, дозволила виявити «зони підвищеного ризику» (Risk Hotspots). Зокрема, для Фінансового відділу, де рівень компрометації склав 45%, далі запропонована поглиблена програма з протидії атакам типу Business Email Compromise (BEC). (табл.3.2)

Таблиця 3.2

Програма протидії BEC

Етап програми	Зміст та інструменти реалізації	Очікуваний ефект
Аналітична діагностика ризику	Використання результатів імітаційного тестування для фінансового підрозділу з підвищеним PPP та низьким Report Rate. Аналіз сценаріїв, у яких експлуатуються зміна платіжних реквізитів, термінові запити керівництва або контрагентів, підробка ланцюгів ділового листування.	Визначення BEC як пріоритетного ризику з високим потенційним впливом на фінансові активи організації.
Сценарно-орієнтоване навчання	Розробка навчальних модулів на основі реальних імітаційних кейсів, зафіксованих під час тестування. Навчання фокусується не лише на технічних ознаках, а передусім на психологічних тригерах BEC: авторитет керівництва, дефіцит часу, фінансова відповідальність.	Формування здатності розпізнавати типові патерни BEC незалежно від технічного рівня атаки.
Мікронавчання (Micro-learning)	Впровадження коротких інтерактивних навчальних сесій тривалістю до 5 хвилин, кожна з яких присвячена одному конкретному BEC-вектору.	Підвищення засвоюваності матеріалу та зниження PPP шляхом регулярного, але ненавантажувального навчання.
Teachable Moment (навчальний момент)	Автоматичне перенаправлення користувача на навчальну сторінку у момент помилкової дії в імітаційному сценарії. Зворотний зв’язок має виключно некаральний характер.	Створення стійкого асоціативного зв’язку між помилкою та загрозою, що значно знижує ймовірність повторення аналогічної дії.
Організаційні процедури перевірки	Запровадження обов’язкової двоетапної перевірки для фінансових операцій: зміни платіжних реквізитів, термінові платежі, запити від імені керівництва. Перевірка здійснюється через альтернативний канал зв’язку.	Різке зниження ефективності BEC-атак навіть у разі помилкової поведінки користувача.
Технологічна підтримка звітування	Впровадження кнопки «Phish Alert Button» (PAB) у поштовому клієнті з автоматичною передачею заголовків листа до SOC. Налаштування сценаріїв автоматичного реагування у разі виявлення реальної загрози.	Зростання Report Rate, скорочення часу виявлення атак і зменшення SLE за рахунок швидкого блокування поширення.
Гейміфікація та мотивація	Впровадження системи позитивного заохочення за пильність: рейтинги стійкості, статуси «кібер-експерт», публічне визнання користувачів, які першими повідомили про атаку.	Формування соціальної норми безпечної поведінки та підвищення колективної відповідальності.
Економічне обґрунтування (ROI)	Використання показників PPP, ARO та ALE для демонстрації фінансового ефекту заходів.	Забезпечення підтримки топ-менеджменту та обґрунтування інвестицій у програму протидії BEC.
Повторна оцінка (Retest)	Проведення повторних імітаційних кампаній з аналогічною складністю сценаріїв після впровадження заходів. Порівняння динаміки PPP, Report Rate та ALE.	Кількісне підтвердження ефективності програми та її коригування.

Навчання має базуватися на реальних кейсах, зафіксованих під час імітації, що дозволяє персоналу побачити конкретні вектори маніпуляцій, які спрацювали саме в їхньому робочому середовищі. Пріоритетним є навчання не лише розпізнаванню технічних ознак фішингу (підроблені домени, підозрілі URL), а й розумінню психологічних тригерів, таких як «дефіцит часу» або «апеляція до авторитету керівництва». Для адміністративного персоналу та HR-департаменту акцент слід змістити на безпечну роботу з вкладеннями та перевірку автентичності запитів щодо персональних даних співробітників.

Одним із найбільш ефективних методів зниження PPP є впровадження технології Teachable Moment (навчальний момент). Традиційні щорічні лекції мають низький рівень засвоєння матеріалу через відсутність емоційного залучення. Практична рекомендація полягає в автоматизації процесу зворотного зв’язку: у момент, коли користувач припускається помилки в імітаційному сценарії (наприклад, вводить дані на підробленій сторінці), він має бути миттєво перенаправлений на інтерактивну навчальну сторінку.

Така сторінка повинна містити графічний розбір «червоних прапорців» саме того листа, на який зреагував користувач. Це створює стійкий асоціативний зв’язок між дією та загрозою. Важливо, щоб такий зворотний зв'язок мав конструктивний, а не каральний характер, що сприятиме формуванню культури відкритості та відповідальності за безпеку.

Критично низький показник Report Rate (5%) свідчить про те, що організація є фактично «сліпою» перед обличчям реальних атак, оскільки служба безпеки не отримує вчасної інформації про загрози, що поширюються. Для виправлення цієї ситуації рекомендовано:

Технічне спрощення звітування: Впровадження спеціалізованого програмного модуля «Phish Alert Button» у поштовий інтерфейс. Це дозволяє користувачеві повідомити про підозрілий об'єкт одним натисканням, автоматично передаючи всі заголовки листа (headers) до аналітичного центру безпеки (SOC).

Гейміфікація та позитивна мотивація: Замість фокусування на «порушниках», компанії варто створити систему заохочень для «захисників». Публічне визнання співробітників, які першими виявили імітаційну або реальну атаку, створює соціальний доказ корисності пильної поведінки.

Збільшення Report Rate безпосередньо корелює зі зниженням SLE (Single Loss Expectancy), оскільки швидке виявлення дозволяє блокувати шкідливі ресурси на рівні шлюзу до того, як інші співробітники встигнуть з ними взаємодіяти.

Для забезпечення підтримки з боку топ-менеджменту, рекомендується використовувати результати тестування як основу для розрахунку повернення інвестицій (ROI) у безпеку. Встановлений базовий рівень ALE на рівні $40,000 є фінансовим виразом ризику, який компанія несе щороку. Практична реалізація контрзаходів (навчання, імітації) має на меті зниження показника ARO (річної частоти успішних інцидентів) шляхом зменшення PPP.

Якщо після проведення комплексу заходів повторний тест (Retest) покаже зниження PPP з 30% до 10%, це дозволить математично довести зменшення потенційних річних втрат, наприклад, до $12,000. Різниця у $28,000 є прямим економічним ефектом від впровадженої методики, що дозволяє обґрунтувати бюджети на подальший розвиток системи захисту.

Реалізація імітаційних атак потребує суворого дотримання етичних рамок, щоб не підірвати моральний дух колективу. Рекомендується:

1. Виключення дисциплінарних стягнень: Офіційна політика компанії має закріплювати, що результати тестів використовуються виключно для навчання. Покарання за «провал» тесту призведе до того, що співробітники почнуть приховувати помилки, що є катастрофічним для безпеки;

2. Контроль контенту: Уникати сценаріїв, що експлуатують глибоко особисті трагедії, стан здоров'я або критичні фінансові загрози (наприклад, повідомлення про невиплату заробітної плати), оскільки це викликає надмірний стрес і відторгнення навчального процесу;

3. Анонімізація звітів: На рівні керівництва департаментів результати мають подаватися у вигляді агрегованої статистики. Персоналізовані дані повинні бути доступні лише фахівцям з навчання для точкової роботи з найбільш вразливими особами.

Ефективність запропонованих рекомендацій залежить від системності їх впровадження. Процес перетворення статичних звітів про вразливість у динамічну систему захисту потребує деталізації етапів розгортання, інтеграції технологічних рішень та формування нової корпоративної етики.

На основі зафіксованого PPP у 45% для фінансового сектору, практична реалізація має починатися з розробки вузькоспеціалізованих модулів. Замість загальних лекцій про цифрову гігієну, рекомендується впровадити «мікронавчання» (micro-learning). Це короткі, тривалістю до 5 хвилин, інтерактивні сесії, що фокусуються на одному конкретному векторі.

Наприклад, для бухгалтерських підрозділів розробляється симуляція, яка імітує зміну реквізитів у рахунку-фактурі, надісланому від імені реального контрагента. Практичне завдання полягає не лише у виявленні підробки, а й у відпрацюванні процедури «двоетапної перевірки» поза межами електронної пошти (телефонний дзвінок партнеру, верифікація через альтернативний канал зв'язку). Таким чином, навчання перетворюється з пасивного спостереження на активне формування навички, що безпосередньо знижує річну ймовірність інцидентів (ARO).

Впровадження кнопки «Phish Alert Button» (PAB) потребує не лише встановлення плагіна, а й налаштування серверної логіки взаємодії з Security Operations Center (SOC). Коли користувач натискає PAB, система повинна автоматично виконувати наступні кроки:

1. Агрегація даних: Збір технічних заголовків (headers), IP-адрес відправника та аналіз вбудованих посилань через системи пісочниць (sandboxing);

2. Ідентифікація імітації: Якщо лист є частиною навчальної кампанії, користувач миттєво отримує позитивне підкріплення, а його статус у системі моніторингу оновлюється як «пильний»;

3. Реагування на реальну загрозу: Якщо лист визнано шкідливим, SOC отримує можливість автоматизованого видалення аналогічних повідомлень зі скриньок усіх інших співробітників (Search-and-Destroy).

Така автоматизація дозволяє перетворити кожного навченого співробітника на «живий датчик» системи безпеки. Це кардинально змінює парадигму: персонал перестає бути слабкою ланкою і стає активним елементом системи раннього попередження, що критично важливо при низькому базовому Report Rate.

Для подолання пасивності персоналу рекомендується впровадити модель «цифрового імунітету». Гейміфікація процесу звітування може включати систему балів та внутрішніх рейтингів стійкості (Security Score). Співробітники, які стабільно ідентифікують фішингові листи та не припускаються помилок протягом кварталу, отримують статус «Кібер-експерта».

Практичне значення гейміфікації полягає у створенні соціального доказу. Коли колеги бачать, що пильність заохочується керівництвом, вони підсвідомо починають копіювати безпечну модель поведінки. Це дозволяє знизити PPP природним шляхом через зміну колективних норм, а не через примус.

Кількісна оцінка ефективності через показник ALE має проводитися після кожного циклу повторного тестування (Retest). Важливо розуміти, що зниження PPP з 30% до 10% — це не просто цифри, а реальне зменшення площі атаки. Для фінансового обґрунтування рекомендується використовувати таблицю порівняння витрат на навчання та потенційних втрат від простою. Якщо вартість річної підписки на платформу імітації та навчання становить $5,000, а розраховане зниження ALE дорівнює $28,000, то чистий прибуток від впровадження програми складає $23,000. Такий розрахунок є безапеляційним аргументом для фінансового директора (CFO) при затвердженні бюджетів на інформаційну безпеку.

На завершення, критично важливою є прозорість процесу. Керівництво має офіційно видати наказ або меморандум, який гарантує «імунітет» від покарань за результатами тестів. Будь-яка спроба використати результати тестування для звільнення чи штрафування призведе до того, що персонал почне видаляти навіть потенційно важливі робочі листи через страх помилитися, що зашкодить бізнес-процесам.

Наукові дослідження показують, що навички розпізнавання фішингу починають деградувати вже через 3–4 місяці після навчання. Тому практичною рекомендацією є впровадження концепції «безперервного циклу стійкості»[59].

1. Квартальні імітації: Кожен квартал вектор атаки має змінюватися. Якщо в першому кварталі це була «апеляція до авторитету», то в другому - «експлуатація цікавості» щодо соціальних пакетів чи премій;

2. Адаптивність: Якщо певна група користувачів демонструє негативну динаміку (зростання PPP), система повинна автоматично призначати їм додатковий короткий відео-урок.

Керівництво має офіційно видати наказ або меморандум, який гарантує «імунітет» від покарань за результатами тестів. Будь-яка спроба використати результати тестування для звільнення чи штрафування призведе до того, що персонал почне видаляти навіть потенційно важливі робочі листи через страх помилитися, що зашкодить бізнес-процесам.

Метою методу є створення атмосфери, де безпека є спільною відповідальністю. Тільки за умови дотримання етичних норм, технічної підтримки через кнопку PAB та фінансового обґрунтування через ALE, організація зможе перетворити свою «найбільш вразливу ланку» на надійний бар'єр проти сучасних соціоінженерних загроз. Запропонований комплекс заходів забезпечує не лише миттєве зниження ризику, а й закладає фундамент для довгострокової стійкості цифрової екосистеми підприємства.

Висновки до розділу 3

У третьому розділі здійснено практичну реалізацію розробленого методу тестування користувачів на стійкість до соціоінженерних маніпуляцій та проведено оцінку ефективності запропонованих контрзаходів зі зменшення ризику компрометації користувачів. Розділ логічно поєднує результати теоретичного та аналітичного дослідження з прикладним застосуванням імітаційних сценаріїв у контрольованому організаційному середовищі.

У межах розділу сформовано методику оцінювання базового рівня стійкості користувачів до соціоінженерних впливів, яка ґрунтується на використанні поведінкових метрик та аналізі реакцій користувачів на реалістичні сценарії атак. Це дозволило кількісно та якісно охарактеризувати рівень сприйнятливості персоналу, виявити типові моделі небезпечної поведінки та визначити групи підвищеного ризику з урахуванням їх ролей і доступу до інформаційних активів.

Основним результатом розділу є розробка та обґрунтування методу тестування користувачів на стійкість до соціоінженерних маніпуляцій на основі імітаційних сценаріїв. Запропонований метод забезпечує комплексне оцінювання поведінкових реакцій, поєднуючи аналіз кількісних показників із контекстною інтерпретацією психологічних та організаційних чинників. Його застосування дає змогу не лише фіксувати факт помилкових дій, а й встановлювати першопричини вразливості, що є критично важливим для управління ризиками людського фактора.

На основі результатів тестування сформовано практичні рекомендації щодо зниження ризику компрометації користувачів, які охоплюють навчальні, організаційні та технологічні заходи. Показано, що найбільшої ефективності досягає комплексний підхід, за якого імітаційне тестування інтегрується у систему підвищення обізнаності, внутрішні процедури перевірки та технічні механізми контролю. Такий підхід сприяє переходу від формального навчання до системного управління поведінковими ризиками.

Загалом результати третього розділу підтверджують практичну придатність і ефективність запропонованого методу тестування користувачів на стійкість до соціоінженерних впливів. Реалізація методу дозволяє підвищити рівень кіберстійкості організації, трансформуючи людський фактор з потенційної вразливості у керований елемент системи інформаційної безпеки та створюючи основу для подальшого вдосконалення превентивних заходів у сфері протидії соціальній інженерії.

ВИСНОВКИ

У ході виконання кваліфікаційної роботи здійснено комплексне дослідження соціальної інженерії як одного з найбільш небезпечних і водночас складних для протидії векторів загроз у сфері інформаційної безпеки. Встановлено, що ефективність соціоінженерних атак значною мірою обумовлена експлуатацією психологічних, поведінкових та організаційних особливостей користувачів, унаслідок чого людський фактор виступає критичною ланкою в системі захисту інформаційних ресурсів. У роботі формалізовано поняття соціальної інженерії та здійснено її систематизацію за основними ознаками, зокрема за каналами реалізації, типами впливу, спрямованістю атак і потенційними наслідками, що дозволило структуровано окреслити спектр актуальних загроз для сучасних організацій.

У межах дослідження проаналізовано еволюцію підходів до інформаційної безпеки та обґрунтовано необхідність переходу від переважно технічно орієнтованих моделей захисту до комплексних підходів, які враховують поведінкові аспекти діяльності користувачів. Показано, що традиційні засоби безпеки є недостатніми для протидії соціоінженерним атакам без системного розвитку обізнаності персоналу та впровадження механізмів контролю поведінкових ризиків. Проведений аналіз існуючих методів оцінювання стійкості користувачів засвідчив їх обмеженість у частині реалістичності, повторюваності та практичної інтеграції результатів у систему управління інформаційною безпекою.

Другий розділ роботи був присвячений аналізу векторів соціоінженерних загроз та підходів до їх імітації. Виявлено, що найбільш небезпечними є таргетовані сценарії атак, зокрема типу Business Email Compromise, які поєднують психологічний тиск, використання внутрішнього контексту організації та високий рівень правдоподібності. Оцінювання ефективності навчальних і профілактичних заходів показало, що формальні тренінги без практичної складової не забезпечують стійкого зниження рівня вразливості, тоді

як імітаційні сценарії дозволяють отримати об’єктивні дані про реальну поведінку користувачів.

Ключовим результатом роботи стала розробка та обґрунтування методу тестування користувачів на стійкість до соціоінженерних маніпуляцій на основі імітаційних сценаріїв. Запропонований метод забезпечує комплексне оцінювання поведінкових реакцій користувачів, поєднуючи кількісні метрики з якісним аналізом причин помилкових дій та їх зв’язку з організаційним контекстом. Практична реалізація методу дозволила ідентифікувати пріоритетні ризики, визначити слабкі місця в поведінці користувачів і сформувати обґрунтовані рекомендації щодо зниження ризику компрометації інформаційних активів.

У межах третього розділу розроблено та апробовано комплекс контрзаходів, який включає адаптивні навчальні програми, організаційні процедури перевірки критичних дій та технологічні обмеження, спрямовані на мінімізацію наслідків людських помилок. Результати повторного тестування підтвердили ефективність запропонованого підходу, що проявилося у зниженні показників сприйнятливості до соціоінженерних атак та підвищенні готовності користувачів до своєчасного виявлення загроз.

Отримані результати свідчать про доцільність інтеграції імітаційного тестування та поведінкового аналізу у загальну систему управління інформаційною безпекою організації. Запропонований метод і сформовані рекомендації мають практичну цінність для вдосконалення корпоративних програм підвищення обізнаності, управління ризиками соціальної інженерії та розвитку культури безпеки. Водночас результати роботи створюють наукове підґрунтя для подальших досліджень у сфері поведінкової інформаційної безпеки, зокрема щодо адаптації сценаріїв атак до нових технологічних і соціальних умов та вдосконалення методів оцінювання стійкості користувачів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Schmitt M., Flechais I. Digital deception: generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review*. 2024. Vol. 57, no. 12. URL: https://doi.org/10.1007/s10462-024-10973-2

2. Andrew T. Rozema, James C. Davis Anti-Phishing Training (Still) Does Not Work: A Reproduction of Phishing Training Inefficacy Grounded in the NIST Phish Scale 2025. URL: https://arxiv.org/pdf/2506.19899

3. ADVERT: An Adaptive and Data-Driven Attention Enhancement Mechanism for Phishing Prevention / L. Huang et al. *IEEE Transactions on Information Forensics and Security*. 2022. P. 1. URL: https://doi.org/10.1109/tifs.2022.3189530

4. Rebeka Toth, Richard A. Dubniczky, Olga Limonova, Norbert Tihanyi Sustaining Cyber Awareness: The Long-Term Impact of Continuous Phishing Training and Emotional Triggers 2025. URL: https://arxiv.org/pdf/2510.27298

5. Solar Winds Cyber Attack fortinet.com URL: https://www.fortinet.com/resources/cyberglossary/solarwinds-cyber-attack

6. Dawkins S. NIST Phish Scale User Guide. Gaithersburg, MD : National Institute of Standards and Technology, 2023. URL: https://doi.org/10.6028/nist.tn.2276

7. What Is Reverse Social Engineering? And How Does It Work? URL: https://aware.eccouncil.org/what-is-reverse-social-engineering.html

8. Соціальна інженерія URL: https://stopfraud.gov.ua/cybersecurity-in-work/sotsialnyj-inzhyniryng-i317

9. Що Таке OSINT у 2025 URL: https://www.molfar.institute/shcho-take-osint-u-2024-gaid-vid-molfar/

10. Що таке фішинг, як його розпізнати і як із ним боротися URL: https://digvel.com.ua/blog/shho-take-fishyng-i-yak-iz-nym-borotysya/

11. Основні типи фішингових атак. Як бізнесу захиститися від дій зловмисників? URL: https://ua.issp.com/post/phishing

12. Вішинг URL: https://www.eset.com/ua/support/information/entsyklopediya-zahroz/vishynh

13. Principle of Information System Security: History URL: https://www.geeksforgeeks.org/computer-networks/principal-of-information-system-security-history/

14. Tzavara V., Vassiliadis S. Tracing the evolution of cyber resilience: a historical and conceptual review. International Journal of Information Security. 2024. URL: https://doi.org/10.1007/s10207-023-00811-x

15. Method of vulnerabilities analysis of socio-technical systems to the social engineering influences / R. Herasymov et al. Collection "Information Technology and Security". 2020. Vol. 8, no. 1. P. 31–39. URL: https://doi.org/10.20535/2411-1031.2020.8.1.218001

16. Zhmurko O. Social engineering as a threat to cybersecurity: methods of prevention and protection. Health and Safety Pedagogy. 2024. Vol. 9, no. 1. P. 37–42. URL: https://doi.org/10.31649/2524-1079-2024-9-1-037-042

17. Інструменти віртуальної лабораторії тестування співробітників для визначення готовності протидії фішинговим атакам / С. Бучик та ін. Information and communication technologies, electronic engineering. 2022. Т. 2, № 1. С. 44–51. URL: https://doi.org/10.23939/ictee2022.01.044

18. Evaluating the Information Security Awareness of Smartphone Users / R. Bitton et al. CHI '20: CHI Conference on Human Factors in Computing Systems, Honolulu HI USA. New York, NY, USA, 2020. URL: https://doi.org/10.1145/3313831.3376385

19. Oner U., Cetin O., Savas E. Human factors in phishing: Understanding susceptibility and resilience. Computer Standards & Interfaces. 2025. Vol. 94. P. 104014. URL: https://doi.org/10.1016/j.csi.2025.104014

20. Content, Nudges and Incentives: A Study on the Effectiveness and Perception of Embedded Phishing Training / D. Lain et al. CCS '24: ACM SIGSAC Conference on Computer and Communications Security, Salt Lake City UT USA. New York, NY, USA, 2024. P. 4182–4196. URL: https://doi.org/10.1145/3658644.3690348

21. Predicting User Susceptibility to Phishing Based on Multidimensional Features / R. Yang et al. Computational Intelligence and Neuroscience. 2022. Vol. 2022. P. 1–11. URL: https://doi.org/10.1155/2022/7058972

22. What Is Credential Harvesting? URL: www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/credential-harvesting

23. Merritt M. Building a Cybersecurity and Privacy Learning Program. Gaithersburg, MD : National Institute of Standards and Technology, 2023. URL: https://doi.org/10.6028/nist.sp.800-50r1.ipd

24. ERNEST O. NONUM, OGHENETEGA AVWOKURUAYE, ALIYU MUSTAPHA UMAR. SOCIAL ENGINEERING: UNDERSTANDING HUMAN FACTORS IN CYBER SECURITY. International Journal of Convergent and Informatics Science Research. 2025. URL: https://doi.org/10.70382/hijcisr.v07i9.032

25. Building your ISMS: From legal compliance to risk maturity URL: https://www.dataguard.com/blog/building-isms-framework-steps-best-practices/

26. Haney J. The Federal Cybersecurity Awareness Programs:. Gaithersburg, MD : National Institute of Standards and Technology, 2022. URL: https://doi.org/10.6028/nist.ir.8420

27. HANDBOOK FOR CYBER STRESS TESTS ENISA URL: https://www.enisa.europa.eu/sites/default/files/2025-05/2025.04311_01_ms_v2.0_Handbook%20for%20Cyber%20Stress%20Tests_en.pdf

28. Prümmer J., van Steen T., van den Berg B. A systematic review of current cybersecurity training methods. Computers & Security. 2023. P. 103585. URL: https://doi.org/10.1016/j.cose.2023.103585

29. RAISING AWARENESS OF CYBERSECURITY ENISA URL: https://ega.ee/wp-content/uploads/2021/12/ENISA-Report-Raising-awareness-a-key-element-of-national-cybersecurity-strategies.pdf

30. Покращення захищеності інформаційних систем у сучасних умовах URL: https://snt.ua/en/about/snt-ukraine-media/pokrashchennya-zahishchenosti-informacijnih-sistem-v-suchasnih-umovah

31. Understanding the Efficacy of Phishing Training in Practice / G. Ho et al. 2025 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 12–15 May 2025. 2025. P. 37–54. URL: https://doi.org/10.1109/sp61157.2025.00076

32. ENISA ETL2020 – Phishing URL: https://www.enisa.europa.eu/sites/default/files/publications/ETL2020%20-%20Phishing%20A4.pdf

33. Phishing Simulation Benchmarks: How Does Your Organization Compare URL: https://keepnetlabs.com/blog/phishing-simulation-benchmarks-how-does-your-organization-compare

34. Create targeted attack simulation training campaigns with dynamic groups URL: https://techcommunity.microsoft.com/blog/microsoftdefenderforoffice365blog/create-targeted-attack-simulation-training-campaigns-with-dynamic-groups/4287637

35. 7 Phishing Simulation Best Practices: The 2025 Guide URL: https://www.brside.com/blog/7-phishing-simulation-best-practices-the-2025-guide

36. Phishing Simulation Best Practices: 2025 Playbook for Real-World Behavior Change URL: https://hoxhunt.com/blog/phishing-simulation-best-practices

37. What is a phishing simulation? URL: https://sosafe-awareness.com/glossary/phishing-simulation/

38. Соціальна інженерія: Атака і захист URL: https://cyberset.com.ua/beginners/social-engineering-what-it-is-and-methods

39. Захист фінансових транзакцій від соціальної інженерії URL: https://ipag.com.ua/2025/09/zahyst-finansovyh-tranzaktsij-vid-sotsialnoyi-inzheneriyi

40. Козубцова Л., Хлапонін Ю., Козубцов І. Методика оцінювання ефективності виконання заходів забезпечення кібербезпеки об’єктів критичної інформаційної інфраструктури організацій. Сучасні інформаційні технології у сфері безпеки та оборони. 2021. Т. 41, № 2. С. 17–22. URL: https://doi.org/10.33099/2311-7249/2021-41-2-17-22

41. Chubaievskyi V., Bogma O., Silakova H. METHODS OF EVALUATION OF EFFICIENCY OF CORPORATE INFORMATION PROTECTION SYSTEMS OF DOMESTIC ENTERPRISES. Economic scope. 2022. URL: https://doi.org/10.32782/2224-6282/177-10

42. Diana Ussher-Eke. From awareness to action: Designing effective cybersecurity training programs. International Journal of Science and Research Archive. 2025. Vol. 16, no. 2. P. 494–504. URL: https://doi.org/10.30574/ijsra.2025.16.2.2348

43. Навчання персоналу: ключ до підвищення рівня кібербезпеки в компанії URL: https://speka.ua/business/navcannya-personalu-klyuc-do-pidvishhennya-rivnya-kiberbezpeki-v-kompaniyi-pn0kq1

44. TASEP: A Collaborative Social Engineering Tabletop Role-Playing Game to Prevent Successful Social Engineering Attacks / L. Hafner et al. ARES 2023: The 18th International Conference on Availability, Reliability and Security, Benevento Italy. New York, NY, USA, 2023. URL: https://doi.org/10.1145/3600160.3605005

45. Rahartomo A., Ghaleb A. T. A., Ghafari M. Phishing Awareness via Game-Based Learning. 2025 IEEE/ACM 37th International Conference on Software Engineering Education and Training (CSEE&T), Ottawa, ON, Canada, 27 April – 3 May 2025. 2025. P. 287–291. URL: https://doi.org/10.1109/cseet66350.2025.00036

46. СОЦІАЛЬНО-ПРАВОВІ ТА МОРАЛЬНО-ЕТИЧНІ ПРОБЛЕМИ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ТА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ / Н. Є. Філіпенко та ін. Вісник Пенітенціарної асоціації України. 2024. № 4. С. 95–103. URL: https://doi.org/10.34015/2523-4552.2023.4.10

47. Legal Framework for Phishing Simulations: A Compliance Guide for CISOs (GDPR, NIS2, DORA) URL: https://kymatio.com/blog/legal-framework-for-phishing-simulations-a-compliance-guide-for-cisos-gdpr-nis2-dora

48. Steves M., Greene K., Theofanos M. Categorizing human phishing difficulty: a Phish Scale. Journal of Cybersecurity. 2020. Vol. 6, no. 1. URL: https://doi.org/10.1093/cybsec/tyaa009

49. SoK: Human-Centered Phishing Susceptibility / S. Zhuo et al. ACM Transactions on Privacy and Security. 2022. URL: https://doi.org/10.1145/3575797

50. Vestad A., Yang B. A survey of agent-based modeling for cybersecurity. 15th International Conference on Applied Human Factors and Ergonomics (AHFE 2024). 2024. URL: https://doi.org/10.54941/ahfe1004768

51. Machine Learning and Neural Networks for Phishing Detection: A Systematic Review (2017–2024) / J. L. Wilk-Jakubowski et al. Electronics. 2025. Vol. 14, no. 18. P. 3744. URL: https://doi.org/10.3390/electronics14183744

52. The Anatomy of a Deepfake Voice Phishing Attack: How AI-Generated Voices Are Powering the Next Wave of Scams URL: https://www.group-ib.com/blog/voice-deepfake-scams

53. Machine learning techniques for phishing detection: A review of methods, challenges, and future directions / E. Kytidou et al. Intelligent Decision Technologies. 2025. URL: https://doi.org/10.1177/18724981251366763

54. Phishing Trends Report (Updated for 2025) URL: https://hoxhunt.com/guide/phishing-trends-report

55. Zero Trust Architecture / S. Rose et al. National Institute of Standards and Technology, 2020. URL: https://doi.org/10.6028/nist.sp.800-207

56. The history and evolution of zero-trust security URL: https://www.techtarget.com/whatis/feature/History-and-evolution-of-zero-trust-security

57. How Social Engineering Is a Threat in Cybersecurity URL: https://www.uscsinstitute.org/cybersecurity-insights/blog/how-social-engineering-is-a-threat-in-cybersecurity

58. What real-world data reveals about the effectiveness of phishing simulations URL: https://sosafe-awareness.com/blog/real-world-data-effectiveness-phishing-simulations

59. Simulation Model of Social Engineering Attacks in Business Enterprises. Journal of Information Engineering and Applications. 2012. URL: https://doi.org/10.7176/jiea/11-2-10

60. BEC: The Growing Threat of Business Email Compromise URL: https://www.fortinet.com/resources/cyberglossary/business-email-compromise

61. Siddiqi M. A., Pak W., Siddiqi M. A. A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. Applied Sciences. 2022. Vol. 12, no. 12. P. 6042. URL: https://doi.org/10.3390/app12126042