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

«На правах рукопису»
УДК _____

«До захисту допущено»
Завідувач кафедри
_____ Дмитро ЛАНДЕ
(підпис)
«_____»_____2025 р.

Магістерська дисертація

на здобуття ступеня магістра

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

на тему: Цифрова форензика соціальної інженерії у середовищі критичної інфраструктури

Виконав (-ла): здобувач вищої освіти ІІ курсу, групи ФБ-42мп
(шифр групи)

Алькова Аліна Максимівна
(прізвище, ім'я, по батькові) (підпис)

Керівник доцент кафедри ІБ, к.т.н, Стьопочкіна Ірина Валеріївна
(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові) (підпис)

Рецензент доцент кафедри ММЗІ, к.т.н, Яковлев Сергій Володимирович
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище, ім'я, по батькові) (підпис)

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

Київ – 2025 року

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

Рівень вищої освіти – другий (магістерський)
Спеціальність – 125 «Кібербезпека та захист інформації»
Освітньо-професійна програма «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ Дмитро ЛАНДЕ
(підпис)

«___»_____2025 р.

ЗАВДАННЯ
на магістерську дисертацію здобувачу вищої освіти

Алькова Аліна Максимівна
(прізвище, ім'я, по батькові)

1. Тема роботи: «Цифрова форензика соціальної інженерії у середовищі критичної інфраструктури»,
керівник роботи: Стьопочкіна Ірина Валеріївна, кандидат наук, доцент кафедри інформаційної безпеки,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом по університету від 4 листопада 2025 р. № 4797-С

2. Термін подання здобувачем вищої освіти роботи 17 грудня 2025 р.

3. Вихідні дані до роботи: джерела цифрової форензики для SCADA/OT середовищ, опис характерних атак соціальної інженерії та їх індикаторів, положення ризик-моделі FAIR, вимоги міжнародних стандартів кібербезпеки, що визначають контрольні заходи та вимоги до моніторингу.

4. Зміст роботи: аналіз загроз соціальної інженерії в середовищі критичної інфраструктури, визначення основних індикаторів таких атак на основі дослідження реальних випадків, огляд процессу цифрової форензики для ОКІ, формування чеклісту індикаторів для різних сценаріїв, розробка методики кваліметричного оцінювання ризику пропуску інцидентів соціальної інженерії, створення програмної реалізації запропонованої методики.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо): Презентація до захисту дипломної роботи

6. Дата видачі завдання : 19.03.2025

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Визначення напрямку роботи, узгодження теми з науковим керівником	19.03.2025	Виконано
2	Уточнення об’єкта та предмету дослідження, постановка дослідницьких завдань	20.03.2025 – 24.03.2025	Виконано
3	Огляд суміжних наукових робіт, розробка плану для першого розділу	30.03.2025 – 06.04.2025	Виконано
4	Детальний аналіз методів та видів атак соціальної інженерії	08.04.2025 – 21.04.2025	Виконано
5	Збір та вивчення реальних кейсів атак соціальної інженерії на ОКІ	23.04.2025 – 05.05.2025	Виконано
6	Огляд проблеми людського фактора та психологічних маніпуляцій в контексті соціальної інженерії	10.05.2025 – 19.05.2025	Виконано
7	Огляд процесу цифрової форензики в контексті критичної інфраструктури	02.06.2025 – 16.06.2025	Виконано
8	Формування чеклісту індикаторів різних сценаріїв атак соціальної інженерії	23.06.2025 – 11.07.2025	Виконано
9	Визначення джерел форензичних даних та співвідношення їх до індикаторів та сценаріїв	21.07.2025 – 04.08.2025	Виконано
10	Побудова відповідної матриці співвідношення, а також графіку важливості активів	06.08.2025 – 18.08.2025	Виконано
11	Розробка методики до оцінювання ризику пропуску системою таких інцидентів на ОКІ	29.08.2025 – 06.09.2025	Виконано
12	Формування контрольних запитань для методики, побудова матриць вагових коєфіцієнтів	08.09.2025 – 22.09.2025	Виконано
13	Створення програмної реалізації методики та тестування результатів	29.09.2025 – 23.10.2025	Виконано
14	Формування висновків, підготовка презентації	06.11.2025 – 31.11.2025	Виконано
15	Передзахист	17.12.2025	Виконано
16	Захист	24.12.2025	Виконано

Здобувач вищої освіти _____ Аліна АЛЬКОВА
(підпис) **(Власне ім’я, ПРІЗВИЩЕ)**

Керівник роботи _____ Ірина СТЬОПОЧКІНА
(підпис) **(Власне ім’я, ПРІЗВИЩЕ)**

РЕФЕРАТ

Обсяг дипломної роботи 79 сторінки, 13 ілюстрацій, 2 таблиці, 1 додаток і 32 джерел літератури.

Об’єкт дослідження: інциденти кібербезпеки на основі атак соціальної інженерії у середовищі критичної інфраструктури.

Предмет дослідження: методи оцінювання ризиків пропуску інцидентів соціальної інженерії.

Мета дослідження: розробка методики кваліметричного оцінювання ризику пропуску інцидентів соціальної інженерії на об’єктах індустріального типу на основі аналізу покриття форензичними індикаторами.

Методи дослідження: огляд літературних джерел за суміжною тематикою, аналіз головних індикаторів кожного типу соціальної інженерії, формування методики оцінювання ризику пропуску таких інцидентів, застосування програмної реалізації алгоритму обрахунку.

Отримані результати: сформовано список індикаторів для різних типів атак соціальної інженерії у поєднанні з пристроями фіксації, побудовано графік важливості активів ОТ-середовища, реалізовано методику оцінювання ризику пропуску інцидентів соціальної інженерії у середовищі критичної інфраструктури.

Результати роботи були представлені на ІІ Міжнародній науково-практичній студентській конференції «ІТ-ПРОСТІР СЬОГОДЕННЯ: ТЕНДЕНЦІЇ, ІННОВАЦІЇ ТА ПЕРСПЕКТИВИ РОЗВИТКУ» 2025 року.

Ключові слова: соціальна інженерія, критична інфраструктура, цифрова форензика, кваліметричне оцінювання ризику

ABSTRACT

The volume of the thesis is 79 pages, 13 illustrations, 2 tables, 1 appendix, and 32 literature sources.

Object of research: Cybersecurity incidents caused by social engineering attacks in critical infrastructure environments.

Subject of research: Methods for assessing the risk of missing (non-detecting) social engineering incidents.

Purpose of the study: To develop a methodology for qualimetric assessment of the risk of missing social engineering incidents at industrial-type facilities based on the analysis of coverage by forensic indicators.

Research methods: Review of scientific and technical literature in related fields; analysis of key indicators associated with different types of social engineering attacks; development of a qualimetric methodology for assessing the risk of missing such incidents; implementation of a software-based calculation algorithm.

Results: A set of forensic indicators for various types of social engineering attacks has been identified and correlated with corresponding detection devices; an asset importance graph for the OT environment has been constructed; a methodology for qualimetric assessment of the risk of missing social engineering incidents in critical infrastructure environments has been developed and implemented.

The results of the work were presented at the 2nd International Scientific and Practical Student Conference “IT Space of Today: Trends, Innovations and Development Prospects” (2025).

Keywords: social engineering, critical infrastructure, digital forensics, qualimetric assessment of the risk

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

SCADA – система диспетчерського керування та збору даних (Supervisory Control And Data Acquisition).

OT/IT – операційні та інформаційні технології (Operational Technology/Information Technology).

ICS – промислові системи керування (Industrial Control Systems).

ОКІ – об’єкти критичної інфраструктури.

ПЗ/ШПЗ – програмне забезпечення та шкідливе програмне забезпечення.

MFA – багатофакторна автентифікація (Multi-Factor Authentication).

IDS/IPS – системи виявлення та запобігання вторгненням (Intrusion Detection System/Intrusion Prevention System).

PLC – програмований логічний контролер (Programmable Logic Controller)

RTU – віддалений термінальний пристрій (Remote Terminal Unit).

HMI – людино-машинний інтерфейс (Human Machine Interface).

MTU – головний термінальний пристрій SCADA-системи (Master Terminal Unit).

OPC server – сервер обміну даними між компонентами промислових систем (OLE for Process Control server).

IED – інтелектуальний електронний пристрій (Intelligent Electronic Device).

ВСТУП

Актуальність роботи:

У контексті цифрової трансформації критична інфраструктура інтегрує дедалі більше автоматизованих систем керування, розподілених сенсорних мереж і взаємопов’язаних сервісів. Це підвищує ефективність технологічних процесів, але водночас створює нові точки вразливості, особливо у взаємодії між людьми та технологіями. SCADA-системи, що керують виробничими та технологічними процесами перебувають під зростаючим тиском кіберзагроз, значна частина яких починається не з технічних, а з психологічних маніпуляцій персоналом.

Дослідження у сфері OT-безпеки свідчать, що до 70% атак на SCADA-платформи починаються з компрометації персоналу – через фішинг, підроблені запити, маніпуляції чи інші методи психологічного впливу. Через специфіку SCADA-середовищ, у яких пріоритет часто надається безперервності роботи, а не інтенсивному моніторингу, велика частина інцидентів залишається непоміченою або фіксується із запізненням. Усе це створює потребу в інструментах, які дозволяють оцінювати ризики саме пропуску таких атак, використовуючи доступні форензичні дані. З огляду на обмеження традиційних методів і фрагментарність джерел цифрових доказів у промислових системах, виникла необхідність у створенні інструменту, який би поєднав структуровану експертну оцінку, принципи цифрової форензики та елементи кваліметричного аналізу для оцінювання рівня ризику пропуску інцидентів соціальної інженерії у SCADA-середовищах.

Мета цієї дипломної роботи: розробка методики кваліметричного оцінювання ризику пропуску інцидентів соціальної інженерії на об’єктах критичної інфраструктури на основі аналізу покриття форензичними індикаторами.

Завдання дослідження:

1. Ознайомитися сучасними методами соціальної інженерії у сфері критичної інфраструктури та провести детальний огляд реальних кейсів атак, визначити їх основі напрями.
2. Дослідити процес цифрової форензики соціальної інженерії та визначити основні індикатори загроз, що можуть фіксуватися на SCADA пристроях.
3. На основі проведеного аналізу сформувати чекліст співвідношення різних сценаріїв атак до відповідних індикаторів та пристроїв фіксації. За допомогою цього побудувати матрицю та графік важливості активів щодо форензичних даних.
4. Дослідити модель FAIR та визначити, які її елементи можуть бути адаптовані для оцінювання ризиків в OT-контексті. На основі цього розробити алгоритм оцінювання ризику пропуску інцидентів соціальної інженерії.
5. Створити програмний прототип методики та продемонструвати його здатність оцінювати ризики пропуску системою атак соціальної інженерії.

Об'єкт дослідження: інциденти кібербезпеки на основі атак соціальної інженерії у середовищі критичної інфраструктури.

Предмет дослідження: методи оцінювання ризиків пропуску інцидентів соціальної інженерії.

Методи дослідження: огляд літературних джерел за суміжною тематикою, аналіз головних індикаторів кожного типу соціальної інженерії, формування методики оцінювання ризику пропуску таких інцидентів, застосування програмної реалізації алгоритму обрахунку.

Новизна одержаних результатів: У роботі вперше запропоновано методику кваліметричного оцінювання ризику пропуску інцидентів соціальної інженерії у SCADA-середовищах на основі аналізу покриття форензичними індикаторами. Методика інтегрує структуровану експертну оцінку, принципи цифрової

форензики та окремі елементи моделі FAIR для формалізації ймовірнісної складової ризику пропуску інцидентів. Додатково сформовано спеціалізований чекліст форензичних індикаторів для OT/SCADA-систем і реалізовано програмний інструмент для оцінювання рівня ризику пропуску, що не представлено в існуючих дослідженнях.

Практичне значення одержаних результатів: Можливість застосування запропонованого підходу для підсилення наявних систем моніторингу OT/ICS, оптимізації політик безпеки та підвищення рівня кіберстійкості критичних об’єктів. Розроблений прототип може бути інтегрований як допоміжний модуль у середовище SOC/SIEM або використовуватись у внутрішніх аудитах для визначення прогалин у системах виявлення. У перспективі підхід може слугувати основою для вдосконалення систем оцінювання ризиків, що враховують як форензичні дані, так і поведінкові характеристики атак соціальної інженерії.

Апробація результатів: Результати роботи були представлені на II Міжнародній науково-практичній студентській конференції «ІТ-ПРОСТІР СЬОГОДЕННЯ: ТЕНДЕНЦІЇ, ІННОВАЦІЇ ТА ПЕРСПЕКТИВИ РОЗВИТКУ» 2025 року [32].

1 ТЕОРИТИЧНІ ЗАСАДИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ ТА ОСОБЛИВОСТІ ЇЇ ПРОЯВІВ В СЕРЕДОВИЩІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1 Розвиток соціальної інженерії як загрози інформаційній безпеці

Сфера інформаційної безпеки стрімко розвивається у відповідь на зростаючі загрози незаконного доступу до конфіденційної інформації. Незважаючи на розвиток технологічних засобів захисту, людський фактор часто залишається найслабшою ланкою у системі безпеки.

Термін «соціальна інженерія» вперше з’явився у 1842 році в книзі британського економіста Джона Грея "Ефективний засіб для подолання бідності націй". Грей використовував його для опису спроб маніпулювання суспільними процесами з метою досягнення економічних або політичних цілей [1]. Він порівнював «політичних і соціальних інженерів», які намагалися оптимізувати соціальні процеси за допомогою раціонального планування, з тими, хто прагнув реформувати економічні системи. Ця рання концепція заклала основу сучасного розуміння соціальної інженерії як маніпулятивного впливу на людей для досягнення певних цілей. Починаючи з 2007 року, спостерігається зближення політичного та кібербезпекового використання терміна "соціальна інженерія". Маніпулятивні техніки політичних кампаній, спрямовані на вплив на громадську думку через соціальні мережі, мають багато спільного з методами кіберсоціальної інженерії. У контексті критичної інфраструктури це створює додаткові виклики: зловмисники можуть використовувати фальшиві профілі, дезінформацію або соціальні мережі для маніпуляції працівниками, що потенційно загрожує роботі енергетичних, медичних та інших критичних систем.

Автори статті [2] запропонували найбільш точне визначення соціальної інженерії, як «науки використання соціальної взаємодії для переконання особи чи організації виконати певний запит зловмисника, де соціальна взаємодія,

переконання або запит пов’язані з комп’ютерною сутністю». У NIST SP 800-53, версії Revision 5, підконтроль AT-2(3) соціальна інженерія визначається як спроба обманом змусити особу розкрити інформацію або виконати дію, яка може бути використана для порушення безпеки [3].

Насправді розвиток соціальної інженерії як дисципліни перебуває на відносно ранніх стадіях. Існує багато моделей атак, запропонованих різними дослідниками. Найпопулярніші з них включають [4]:

- Mitnick & Simon (2002): запропонували практичний підхід до соціальної інженерії, описавши її через низку етапів атаки: збір інформації, виклик довіри, експлуатація, виконання цілі. Ця модель орієнтована на практичне розуміння, як зловмисники отримують доступ до конфіденційної інформації через взаємодію з людьми.
- Hadnagy (2010): розробив модель психологічного впливу, яка акцентує увагу на емоційних та когнітивних механізмах, що змушують жертву реагувати на маніпуляції. Вона використовується для оцінки вразливостей поведінки користувачів у кіберпросторі.
- Ahlfeldt(2005) і Culpepper (2004): створили концептуальні моделі, що систематизують види соціальної інженерії та техніки атак, виділяючи категорії, такі як фішинг, вішинг, прептекстинг і байтинг. Їхні роботи допомагають класифікувати атаки та розробляти методи запобігання.
- Hamill(2005) і Lenkart (2011): запропонували багаторівневі моделі, які описують фазову структуру атак – від попереднього збору інформації до реалізації цільових дій, включно з механізмами психологічного впливу.
- Mouton(2012, 2014): розробив онтологічну модель соціальної інженерії, яка уточнює визначення терміна та формалізує взаємозв’язки між етапами атаки, психологічними чинниками та комп’ютерними системами.
- Nohlberg (2008) і Thornburgh (2004): акцентують увагу на методологічних аспектах дослідження соціальної інженерії, надаючи рекомендації щодо формалізації даних і оцінки ризиків.

- Kingsley Ezechi (2011): розробив узагальнену модель атак, що поєднує технічні та поведінкові аспекти, дозволяючи інтегрувати кібер- та організаційні ризики.

У типовій атаці соціальної інженерії кіберзлочинець встановлює контакт із потенційною жертвою, представляючись співробітником довіреної організації. У деяких випадках зловмисник навіть імітує особу, яку жертва добре знає, щоб підвищити рівень довіри.

Якщо маніпуляція вдається і жертва вірить, що співрозмовник є тим, за кого себе видає, зловмисник заохочує її до подальших дій. Це може включати надання конфіденційної інформації, такої як паролі, дата народження чи реквізити банківського рахунку. Крім того, жертву можуть спрямувати на вебсайт, на якому встановлено шкідливе програмне забезпечення, здатне порушити роботу її пристрою. У гірших випадках такий вебсайт може викрасти конфіденційні дані або навіть повністю взяти під контроль пристрій жертви.

Особливу небезпеку соціальної інженерії становить те, що атака не потребує успіху проти всіх співробітників організації. Навіть один обманутий користувач може надати достатньо інформації для проведення атаки, яка вплине на всю організацію [5].

З часом атаки соціальної інженерії стали дедалі витонченішими. Підроблені вебсайти та електронні листи часто виглядають настільки реалістично, що жертви не помічають загрози та надають дані, які зловмисники можуть використати для крадіжки особистості. Крім того, соціальна інженерія залишається однією з найпоширеніших стратегій для порушення початкового рівня захисту організації з метою подальших руйнівних дій.

1.2 Основні техніки та типи атак соціальної інженерії в цифровому та фізичному середовищах

Соціальна інженерія належить до категорії атак, які здатні обійти апаратні чи програмні засоби захисту, що традиційно застосовуються для запобігання кіберзагрозам. Як вже зазначалось її складність полягає у тому, що технічні механізми безпеки малоефективні, якщо основною ціллю зловмисника є користувач, який взаємодіє з системою.

Отже, ефективна протидія таким загрозам неможлива виключно за рахунок технічних рішень – вона обов'язково має включати активну участь користувача. Важливим елементом стає навчання персоналу, розвиток навичок критичного мислення та формування усвідомленої поведінки в цифровому середовищі.

Для кращого відображення суті соціальної інженерії, нижче наведена схема взята з одного з джерел [6]:

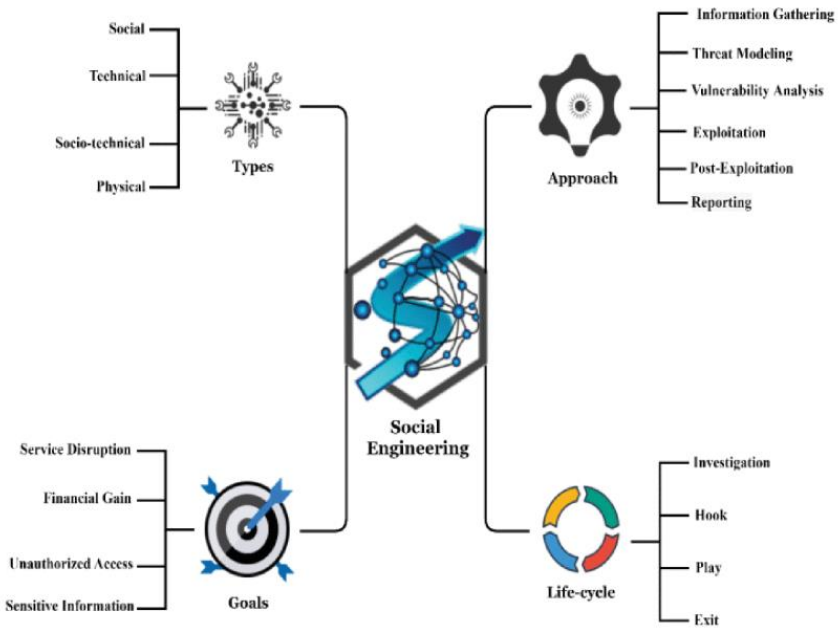

Рисунок 1.1 – Схема опису поняття атак соціальної інженерії

Розглянемо її детальніше. Загалом у науковій літературі соціальну інженерію поділяють на кілька основних категорій залежно від засобів і підходів, які використовують зловмисники:

1. Фізичні методи: цей підхід ґрунтується на пошуку інформації у матеріальних носіях – наприклад, у викинутих документах, нотатках, внутрішніх інструкціях чи довідниках. Мета полягає у зборі будь-яких чутливих відомостей, що можуть допомогти сформувати профіль жертви або організації.
2. Соціальні методи: найпоширеніший тип соціальної інженерії, що використовує психологічні прийоми для впливу на людину. Сюди належать встановлення довіри, створення фальшивих сценаріїв, а також техніки, як-от фішинг, вішинг, смішинг, бейтинґ чи зворотна соціальна інженерія. Ці методи зазвичай реалізуються через електронні листи, телефонні дзвінки або текстові повідомлення.
3. Технічні методи**:** у цьому випадку акцент робиться на використанні онлайн-ресурсів і спеціалізованих інструментів. Соціальні мережі та пошукові системи стають основними джерелами інформації про потенційних жертв. Зловмисники можуть намагатися підбирати або зламувати паролі, а також застосовувати автоматизовані інструменти, зокрема Social-Engineer Toolkit (SET) чи Maltego, для збору даних і проведення атак.
4. Соціотехнічні методи: це найбільш комплексний підхід, що поєднує соціальні й технічні елементи. При плануванні атаки враховуються культурні особливості жертви, поведінкові чинники, наявні технології та навіть архітектура будівель чи організаційні процеси. Завдяки такому синтезу й багаторівневому впливу ефективність атак суттєво зростає.

Соціальна інженерія як складний процес включає низку послідовних етапів та підходів, спрямованих на пошук, використання та експлуатацію слабких місць людини й системи.

Серед етапів соціально-інженерної атаки виділяють:

1. Збір інформації – найбільш трудомістка фаза, де атакувальники збирають усі доступні відомості про жертву чи організацію. Використовуються як технічні інструменти (сканери, пошукові сервіси), так і традиційні методи, зокрема «dumpster diving» (пошук документів у смітті).
2. Моделювання загроз – виявлення слабких місць у системі безпеки, оцінка можливих сценаріїв атаки та визначення стратегій їх використання.
3. Аналіз вразливостей – визначення слабких сторін як технічного середовища, так і поведінки користувача, з подальшим підбором персоналізованих технік впливу.
4. Експлуатація – безпосереднє використання виявлених прогалин для отримання доступу до ресурсів, викрадення даних чи нанесення шкоди (наприклад, через шкідливе ПЗ або вимагання).
5. Постексплуатація – збереження контролю, збір додаткових даних, встановлення бекдорів і приховування слідів, щоб залишатися непомітним та мати можливість повторного доступу.
6. Завершення та звітність – коли цілі досягнуто, зловмисники завершують активність, приховуючи свою присутність.

Ці етапи також описують цикл атак соціальної інженерії, запропонований Кевіном Митніком у книзі «The art of deception: controlling the human element of security» [7], що вважається найбільш відомою та широко визнаною моделлю таких атак. У спрощеному вигляді його можна описати чотирма ключовими фазами:

- Ідентифікація цілі (Investigation/Target Identification) – вивчення жертви й пошук точок входу.
- «Гачок» (Hook/Deception) – встановлення контакту та формування довіри.
- Гра/Експлуатація (Play/Exploitation) – безпосереднє використання довіри та отримання доступу до даних чи систем.

- Вихід (Exit/Disengagement) – завершення атаки без підозри з боку жертви, маскування слідів та збереження можливості повернення.

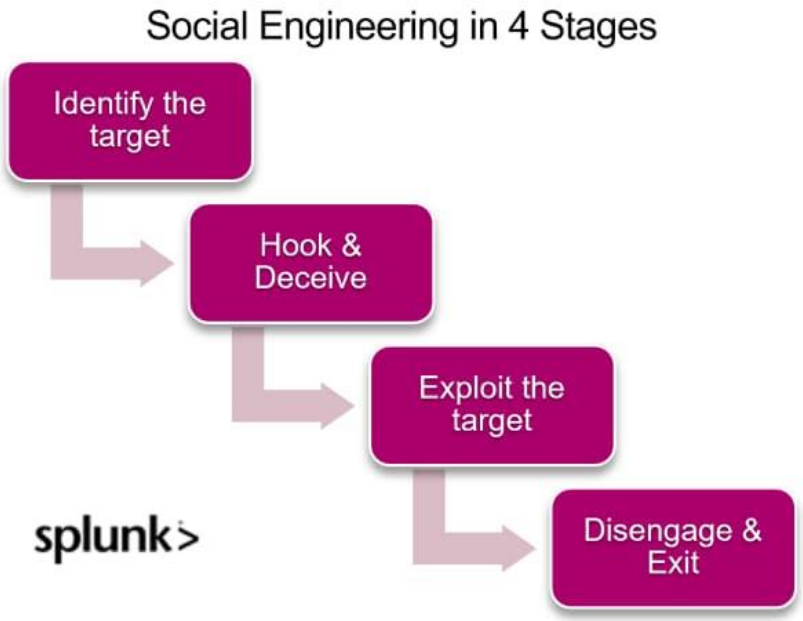

Рисунок 1.2 – Стадії атаки соціальної інженерії [8]

Таким чином, соціальна інженерія поєднує психологічні маніпуляції з технічними інструментами та вибудовується як системний підхід. Така структуризація дозволяє краще зрозуміти логіку дій атакуючого й будувати ефективні контрзаходи.

Методи соціальної інженерії надзвичайно різноманітні та постійно еволюціонують залежно від конкретних технік маніпуляції. Вони можуть варіюватися від класичного фішингу до складніших форм, що поєднують технічні засоби з психологічним впливом.

Як зазначено в NIST SP 800-53, версії Revision 5, підконтроль AT-2(3) серед найбільш поширених методів у кібербезпеці – фішинг, вішинг, підробка ідентичності, створення фальшивих вебсайтів, а також комбіновані багатокрокові атаки, які спрямовані на співробітників організацій із доступом до критичних систем.

Але в одному відкритому джерелі [9] вдалось знайти найбільш розширений опис усіх існуючих видів:

1. Phishing. Такий тип передбачає надсилання повідомлень, листів, які виглядають як легітимні, із метою змусити користувача виконати певні дії. Основна мета – отримати конфіденційні дані (логіни, паролі, банківські реквізити). Різновиди:

    - Email/Website Phishing – підроблені листи або вебсайти, які змушують користувачів розкривати дані.
    - Vishing – телефонні дзвінки, де жертва під психологічним тиском розкриває PIN-коди або одноразові паролі.
    - Smishing – SMS-повідомлення з вимогою термінових дій або передачі інформації.
    - Spear-phishing/Whaling – таргетовані атаки на конкретних осіб або керівників організацій; відрізняються високою персоналізацією і підготовкою.
    - Pharming – перенаправлення користувачів на підроблені сайти для збору інформації або фінансової вигоди.
    - Angler Phishing – клонування акаунтів служби підтримки компаній у соцмережах для обману клієнтів.

2. Grooming. Техніка психологічної маніпуляції, яка використовується для отримання конфіденційної інформації або контролю над потенційними жертвами через електронні засоби комунікації (SMS, електронна пошта, дзвінки). Основний механізм – встановлення довіри та поступове втягування жертви в небезпечну ситуацію.
3. Pretexting. Атакуючий створює переконливу легенду або фальшивий контекст, у якому він спілкується з жертвою, наприклад, пропонує допомогу, роботу або виграш призу. Цей метод передбачає двосторонню взаємодію і

використовує психологічні тригери: довіру, соціальний тиск або бажання вигоди.

4. Profile Cloning. Використання публічної інформації для створення фальшивого акаунта, що імітує реальну особу, з метою отримання доступу до контактів або конфіденційних даних. Часто поєднується з іншими методами, наприклад, претекстинг або фішинг.
5. Face-to-Face Interaction. Прямий контакт із жертвою для отримання фізичного доступу або інформації. Використовує психологічні слабкості: готовність допомогти, ввічливість або бажання уникнути конфлікту.
6. Shoulder Surfing. Спостереження за діями користувача при введенні конфіденційних даних. Відрізняється від інших методів тим, що не потребує технічних знань і не взаємодіє з жертвою прямо.
7. Quid Pro Quo. Метод взаємної вигоди: атакуючий пропонує допомогу чи сервіс в обмін на інформацію або доступ. Використовує принцип соціальної взаємності – люди схильні відповідати взаємністю.
8. Dumpster Diving. Збір конфіденційної інформації з фізичних документів, відходів або цифрових носіїв. Акцент на людській недбалості щодо утилізації інформації.
9. Diversion Theft. Впровадження шкідливого ПЗ через доставлені товари або пристрої. Основна відмінність – використання фізичних каналів доставки для проникнення у систему.
10. Piggybacking/Tailgating. Проникнення до об’єкта за супроводом працівників, які мають доступ. Метод заснований на експлуатації соціальної довіри та правил організаційного доступу.
11. File Masquerade. Вставляння шкідливих файлів під виглядом звичайних документів або медіа. Використовує психологічну впевненість користувачів у безпеці своїх пристроїв.
12. Baiting. Використання цікавості користувача: заражені USB-накопичувачі або інші фізичні та цифрові носії, що заманюють жертву.

13. Reverse Social Engineering. Атакуючий створює проблему для жертви, а потім пропонує рішення, що дозволяє йому отримати контроль над системою або інформацією.
14. Scareware/Pop-up атаки. Використання спливаючих вікон, повідомлень або звукових сигналів, які змушують жертву діяти необдумано, наприклад, встановлювати шкідливе ПЗ або надавати дані.
15. Water-Holing. Взлом сайтів із високим трафіком і розміщення на них шкідливого ПЗ. Метод націлений на жертву, яка регулярно відвідує ресурс.

Щодо основної мети соціальних інженерів – це маніпулювання людьми для отримання інформації чи доступу, що зазвичай недоступний. Серед конкретних мотивів атакуючих виділяють [6]:

- Фінансова вигода – прямий або опосередкований прибуток від шахрайських дій, наприклад через викрадення банківських даних або вимагання викупу.
- Самоствердження – бажання довести власну спритність і здатність обійти систему безпеки.
- Помста – атаки з метою завдати шкоди конкретній особі чи організації.
- Отримання знань – збір інформації про систему, організацію або індивідів для майбутніх атак або досліджень.
- Розваги – деякі соціальні інженери здійснюють атаки заради власного задоволення чи цікавості.

1.3 Вплив соціальної інженерії на критичну інфраструктуру: особливості та вразливості

Критична інфраструктура охоплює об’єкти та системи, порушення функціонування яких може мати масштабні наслідки для національної безпеки, економічної стабільності, соціального добробуту та охорони здоров’я населення. Вихід з ладу або навіть тимчасові збої у її роботі здатні спричинити значні втрати,

що відчутно впливають на суспільство й економіку, а також викликати ланцюгові ефекти, коли відмова одного елемента провокує перебої у суміжних секторах, створюючи потенційно катастрофічні сценарії [10].

Згідно з українським законодавством, зокрема Законом України «Про критичну інфраструктуру» та іншими нормативно-правовими актами, визначено 10 основних секторів критичної інфраструктури: енергетика та енергетичні ресурси, транспорт, комунальні послуги, інформаційно-комунікаційні технології та телекомунікації, охорона здоров'я, фінансовий сектор, виробничий сектор, аграрний сектор, державне управління та органи влади, освіта та наука [11].

Для приклада, було знайдено статтю [12], в якій розповідається, що у 2024 році Центр скарг на злочини в Інтернеті ФБР отримав 4 878 повідомлень від організацій, що належать до 14 із 16 секторів критичної інфраструктури, які постраждали від кіберзагроз. Серед цих повідомлень IC3 визначили критичні сектори інфраструктури, що найчастіше зазнавали атак програм-вимагачів та витоків даних, ранжуючи їх за кількістю інцидентів. Нижче наведена діаграма з їх звіту:

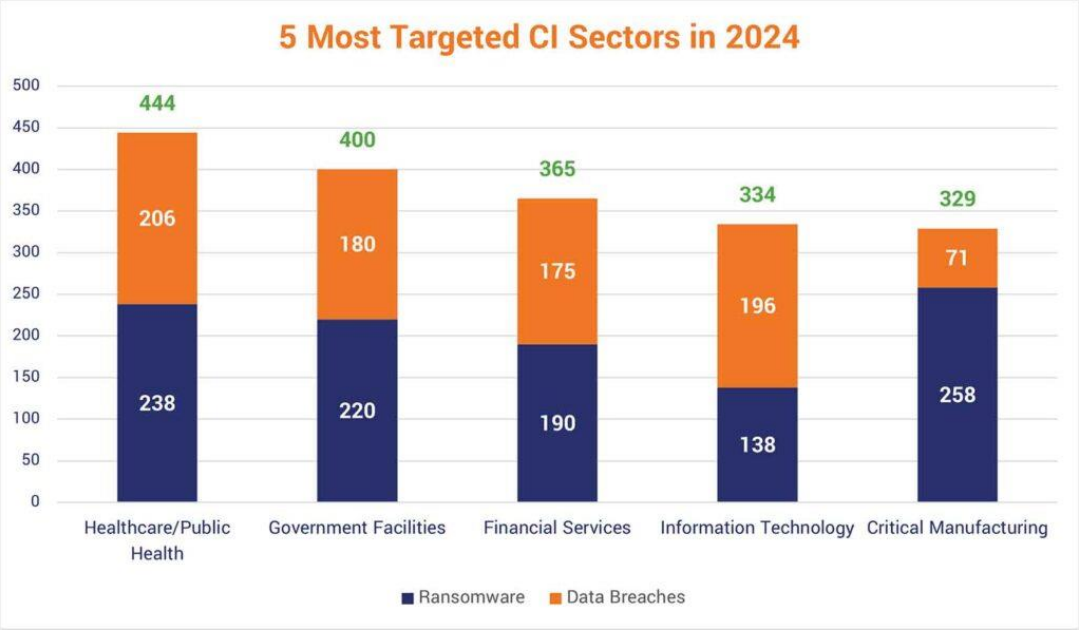

Рисунок 1.3 – Топ секторів критичної інфраструктури, що зазнали кіберзагроз у 2024 році [12]

Згідно з даними іншої статті [13], у США кількість потенційно вразливих об’єктів енергетичних мереж зростає приблизно на 60 щодня. Загалом між січнем 2023 і січнем 2024 року критична інфраструктура зазнала понад 420 мільйонів атак, що еквівалентно приблизно 13 атакам на секунду.

На практиці найбільш поширеним способом доставки програм-вимагачів залишаються саме методи соціальної інженерії, зокрема фішингові листи та шкідливі вкладення. Особливо вразливими є системи операційних технологій (OT) та промислові системи управління (ICS). Підключення OT і ICS до Інтернету або інших мереж робить їх привабливою ціллю для кіберзлочинців.

Зазвичай у відкритих джерелах [14] класифікують такі наслідки кібернападів на ОКІ:

- перебої в наданні основних послуг, таких як електроенергія, вода та природний газ;
- порушення виробництва та постачання продуктів харчування та медичних матеріалів;
- втрата довіри населення до економіки, національної безпеки та демократичних процесів;
- шкода довкіллю та ризики для здоров’я населення через викиди токсичних речовин або аварійні хімічні розливи;
- фінансові втрати, репутаційні ризики, скорочення робочих місць або юридичні наслідки для компаній і працівників;
- порушення роботи лікарень або критичних медичних пристроїв, що може призвести до втрат життя;
- пошкодження компонентів ОКІ, що може призвести до зупинки, руйнування або деградації процесів і операцій.

Основні загрози для критичної інфраструктури включають крадіжку критично важливої інформації, блокування конфіденційних файлів або витік комерційної та чутливої інформації.

Серед потенційних зловмисників, які атакують SCADA-мережі, можна виділити державні органи та спецслужби, промислових шпигунів, незадоволених співробітників, терористичні угруповання, хакерів, кримінальні організації та хактивістів [15].

Хоча атаки на ICS/SCADA у медіа часто асоціюються з такими як Stuxnet або Flame, насправді більшість загроз походить від стандартних методів соціальної інженерії, адже їх легко виконувати та не потребують високих технічних ресурсів. Найпоширенішими формами атак соціальної інженерії саме на ОКІ є:

- Phshing – такі атаки часто спрямовані на розвідку та отримання доступу для подальшого проникнення, а не на негайне виведення систем з ладу.
- Spearphishing – персоналізовані фішингові атаки, що таргетують конкретних співробітників, наприклад адміністраторів систем. Такі атаки можуть мати катастрофічні наслідки, як це сталося у грудні 2015 року в Україні, коли відімкнення електромережі почалося зі спірфішингової кампанії, що відкрила доступ до систем компаній через шкідливі документи Word.
- Pretexting – часто використовується через телефонні дзвінки, де зловмисники видають себе за представників сторонніх постачальників та намагаються отримати віддалений доступ до систем.

На даний момент, атаки соціальної інженерії залишаються одними з найнебезпечніших кіберзагроз у світі. Наприклад, автор статті [16] зазначає, що загальна сума збитків від соціальної інженерії в США оцінюється в 121,22 мільярда доларів.

Інший випадок – атака на Центральний банк, де зловмисники викрали понад 80 мільйонів доларів, використавши троянські програми віддаленого доступу,

встановлені на комп’ютерах банку. Значно популярні атаки типу «CEO fraud», коли зловмисники, видаючи себе за керівників компаній, надсилають електронні листи співробітникам із вимогами переказу коштів. Такі схеми призвели до втрат у розмірі понад 2,3 мільярда доларів.

Ці дані свідчать, що наслідки таких атак можуть перевищувати збитки навіть від природних катастроф, підкреслюючи критичну важливість своєчасного виявлення та протидії подібним кіберзагрозам.

1.4 Огляд реальних кейсів атак соціальної інженерії на ОКІ

Соціальна інженерія, як один із ключових методів кіберзагроз, у сучасних атаках на об’єкти критичної інфраструктури набуває особливого значення не стільки як самостійний інструмент, скільки як вступна процедура, що слугує «мостом» для подальшого впровадження більш складних технік, таких як розгортання шкідливого програмного забезпечення, експлуатація вразливостей чи латеральний рух у мережі, що також допомагає отримати перші облікові дані чи привілейовані акаунти. Таким чином, в більшості випадків соціальна інженерія не є ізольованою тактикою, а радше каталізатором.

Задля детального аналізу атак соціальної інженерії, було знайдено у відкритих джерелах хронологію [17], що фіксує значні кіберінциденти, починаючи з 2006 року, а саме кібератаки на державні установи, оборонні та високотехнологічні компанії, а також економічні злочини з втратами понад один мільйон доларів. Серед них була зроблена вибірка, тих атак, що стосуються соціальної інженерії:

- Квітень 2025: Північнокорейські кібершпигуни розширюють свої операції з проникнення, націлюючись на європейські оборонні та державні організації. Хакери видавали себе за віддалених працівників для викрадення даних,

шпигунства та отримання доходу, все частіше використовуючи шантаж щодо колишніх роботодавців після отримання доступу. Позування як віддалені працівники для інфільтрації – класичний приклад pretexting.

- Березень 2025**:** Мережа підставних компаній, пов’язаних із китайською технологічною фірмою, націлилася на нещодавно звільнених співробітників уряду США через оголошення про роботу на сайтах вакансій. Операція використовувала фальшиві консалтингові компанії з неіснуючими контактними даними та адресами, що повторює методи, які ФБР вважає потенційними тактиками вербування для іноземної розвідки. Тут використовувався baiting/pretexting для вербування та шпигунства.
- Лютий 2025: Китайські кіберакторські групи провели координаційну дезінформаційну кампанію у WeChat проти канадської кандидатки на лідерство Ліберальної партії. Операція включала численні акаунти, що поширювали дискредитуючий контент, пов’язаний з КНР, і охопила 2–3 мільйони користувачів WeChat по всьому світу.
- Січень 2025: Підозрювані російські хакери здійснили spearphishing-атаки проти дипломатичних органів Казахстану. Хакери вставили шкідливий код у дипломатичні документи, включаючи один документ, який нібито описував угоду між Німеччиною та кількома країнами Центральної Азії, з метою кібершпигунства.
- Грудень 2024: Російські хакери запустили фішингову кампанію проти Збройних сил України та оборонних підприємств. Атакуючі використовували інструменти віддаленого доступу для проникнення в військові системи та крадіжки облікових даних із платформ на кшталт Telegram та локальних мереж.
- Листопад 2024: Іранські хакери націлилися на аерокосмічну, оборонну та авіаційну промисловість в Ізраїлі, ОАЕ, Туреччині, Індії та Албанії, за даними ізраїльських звітів. Хакери видавали себе за рекрутерів у LinkedIn і розповсюджували шкідливе ПЗ через фальшиві привабливі пропозиції

роботи для шпигунства та крадіжки конфіденційних даних. Позування як рекрутери на LinkedIn це приклад претекстингу.

- Жовтень 2024: Російські кіберзлочинці розсилали шкідливе ПЗ для викрадення інформації нез'ясованій кількості українських призовників, щоб підривати зусилля з рекрутингу до армії. Розсилка malware через маніпуляцію рекрутингом – це прилад baiting.
- Жовтень 2024: Російські хакери надсилали скомпрометовані електронні листи, замасковані під Amazon або Microsoft, для проникнення в українські державні та військові пристрої та викрадення облікових даних.
- Серпень 2024: Російські кіберзлочинці атакували дипломатів через схему електронних листів про продаж уживаних автомобілів. У листі був файл із зображеннями автомобіля, який насправді містив шкідливе ПЗ для створення бекдору.
- Червень 2024**:** Хакери, що спонсоруються державою Білорусі, запустили кампанію зі шпигунства проти Міністерства оборони України та однієї військової бази. Жертвам надсилали фішингові листи з дронами та шкідливою таблицею Excel.
- Травень 2024: ЗМІ повідомляли, що пакистанські кібершпигуни розповсюджували шкідливе ПЗ проти уряду Індії, аерокосмічного та оборонного секторів. Група надсилала фішингові листи, видаючи себе за індійських оборонних посадовців. (Фішинг із позуванням як офіційні особи).
- Квітень 2024: Поліція Великої Британії розслідувала серію «honey trap» атак проти британських депутатів. Атакуючі надсилали відверті повідомлення від імені себе через WhatsApp, щоб отримати компрометуючі знімки цілей.
- Березень 2024: Російські хакери атакували німецькі політичні партії за допомогою фішингу. Шкідливе ПЗ було приховане у фальшивому запрошенні на вечерю від Християнсько-демократичного союзу Німеччини, щоб встановити бекдор.

- Березень 2024: Уряд Індії та енергетичний сектор зазнали кібершпигунської атаки. Хакери надіслали шкідливий файл, замаскований під лист від Королівських ВПС Індії, до відділів електронного зв’язку, ІТ-управління та національної оборони.
- Листопад 2023: Підозрювані китайські хакери провели кампанію зі шпигунства проти Узбекистану та Республіки Корея, використовуючи фішинг для доступу до систем та дешифрування даних.
- Листопад 2023: Китайські хакери скомпрометували урядові мережі Філіппін. Починаючи з серпня 2023 року, вони використовували фішингові листи для впровадження шкідливого коду та встановлення командно-контрольної інфраструктури.
- Жовтень 2023: Нові звіти показують, що китайські хакери націлювалися на урядові агентства Гайани з лютого 2023 року через фішингові листи для викрадення конфіденційної інформації.
- Жовтень 2023: Північнокорейські хакери надсилали phishing emails із шкідливим ПЗ працівникам суднобудівного сектору Південної Кореї.
- Вересень 2023: Іранські хакери атакували залізничну мережу Ізраїлю через фішингову кампанію.
- Вересень 2023: Атака програмою-вимагачем знищила чотири місяці даних уряду Шрі-Ланки. Зловмисники почали атаку у серпні 2023 року через інфіковані посилання.
- Серпень 2023: Іранські кібершпигуни націлюються на дисидентів у Німеччині. Використовували фальшиві цифрові персони для встановлення довіри, після чого надсилали шкідливе посилання на сторінку збору облікових даних. Фальшиві цифрові персони для побудови довіри – це pretexting.
- Липень 2023: Російські кіберхакери націлювались на українські державні сервіси, такі як додаток «Дія», використовуючи фішинг і malware.

- Червень 2023: Північнокорейські хакери видавали себе за технічних працівників або роботодавців для крадіжки понад 3 млрд доларів із 2018 року.
- Травень 2023: Кібербезпекова служба Бельгії пов’язала китайських хакерів зі spearphishing атакою на відомого політика.
- Травень 2023: Фішингова кампанія націлилася на Міністерство закордонних справ Йорданії. Дослідники пов’язали атаку з іранським кібершпигунським актором.
- Квітень 2023: Північнокорейські хакери видавали себе за журналістів у фішинговій кампанії, щоб вкрасти облікові дані експертів з питань КНДР.
- Березень 2023: Північнокорейські хакери націлювалися на американські компанії з кібербезпеки.
- Березень 2023: Російські хакери проводили соціальні інженерні кампанії проти політиків, бізнесменів і знаменитостей США та Європи, які публічно засудили вторгнення Росії в Україну. Хакери переконували жертв брати участь у дзвінках або відео, надаючи оманливі підказки для отримання проросійських заяв. Приклад vishing/pretexting.
- Лютий 2023: Латвійські чиновники повідомили про фішингову кампанію російських хакерів проти Міністерства оборони.
- Лютий 2023: Китайські кібершпигуни провели spear-phishing кампанію проти урядів та публічних організацій у Азії та Європі. Листи містили чернетку листа Єврокомісії як початковий вектор атаки.
- Грудень 2022: Китайські хакери запустили фішингові атаки проти урядових, освітніх та науково-дослідних організацій у Азіатсько-Тихоокеанському регіоні.
- Грудень 2022: Хакери націлилися на українські урядові установи та державні залізниці, використовуючи фішингові листи з інформацією про ідентифікацію дронів-камікадзе та шкідливим ПЗ для шпигунства.

- Серпень 2022: Хакери використовували фішингові листи для розгортання malware в урядових установах і оборонних компаніях у Східній Європі. Звіт Kaspersky пов’язав кампанію з китайською хакерською групою.
- Липень 2022: Хакери атакували ВПС Пакистану за допомогою spearphishing для розгортання malware та отримання конфіденційних файлів.
- Червень 2022: Хакери націлилися на колишніх ізраїльських посадовців, військових та колишнього посла США в Ізраїлі. Ізраїльська кіберкомпанія заявила, що іранські актори використовували фішинг для доступу до поштових скриньок, персональних даних та документів.
- Червень 2022**:** Фішингова кампанія націлилася на американські організації в військовому, програмному, ланцюговому, медичному та фармацевтичному секторах для компрометації облікових записів Microsoft Office 365 та Outlook.
- Квітень 2022: Північнокорейська кампанія з фішинговими листами від фальшивих рекрутерів націлилася на хімічні компанії Південної Кореї.
- Квітень 2022: Соціальна медіа-платформа припинила дві кампанії іранських кібершпигунів, що націлювалися на активістів, науковців і приватні компанії. Кампанія торкнулася енергетичного, напівпровідникового та телеком-секторів у США, Ізраїлі, Росії та Канаді, використовуючи фішинг та інші методи соціальної інженерії.

Насправді аналіз хронології задокументованих кіберінцидентів 2022–2025 років, ще раз демонструє, що соціальна інженерія виступає домінантним вектором первинного проникнення. Найпоширенішим методом є фішинг, передусім його цільова форма – spearphishing. Цей підхід чітко простежується в численних кейсах: від надсилання підроблених дипломатичних документів дипломатам Казахстану у січні 2025 року до фішингових листів, замаскованих під Amazon або Microsoft, спрямованих на українських військових у грудні 2024 року. Спостерігається тенденція переходу від масових розсилок до гіперперсоналізованих кампаній,

побудованих на тематичних приманках, пов’язаних із геополітичними подіями (війна в Україні, оборонні угоди, політичні процеси).

Другим за поширеністю методом у вибірці є pretexting – створення фальшивих сценаріїв для побудови довіри. Він фіксується у значній частці інцидентів і проявляється, зокрема, через схеми фальшивого рекрутингу. Північнокорейські та іранські кіберугруповання видавали себе за рекрутерів або віддалених працівників (листопад 2024 року, квітень 2025 року), націлюючись на спеціалістів оборонної галузі, державних службовців або осіб, що нещодавно залишили державну службу. Такі сценарії дозволяли зловмисникам не лише викрадати дані, але й розгортати довгострокові інфільтраційні операції. Інші форми соціальної інженерії – дезінформаційні кампанії, honey-trap, impersonation – трапляються рідше, але демонструють розширення каналів впливу: від email до LinkedIn, WhatsApp, WeChat та Telegram.

Щодо секторів, що найчастіше стають об’єктами атак, у зібраній вибірці домінують саме ті сфери, де циркулює інформація високого рівня конфіденційності – державне управління, оборона, військові структури, дипломатичні установи та високотехнологічні компанії. Ці спостереження узгоджуються з трендами, зафіксованими у глобальних звітах. За даними IBM X-Force Threat Intelligence Index 2025 [18], виробничий сектор загалом залишається найчастішою ціллю атак четвертий рік поспіль, що обумовлено його критичною роллю у ланцюгах постачання. Однак у вибірці реальних кейсів соціальної інженерії, орієнтованих саме на об’єкти критичної інфраструктури, переважають атаки на державні органи, оборонний сектор, дипломатичні служби та high-tech галузі, що узгоджується з моделями діяльності державних APT-угруповань. Сектори енергетики, транспорту та авіації також зазнавали цілеспрямованих атак, що відображає спрямованість зловмисників на критичні системи із максимальним геополітичним впливом.

1.5 Роль людського фактору у соціальній інженерії

У роботі по темі, що стосується соціальної інженерії не можливо не загадати про роль людського фактору. Він є ключовою передумовою успішності соціально-інженерних атак. Хоча соціальна інженерія часто ототожнюється з помилками або довірливістю користувачів, насправді вона є цілеспрямованим процесом маніпуляції людською поведінкою, який використовує природні когнітивні упередження, емоційні реакції та інформаційні звички. Тому роль людського фактору у соціальній інженерії полягає не лише в слабкостях, а й у тому, що саме люди стають точкою входу, на яку зловмисники спрямовують свої психологічні та технічні інструменти.

В одній статті на тему впливу людського фактору на атаки на ОКІ [19] автори підкреслюють, що соціальні інженери часто обирають мішені серед працівників, які мають доступ до привілейованої інформації або займають керівні позиції. Ці люди зазвичай мають достатню професійну компетентність, але саме ця компетентність й робить їх особливо цінними для атак. Попри всі технічні бар'єри, шахраї значною мірою розраховують на людську поведінку – і їхні психологічні методи виявляються ефективними. Зловмисники маніпулюють емоціями жертв, використовують лестощі, вдають дружелюбність або простоту в спілкуванні – все, щоб завоювати довіру. Коли людина почувається комфортно, вона менше раціоналізує і охочіше реагує на запити, навіть якщо це суперечить її звичайним стандартам безпеки. Саме ця модель добре ілюструє, чому навіть досвідчені і освічені співробітники не застраховані від фішингу або претекстингу.

Ще однією експлуатованою слабкістю є людська наївність. Багато потенційних жертв – це також люди з обмеженим цифровим досвідом, які можуть не розуміти технічні ризики або мають мінімальні навички безпеки в інтернеті. Поєднання такої наївності, малої обізнаності та довірливості створює ідеальний ґрунт для соціально-інженерних атак.

Соціальні інженери активно користуються моментами, коли увага людей знижена або емоційний стан підвищений. Актуальні новини, природні катастрофи, інформаційні приводи, пов’язані з відомими особами, – усе це слугує зручним інструментом для створення клікбейтних посилань і вірусного поширення шкідливих повідомлень. Зламані або фальшиві акаунти у соціальних мережах та сервісах поширюють посилання, які перенаправляють користувачів на шкідливі ресурси, де відбувається викрадення даних або встановлення шкідливого ПЗ. Так формується ланцюгова реакція, коли кожна нова жертва мимоволі поширює атаку далі.

У іншій статті [20] виокремлюються шість ключових принципів, які соціальні інженери застосовують найчастіше:

1. Взаємність – базується на тому, що людина відчуває потребу «відплатити» за будь-яку надану їй послугу чи жест. Навіть дрібна люб’язність може створити відчуття обов’язку, яким зловмисник здатен маніпулювати.
2. Наслідування – працює через сприйняття поведінки інших як орієнтир: люди частіше довіряють тим, кого вважають частиною «свого кола».
3. Симпатія – працює через відчуття схожості: ми більш охоче довіряємо тим, хто здається нам близьким або приємним.
4. Дефіцит – полягає у тому, що обмеженість ресурсу або інформації підвищує його цінність і стимулює людину діяти швидше та менш обдумано (наприклад, як описано вищу у випадку з клікбейтами).
5. Зобов’язання – пов’язане з тим, що люди схильні дотримуватися обіцянок і рішень, які вони вже висловили.
6. Авторитет – є одним із найпотужніших інструментів впливу: люди природно довіряють тим, кого сприймають як керівника, експерта чи інституцію, і тому легше підкоряються вимогам. Саме тому зловмисники часто імітують фігуру авторитету. Надмірна покірність, яка може виглядати як професійна чемність, у такому контексті перетворюється на небезпечну вразливість і суттєво полегшує атаки.

Ця ситуація показує, що технічні засоби захисту, навіть найсучасніші, не завжди ефективні, якщо людина добровільно надає свої облікові дані. Дуже важливим є інтенсивне навчання й підвищення обізнаності персоналу. Без цього користувачі залишаються «людським шлюзом», через який соціальні інженери можуть проникнути навіть у найбільш захищені системи.

1.6 Актуальні підходи до протидії соціальній інженерії

Соціальна інженерія у 2025 році переживає трансформацію під впливом генеративних технологій штучного інтелекту, що суттєво змінює як масштаби, так і характер сучасних кіберзагроз. У публікації SecurityWeek «Cyber Insights 2025: Social Engineering Gets AI Wings» [21] як раз розповідається про те, як генеративний штучний інтелект дозволяє створювати атаки, що виходять далеко за межі класичного фішингу. Якщо раніше переважали електронні листи з примітивними шаблонами, то тепер зловмисники здатні поєднувати текст, аудіо та відео у комплексні мультимодальні сценарії. Використання синтетичних голосів і відео, зокрема діпфейк, відкриває можливості для створення достовірних дзвінків від нібито керівників компаній, державних структур або знайомих осіб. Такі технології, що раніше вимагали значних ресурсів, тепер стали доступними навіть для аматорів, що суттєво спрощує запуск високоякісних атак. Залучення відкритих даних із соціальних мереж та інших публічних джерел дозволяє автоматично генерувати персоналізовані повідомлення, максимально адаптовані до конкретної жертви, що робить соціальну інженерію значно точнішою та ефективнішою.

Особливе занепокоєння викликає використання подібних технологій у контексті кібершпигунства. Аналітики зазначають, що ШІ дозволяє зловмисникам імітувати співбесіди, комунікацію з рекрутерами чи представниками організацій для отримання конфіденційної інформації або вербування. У цьому випадку атаки стають не лише технічно якіснішими, але й стратегічно небезпечнішими, оскільки

зловмисники отримують можливість впливати безпосередньо на високопоставлених або спеціально відібраних осіб.

Необхідні більш активні технологічні підходи, що дозволяють не лише виявляти підозрілі повідомлення, а й запобігати ризиковим діям користувачів у момент їх виникнення. У багатьох випадках першочерговим кроком є формування стійкої обізнаності працівників через регулярне навчання та тренінги. Керівництво має усвідомлювати, що співробітники відіграють ключову роль у захисті організаційних активів, особливо коли мова йде про атаки, орієнтовані на людський фактор. Багато організацій вже давно включають соціальну інженерію до своїх програм тестування безпеки. Зовнішні аудитори зазвичай проводять як технічні перевірки – аудит конфігурацій, тестування на проникнення, пошук вразливостей – так і сценарні вправи, орієнтовані на людей. Останні можуть різнитися за складністю: від звичайних телефонних дзвінків із вигаданими легендами до складних сценаріїв із використанням ролей, підроблених документів чи навіть маскування. Для підвищення стійкості персоналу компанії проводять як фізичні, так і дистанційні перевірки, щоб оцінити, наскільки співробітники здатні розпізнати спроби маніпуляції та як вони реагують у реальних умовах [19].

Проте навіть найкращі програми навчання не гарантують повного захисту. Саме тому поряд із людським фактором необхідно впроваджувати технологічні механізми захисту, які здатні виявляти атаки на ранніх стадіях і запобігати їх реалізації. До таких механізмів належать технології перевірки електронної пошти – наприклад, використання SPF-політик, що дозволяють підтвердити легітимність відправника та зменшити ризик підробки повідомлень. Не менш важливими є антивірусні рішення та інструменти для виявлення шпигунських програм, що допомагають блокувати виконання шкідливих файлів [22].

Організації також можуть застосовувати контент-фільтри, які обмежують доступ до небажаних веб-ресурсів і виявляють фішингові повідомлення. Додатковий рівень безпеки забезпечують біометричні системи для контролю

доступу до критичних об’єктів та системи виявлення вторгнень, які дають змогу оперативно реагувати на підозрілу активність. Водночас технологічні засоби потребують регулярного оновлення, щоб залишатися ефективними в умовах еволюції кіберзагроз.

На ринку з’являється дедалі більше засобів захисту: наприклад, AppRiver може відфільтровувати значну частину фішингових листів до того, як вони потраплять у корпоративну мережу. Також варто впроваджувати багатофакторну автентифікацію та інші механізми підвищеної безпеки. Якщо шкідливий лист усе ж дістався адресата, ключову роль можуть відіграти системи захисту кінцевих точок, здатні блокувати нові зразки malware. І як останній рубіж – використання IDS/IPS рішень, що дозволяють виявляти відомі типи атак, стежити за їх поширенням у мережі та аналізувати поведінкові ознаки зловмисної активності [23].

У статті Державного департаменту США, присвяченій загрозам соціальної інженерії, особлива увага приділяється простим, але водночас ефективним способам захисту, зокрема застосуванню так званого «тесту качки» [24]. Його логіка проста: якщо певна дія або запит видається нелогічним чи підозрілим, варто поставити його під сумнів, незалежно від того, наскільки терміновим або привабливим він виглядає. Послідовне застосування здорового глузду та логічного мислення залишається одним із найважливіших інструментів, що дозволяє мінімізувати ризики та запобігати нав’язаним шахрайським діям.

Висновки до розділу 1

У першому розділі було послідовно розглянуто фундаментальні аспекти соціальної інженерії, що формують теоретичну основу подальшого дослідження цифрової форензики в середовищі критичної інфраструктури. В межах підрозділів була визначена широка класифікація технік і видів атак – від класичного фішингу

та претекстингу до складних соціотехнічних сценаріїв, що комбінують цифрові та фізичні методи впливу.

Подальший огляд продемонстрував, що критична інфраструктура є особливо вразливою до соціальної інженерії через поєднання людського фактору, високої цінності даних та специфіки OT/ICS-середовищ. Статистичні дані міжнародних організацій показали, що саме соціальна інженерія виступає домінуючим первинним вектором проникнення. Ретельний аналіз реальних інцидентів 2022–2025 років підтвердив цю тенденцію: переважна більшість успішних атак починалися зі spear-phishing, фальшивого рекрутингу, impersonation або дезінформаційних сценаріїв.

Окрему увагу було приділено людському фактору як ключовому елементу успішності соціально-інженерних атак. Розгляд психологічних принципів впливу показав, що зловмисники використовують природні когнітивні упередження та емоційні реакції для формування довіри та зниження критичності сприйняття жертви. Це підтверджує, що технічні механізми захисту не є достатніми без врахування поведінкових особливостей персоналу.

Аналіз міжнародних стандартів та статей дозволив зробити висновок, що ефективний захист про атак соціальної інженерії потребує комплексного підходу: поєднання технологічних рішень (MFA, фільтрування пошти, IDS/IPS, аналіз поведінки) та системної роботи з персоналом (тренінги, симуляції фішингу, підвищення культури безпеки).

2 ОСОБЛИВОСТІ ЦИФРОВОЇ ФОРЕНЗИКИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ НА ОКІ ТА СИСТЕМАТИЗАЦІЯ ФОРЕНЗИНЧИХ ІНДИКАТОРІВ

2.1 Процес цифрового слідства та ключові виклики у середовищі критичної інфраструктури

Цифрова форензика є спеціалізованою сферою кібербезпеки та судової експертизи, що спрямована на виявлення, збирання, збереження, аналіз та представлення цифрових доказів таким чином, щоб забезпечити їх достовірність і юридичну прийнятність. У цьому підрозділі доречно буде розглядати усі особливості цифрового слідства спираючись на зміст міжнародно прийнятих стандартів.

Згідно з NIST SP 800-86 «Guide to Integrating Forensic Techniques into Incident Response» (2006) [25], цифрова форензика розглядається як систематичне застосування наукових методів для обробки цифрових даних у рамках реагування на інциденти. У стандарті ISO/IEC 27037:2012 «Guidelines for identification, collection, acquisition and preservation of digital evidence» [26] детально визначено процеси, необхідні для формування довірених цифрових доказів. Він описує чотири ключові процеси:

1. Identification. На цьому етапі встановлюється, які об’єкти, пристрої або дані можуть містити цифрові докази, а також чи є вони релевантними для розслідування.
2. Collection. Процес збору передбачає фізичне отримання носіїв або їх копій, які містять потенційні докази. Стандарт підкреслює: мінімізацію втручання у вихідне середовище; документування того, які дії були виконані, хто їх виконував, яким інструментом; отримання доступу лише уповноваженими особами; запобігання зміні або пошкодженню даних у процесі збору.

3. Acquisition. Цей процес спрямований на створення точної, біт-у-біт копії цифрових даних. Стандарт визначає такі положення: використовувати методи, які гарантують форензичну точність копії; застосування write-blockers (апаратних або програмних) для запобігання модифікації оригіналу; фіксація контрольних сум, що підтверджують цілісність копії.
4. Preservation**.** Збереження має забезпечувати, щоб цифрові докази: залишались неушкодженими і незмінними; зберігалися у середовищі з контрольованим доступом; супроводжувалися документацією, що підтверджує їх цілісність; були доступні для подальшого аналізу або повторної експертизи.

Також стандарт наголошує на критичній важливості підтримання ланцюга зберігання доказів (chain of custody) – це документально підтверджений шлях, який фіксує всі дії з доказами від моменту їх виявлення до передачі компетентним органам або суду.

У контексті об’єктів критичної інфраструктури особливе значення мають стандарти та рекомендації, що стосуються оперативних технологій (OT). Документ NISTIR 8428 «Digital Forensics and Incident Response (DFIR) Framework for Operational Technology» (2022) [27] підкреслює, що цифрова форензика в OT-середовищах значно відрізняється від традиційної IT-форензики. Зокрема, у ньому зазначається, що процес збору доказів у системах SCADA, PLC та промислових мережах повинен враховувати:

- неможливість зупинки або переривання технологічних процесів, оскільки це може призвести до аварій або економічних збитків;
- наявність пропрієтарних протоколів, нестандартних операційних систем та обмеженого журналювання;
- підвищені вимоги до безпеки та безперервності операцій, що обмежує використання традиційних методів форензики (наприклад, вилучення дисків або пам’яті).

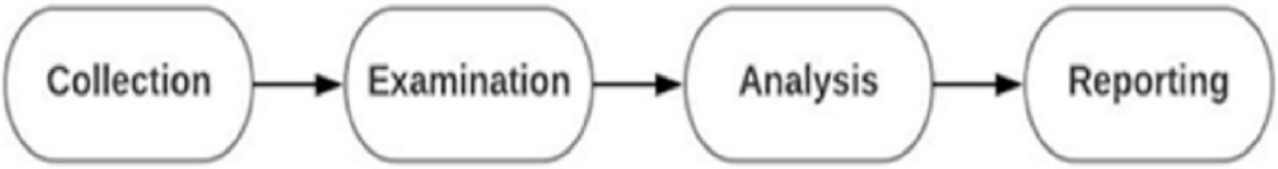

Рисунок 2.1 – Схема процесу цифрової форензики за NIST [28]

Якщо говорити про цифрове розслідування інцидентів соціальної інженерії то весь процес набуває значних складнощів, хоча і не відрізняється особливо за основними етапами. Особлива складність розслідування таких атак полягає в тому, що соціальна інженерія практично не залишає матеріальних слідів, а отже – і традиційні криміналістичні методи виявляються малоефективними. Порушники часто приховують свою присутність: використовують підроблені чи анонімні особистості, сервіси для маскування геолокації, тимчасові акаунти або інструменти для стирання цифрових артефактів. У результаті слідство нерідко заходить у глухий кут, адже відсутні прямі докази, які могли б однозначно вказати на виконавця.

Отже, як було зазначено вище основний процес розслідування соціальної інженерії включає ті самі етапи загальноприйнятих стандартів, лише з деякими уточненнями. Так, наприклад, автор статті [29] описує його наступними кроками:

1. Збір цифрових доказів. Серед основних підходів:
    - Форензичне клонування (Forensic Imaging) – створення повної копії жорсткого диска або іншого носія для збереження цілісності даних;
    - Вилучення даних (Data Extraction) – отримання конкретної інформації, наприклад, електронних листів, текстових повідомлень, історії браузера;
    - Зняття даних із пам’яті (Memory Retrieval) – фіксація поточного вмісту оперативної пам’яті пристрою, де може зберігатися інформація про дії зловмисника;

- Збір даних з мережі – включає аналіз логів мережевої активності та моніторинг трафіку для виявлення підозрілих операцій, таких як незвичні передачі даних.

2. Аналіз цифрових доказів. Після збору даних слідчі проводять їх детальний аналіз, щоб виявити інформацію, що допоможе встановити особу злочинця. Основні методи включають:

    - Аналіз метаданих – дослідження атрибутів файлів, таких як дата та час створення, для визначення походження файлу та осіб, які мали до нього доступ;
    - Реконструкція подій (Event Reconstruction) – відтворення послідовності дій під час інциденту для ідентифікації зловмисника та розуміння методів здійснення атаки;
    - Виявлення ключової інформації – пошук імен жертв, фінансових даних або ключових слів, пов’язаних із застосованими методами соціальної інженерії.

3. Відновлення цифрових доказів. У деяких випадках зловмисники намагаються видалити сліди своєї діяльності. Для цього слідчі використовують спеціальні технології:

    - Відновлення видалених файлів – застосування програмного забезпечення для відновлення даних із жорстких дисків та інших накопичувачів;
    - Стеганографічний аналіз – виявлення прихованих повідомлень, закладених у зображеннях або аудіофайлах.

4. Збереження цифрових доказів. Тут все так само як і за рекомендаціями описаними вище у розділі. Вкрай важливо забезпечити належне зберігання доказів для підтримання їхньої цілісності та запобігання пошкодженню або втраті.

Наприклад, у випадку фішингової атаки, коли зловмисник надсилає підроблений лист, цифрові форензичні методи дозволяють законно встановити особу порушника. Для цього слідчі можуть:

- аналізувати заголовки електронних листів для визначення IP-адреси відправника;
- трасувати IP-адресу до конкретного географічного розташування;
- якщо пристрій злочинця доступний, створювати його образ для подальшого аналізу файлів та мережевої активності;
- поєднувати дані з листів, логів активності та метаданих, щоб скласти повну картину дій зловмисника.

Труднощі розслідування ускладнюються постійною еволюцією схем соціальної інженерії. Окремий виклик становлять етичні та правові ризики, пов’язані з цифровою форензикою. На відміну від суто технічних кібератак, соціальна інженерія спрямована передусім на людину, тому цифрові артефакти часто зберігаються у середовищах, що містять значний обсяг приватної інформації користувача – особисте листування, історію пошуку, медіафайли, контакти тощо. Під час вилучення та аналізу доказів слідчі неминуче стикаються з даними, які не мають прямого стосунку до інциденту, що може порушити приватність та принципи мінімізації й пропорційності, передбачені міжнародними стандартами та законодавством. Тому слідчі повинні забезпечувати суворий контроль доступу й документування всіх дій, щоб гарантувати законність обробки інформації та допустимість доказів.

Додаткову складність у розслідуванні становлять докази, що пов’язані з мережевою інфраструктурою. Мережеві дані є надзвичайно фрагментованими та розподіленими між різними елементами інфраструктури, серед яких маршрутизатори, комутатори, точки доступу Wi-Fi, міжмережеві екрани, VPN-сервери та централізовані лог-системи. Така множинність джерел ускладнює визначення того, які саме записи є релевантними для конкретного інциденту.

Навіть за умови, що місце зберігання необхідної інформації встановлене, доступ до нього може бути обмежений технічними, територіальними або юридичними факторами, зокрема залежністю від зовнішніх провайдерів чи міжнародних хмарних сервісів. Серйозною проблемою є тимчасовий характер зберігання мережевих логів: через обмежену ємність пам’яті пристрої часто використовують циклічні журнали, які швидко перезаписуються. Це створює високий ризик втрати важливих артефактів ще до моменту початку розслідування.

2.2 Аналіз ключових індикатори різних сценарії атак соціальної інженерії

У процесі дослідження впливу соціально-інженерних атак на системи критичної інформаційної інфраструктури виникла необхідність розробити інструмент, який дозволив би комплексно оцінювати як самі сценарії атак, так і цифрові сліди, що виникають у результаті їх реалізації. На відміну від суто технічних атак, соціальна інженерія використовує людський фактор як основну точку входу, однак її наслідки майже завжди відображаються у поведінці інформаційних систем. Тому для ефективного реагування на інциденти та побудови методики оцінювання ризиків пропуску подібних атак (яку буде запропоновано як результат даної роботи) важливо мати систематизований опис того, які саме форензичні артефакти можуть залишатися у відповідних сегментах IT- та OT-інфраструктури.

З цієї причини було вирішено створити чекліст сценаріїв соціальної інженерії за допомогою MITRE ATT&CK [30], орієнтований на контекст SCADA-систем та інших компонентів критичної інфраструктури. Його розробка стала ключовою передумовою розроблення методики оцінювання ризиків, оскільки чекліст дає можливість сформувати уявлення про потенційні джерела доказів, у якій частині системи вони виникають, які активи є найбільш вразливими, а на яких залишаються найбільш інформативні журнали подій. Фактично, він виконує роль зв’язувальної

ланки між поведінковими ознаками атаки та технічними параметрами форензичного аналізу

Створена таблиця-чекліст містить опис дев’ятнадцяти найбільш поширених сценаріїв соціальної інженерії, що можуть бути застосовані у контексті промислових систем управління. Для кожного сценарію наведено коротку характеристику типових ознак атаки, які користувач або оператор може спостерігати у процесі роботи. Це дозволяє зрозуміти контекст, у якому зловмисник взаємодіє з жертвою, та оцінити, яким чином відбувається початкове втручання.

Однією з найважливіших частин чекліста є визначення форензичних даних, що утворюються під час реалізації кожного конкретного сценарію. Вказано, які саме журнали, транзакції, дані аутентифікації, мережеві записи або локальні сліди в системі можуть зберігатися після атаки. Наприклад, фішингові атаки здебільшого призводять до появи записів в email-серверах, логів веб-запитів чи журналів виконання файлів на робочих станціях. А ось атаки, що передбачають фізичну взаємодію (наприклад, tailgating або shoulder surfing), залишають інший тип слідів – журнали контролю доступу, записи відеоспостереження, а також подальші аномальні входи до операційних систем.

Для кожного сценарію також вказано, на яких саме пристроях можуть бути зафіксовані найцінніші для форензичного розслідування артефакти. Такий підхід важливий у контексті промислових систем, де OT-компоненти (HMI, інженерні робочі станції, PLC/RTU, MTU) зазвичай не мають розширеного журналювання, тоді як IT-компоненти (Domain Controller, Email Server, Web Server) надають значно більше можливостей для постфактум-аналізу. Саме тому систематизація джерел даних дозволяє точно визначити, де саме SOC або DFIR-фахівці повинні шукати підтвердження компрометації, і які сегменти інфраструктури є менш покритими у плані обліку подій.

Нижче представлено лише частину цього чекліста, адже сам по собі він вийшов занадто великий. Повну версію було завантажено у відкритий доступ на GitHub [31].

Таблиця 2.1 – Індикатори різних сценаріїв атак соціальної інженерії та пристрої їх фіксації

Сценарій атаки	Як індетифікувати	Форензичні дані	Пристрій фіксації	Оцінка впливу
Phishing через email або website	Отримання несподіваних електронних листів або відвідування веб-сайтів, які імітують офіційні ресурси критичної інфраструктури; ознаки включають граматичні помилки, невідому адресу відправника, терміновість дій або вимогу надати паролі/конфіденційну інформацію про системи	Підозрілі email-транзакції з метаданими (IP-адреси відправника, час відправки/отримання, вкладення чи посилання), журнали сервера з записами про прийом/відправку, а також журнали браузера з історією відвідувань фальшивих URL	Email Server (журнали SMTP/IMAP, заголовки листів, IP); Web Server / Proxy / Firewall (HTTP(S) трафік, переходи за шкідливими лінками), корпоративний сервер, робочі станції	Компрометація облікових даних може призвести до несанкціонованого доступу до SCADA-систем, зміни параметрів керування (наприклад, в IED або PLC), що потенційно спричинить аварії або перерви в роботі

Продовження таблиці 2.1

Сценарій атаки	Як індетифікувати	Форензичні дані	Пристрій фіксації	Оцінка впливу
Vishing (голосовий фішинг)	Телефонні дзвінки від осіб, які представляються як технічна підтримка або керівництво ОКІ; ознаки включають несподівані дзвінки поза робочим часом, тиск на швидкі дії, запит конфіденційної інформації як паролі чи конфігураційні деталі	Не фіксується безпосередньо в цифровому форматі; опосередковано через подальші наслідки, як незвичайні логи входу або зміни конфігурації. Альтернативно: зафіксувати через записи телефонних розмов (якщо система VoIP), свідчення операторів або аудит журналів подій	Domain Controller (логіни після дзвінка, аномальна активність), VoIP/Call Server (якщо є; аудіо/дзвінки)	Отримання доступу може дозволити зловмиснику маніпулювати HMI або PLC, спричиняючи неправильне керування обладнанням, як відключення систем захисту в електромережах
Smishing (SMS-фішинг)	SMS-повідомлення з терміновими вимогами; ознаки: невідомий номер, фальшиві посилання, вимога ввести дані або завантажити «оновлення», часто з елементами паніки	Журнали SMS-транзакцій на мобільних пристроях (якщо інтегровані з системою), або подальші браузерні дії	Робочі станції (для фіксації браузерної історії) або Email Server (якщо SMS перенаправляєтьс я), корпоративний сервер	Клік на шкідливе посилання може встановити ШПЗ, що порушить комунікацію між MTU та польовими пристроями, призводячи до втрати контролю над критичними процесами

Продовження таблиці 2.1

Сценарій атаки	Як індетифікувати	Форензичні дані	Пристрій фіксації	Оцінка впливу
Angler Phishing (фішинг через соціальні мережі)	Повідомлення в соціальних мережах від "колег" або "постачальників" з посиланнями; ознаки: профілі без історії, невідповідність стилю спілкування, терміновість	Історія браузера з доступом до зовнішніх посилань, журнали подій з виконанням файлів, Communication logs з аномальними взаємодіями	Робочі станції (для браузерної історії), Web Server (для запитів), корпоративний сервер	Встановлення шкідливого ПЗ може скомпрометувати Engineering Workstation, дозволяючи маніпуляцію кодом програм в PLC, що загрожує стабільності інфраструктури
Grooming	Тривалі комунікації з поступовими проханнями про дедалі конфіденційніш у інформацію (наприклад, спочатку загальні запитання про SCADA, потім про паролі); ознаки: регулярні контакти без видимої мети, ескалація запитів, використання соціальних мереж чи email	Журнали комунікації з повторюваними взаємодіями, email-транзакції з метаданими, журнали подій з поступовими змінами доступу	Email Server(довгі ланцюжки листування), OPC Server / SCADA logs(якщо зловмисник отримав доступ до оператора)	Витік даних про конфігурацію може призвести до цільових атак на MTU, порушуючи моніторинг і керування критичними процесами

Кінець таблиці 2.1

Сценарій атаки	Як індетифікувати	Форензичні дані	Пристрій фіксації	Оцінка впливу
Pretexting (створення фальшивого сценарію)	Запити інформації під вигаданим, але правдоподібним приводом; ознаки: відсутність верифікації, нестандартні канали зв'язку, тиск на конфіденційність	Журнали подій з незвичайними запитами, зміни конфігурації, Issued commands з нетиповими діями	HMI (для команд) або Domain Controller (спроби входу під виглядом “аудиторів/провайдерів”)	Надання доступу може дозволити зміну налаштувань IED, спричиняючи аномалії в мережі, як перевантаження чи відключення
Profile Cloning	Повідомлення від профілів, що імітують реальних колег чи партнерів; ознаки: дублікат профілів, відмінності в деталях, незвичайні запити	Журнали аутентифікації з дубльованими обліковими записами, незвичайні входи в Logon Events, email-транзакції з фальшивими адресами	Domain Controller (логіни з клонованими обліковками) або Email Server (IMAP/SMTP-авторизація)	Імперсонація може призвести до виконання шкідливих команд на HMI, порушуючи технологічний процес і викликаючи збої

Таким чином, таблиця-чекліст виконує не лише описову, але й аналітичну функцію: вона допомагає інженерам та аналітикам безпеки оцінити вразливість системи з урахуванням людського фактора та скласти повнішу картину того, як саме соціальна інженерія трансформується у технічні наслідки для SCADA-середовища.

Далі на основі розробленого чекліста було побудовано матрицю відповідності між сценаріями соціальної інженерії та окремими активами IT- і OT-інфраструктури. Матриця містить інформацію про те, чи є певний актив потенційним місцем фіксації форензичних артефактів у разі реалізації конкретної атаки. Для цього використовувалося умовне позначення «+», яке означає, що пристрій може містити важливі журнали подій або цифрові дані, пов'язані з атакою.

Нижче також представлена не повна версія матриці:

Сценарій атаки	PLC/RTU	IED	HMI	Engineering Workstation	Комутатори	Historian	OPC Server	Сервери застосунків	MTU	Маршрутизатори	Domain Controll
Фішинг (Email/Website)											
Vishing											+
Smishing											
Spear-phishing / Whaling											+
Angler Phishing											
Grooming							+				
Pretexting			+								+
Profile Cloning											+
Face-to-Face Interaction			+								
Shoulder Surfing			+								+
Quid Pro Quo				+							+
Dumpster Diving						+					
Piggybacking / Tailgating											+
File Masquerade				+			+				
Baiting				+							
Reverse Social Engineering				+							
Scareware / Pop-up атаки											
Water-Holing										+	
Pharming								+		+	

Рисунок 2.2 – Матриця відповідності між активами та сценаріями [31]

На практиці така матриця дозволяє оцінити, наскільки рівномірно покриваються системи інфраструктури журналюванням, а також показує дисбаланс між IT- та OT-компонентами. Зокрема, робочі станції, доменні контролери, email-сервери та веб-сервери значно частіше фігурують як джерела важливих артефактів, що є логічним, оскільки соціальна інженерія у переважній більшості випадків спрямована саме на взаємодію з користувачами та середовищем аутентифікації. У той же час низка критичних OT-компонентів, таких як PLC/RTU, IED чи MTU, практично не містять форензичних слідів безпосередньо, однак саме вони можуть стати об'єктом маніпуляції внаслідок успішної атаки.

Матриця є важливим інструментом подальшого ризик-орієнтованого аналізу, оскільки дозволяє виявити активи, що беруть участь у найбільшій кількості

сценаріїв інцидентів, а також допомагає визначити сегменти інфраструктури, де необхідно підсилити моніторинг або розширити можливості журналювання.

Для узагальнення інформації матриці було здійснено автоматичний підрахунок кількості позначок «+» у кожному стовпці, після чого результати подані у вигляді графіка. Така візуалізація дозволяє порівняти активи між собою та визначити їхню відносну важливість як джерел форензичних даних у контексті соціальної інженерії:

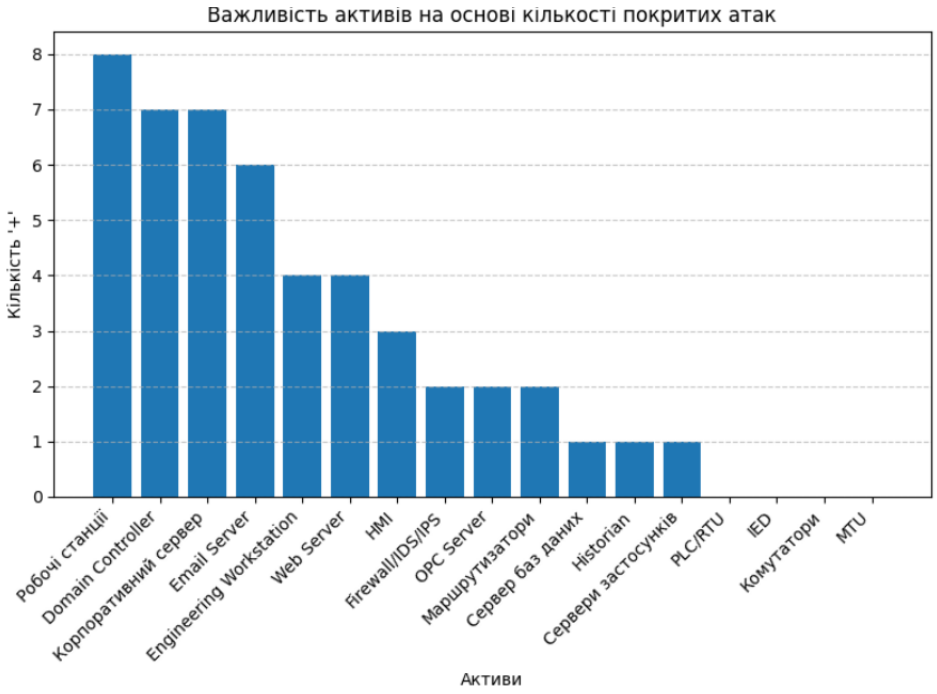

Рисунок 2.3 – Графік важливості активів

Згідно з отриманими результатами, найбільшу кількість позначок «+» отримали робочі станції, що є очікуваним, оскільки саме вони виступають первинною точкою взаємодії користувачів з фішинговими повідомленнями, підозрілими файлами або шкідливими веб-ресурсами. Високий показник також продемонстрували Domain Controller, корпоративний сервер і email-сервер, які відповідають за автентифікацію, обробку листування та виконують функції центральних вузлів взаємодії у корпоративному середовищі. Це підтверджує, що саме ці активи містять найбільше форензичної інформації під час більшості атак соціальної інженерії.

Дещо меншу, але все ще значну кількість випадків фіксації артефактів демонструють інженерні робочі станції та веб-сервери, які можуть брати участь у компрометації на більш пізніх етапах атаки або містити сліди взаємодії зі шкідливими компонентами. Далі розташовуються HMI, а також засоби мережевої безпеки – Firewall/IDS/IPS, які можуть фіксувати аномальні запити, несанкціоновані підключення або підозрілу мережеву активність.

Активи на кшталт OPC Server, маршрутизаторів, серверів баз даних, історіанів та серверів застосунків отримали меншу кількість позначок, що також є закономірним – вони зазвичай не інтегруються безпосередньо у початковий етап соціальної інженерії, однак можуть зберігати вторинні сліди, якщо атака просунулась у глиб інфраструктури.

Найнижчі значення у графіку отримали PLC/RTU, IED, комутатори та MTU. Це підтверджує обмеженість журналювання у більшості OT-компонентів, а також той факт, що соціальна інженерія рідко впливає на них безпосередньо: вони стають ціллю переважно після компрометації IT-середовища.

Таким чином, графік демонструє чіткий дисбаланс між IT- та OT-активами: основні форензичні дані зосереджені у сегменті корпоративних систем, тоді як операційні компоненти SCADA залишаються менш інформативними. Це наочно підкреслює необхідність посилення журналювання та моніторингу у OT-середовищі, щоб забезпечити повніше виявлення та розслідування інцидентів, пов’язаних із соціальною інженерією.

Висновки до розділу 2

У другому розділі було проведено комплексний аналіз особливостей цифрової форензики інцидентів соціальної інженерії в середовищі критичної інфраструктури. Розглянута інформація дозволила сформувати цілісне розуміння того, яким чином відбувається виявлення, збір, фіксація та збереження цифрових

доказів, а також які специфічні труднощі виникають у процесі розслідування подібних інцидентів у поєднанні IT- та OT-секторів. Було встановлено, що традиційна структура цифрового слідства зберігає свою загальну логіку, проте її практична реалізація в промислових середовищах має суттєві відмінності.

Аналіз сценаріїв атак соціальної інженерії показав, що попри людське походження цих інцидентів, їх наслідки систематично відображаються у цифровому просторі – у журналах аутентифікації, мережевих записах, даних електронної пошти, історії браузерів та операційних показниках IT- і OT-пристроїв. Розроблений чекліст дозволив структурувати найпоширеніші сценарії атак і показати, які саме джерела форензичних даних залишаються після їх реалізації. Побудована на його основі матриця відповідності дала змогу порівняти інформативність різних активів і виявити суттєву нерівномірність журналювання між IT- та OT-секторами. Отримані результати продемонстрували, що найбільший обсяг корисних форензичних артефактів зосереджений в IT-компонентах – робочих станціях, доменних контролерах, поштових та веб-серверах.

3 МЕТОДИКА КВАЛІМЕТРИЧНОГО ОЦІНЮВАННЯ РИЗИКУ ПРОПУСКУ ІНЦИДЕНТІВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ НА ОКІ

3.1 Опис алгоритму оцінювання ризику пропуску інцидентів соціальної інженерії

У зв’язку з тим, що значна частина атак на SCADA-системи реалізується через соціальну інженерію та залишається непоміченою традиційними технічними засобами моніторингу, виникає необхідність у створенні методики, яка дозволила б формалізовано оцінювати рівень ризику саме пропуску таких інцидентів. Практика аналізу інцидентів в об’єктах критичної інфраструктури показує, що відсутність або недостатність логів, неповноцінний моніторинг, низька підготовка персоналу та брак процедурної взаємодії призводять до того, що навіть очевидні ознаки атак не фіксуються або не інтерпретуються системою. Враховуючи це, виникає потреба у побудові структурованого підходу, який би поєднував принципи цифрової форензики з методами кількісного ризик-менеджменту та дозволяв би оцінити слабкі місця виявлення атак у комплексі – технічному, організаційному та людському. Саме на цьому підґрунті з’явилася ідея розробити методику оцінювання ризику пропуску соціальних атак у SCADA-середовищі.

Теоретичною основою методики стала модель FAIR (Factor Analysis of Information Risk), яка є міжнародним стандартом кількісного аналізу ризиків і дозволяє формалізувати ризик через математичні співвідношення між частотою інцидентів, їх масштабом та вразливістю системи. FAIR визначає ризик як очікувану величину втрат, яку наведено у базовій формулі:

$$\text{Risk} = \text{LEF} \times \text{PLM}, \tag{3.1}$$

де LEF – Loss Event Frequency, а PLM – Probable Loss Magnitude

При цьому частота інцидентів (LEF) є добутком частоти подій загрози (Threat Event Frequency, TEF) та фактору вразливості (Vulnerability Factor, VF):

$$\mathrm{LEF} = \mathrm{TEF} \times \mathrm{VF} \quad (3.2)$$

Ключовим елементом, що визначає ймовірність успішної атаки, є саме VF. У FAIR він формується через співвідношення можливостей атакувальника (Threat Capability, TC) та сили захисту (Control Strength, CS). VF описується як ймовірність того, що TC перевищить CS:

$$\mathrm{VF} = \mathrm{P}(\mathrm{TC} > \mathrm{CS}) \quad (3.3)$$

Для спрощених практичних оцінок FAIR також допускає використання апроксимацій, наприклад:

$$\mathrm{VF} \approx 1 - \frac{\mathrm{CS}}{\mathrm{TC}} \quad (3.4)$$

Таким чином, збільшення CS знижує VF, тобто зменшує ймовірність успіху атаки.

У класичній моделі FAIR показник Control Strength (CS) розглядається як інтегральна характеристика сукупності технічних, організаційних та людських контрольних заходів, а не виключно технічних механізмів захисту. Саме цей компонент є концептуальним зв’язком між моделлю FAIR та запропонованою методикою, оскільки дозволяє формалізувати рівень здатності системи протидіяти або виявляти небажані події. На відміну від повної FAIR-моделі, у якій Vulnerability Factor (VF) визначається як функція Threat Capability (TC) та Control Strength (CS), у межах даного дослідження зосереджено увагу виключно на оцінюванні Control Strength. Такий вибір обумовлений специфікою соціальної інженерії у SCADA-середовищах, де реальна здатність зловмисника (TC) є надзвичайно варіативною, контекстно залежною та практично не піддається надійному кількісному вимірюванню.

У роботі пропонується описувати Control Strength через сукупність доступних форензичних можливостей та контрольних заходів:

$$CS = g(I, A, C) \quad (3.5)$$

де I – набір форензичних індикаторів; A – активи/пристрої фіксації; C – контрольні заходи.

Для кількісної інтерпретації Control Strength у контексті виявлення соціально-інженерних атак вводиться показник Detection Probability (DP), який залежить від оціненого рівня CS та конкретного сценарію атаки S:

$$DP = f(CS, S) \quad (3.6)$$

Оскільки об’єктом дослідження є саме ризик пропуску інцидентів, далі розглядається комплементарний показник:

$$P_{nd} = 1 - DP \ , \quad (3.7)$$

який характеризує ймовірнісну складову ризику пропуску інциденту, тобто дефіцит ефективності контрольних заходів у частині виявлення.

На відміну від показника VF у моделі FAIR, P_{nd} не розглядається як повноцінна оцінка ризику. Натомість у запропонованій методиці він використовується як базова кількісна складова для формування якісного показника ризику пропуску, що ґрунтується на величині дефіциту контрольних заходів. Такий підхід дозволяє ранжувати сценарії соціальної інженерії за критичністю з точки зору їх потенційного пропуску, не претендуючи на статистичну точність повноцінних ризик-орієнтованих моделей.

Для методики було відібрано п’ять типових сценаріїв атак соціальної інженерії, які у сукупності покривають близько 70% інцидентів такого типу на SCADA-інфраструктуру:

- фішинг
- spear-phishing/whaling

- baiting
- watering holing
- pretexting

Для кожного сценарію і буде формуватися незалежна оцінка DP і P_{nd}, що дозволяє точно визначати, проти яких типів атак система є найбільш уразливою.

Для оцінювання стану контрольних заходів заздалегідь формується набір із 25 питань, що охоплюють усі аспекти безпеки: технічні (логування, моніторинг, аналіз трафіку), організаційні (політики, інструкції, регулярність аудиту), людські (навчання персоналу), а також фізичні (контроль доступу, відеоспостереження). На відміну від традиційних чек-листів, питання орієнтовані саме на визначення спроможності системи виявити атаку, а не запобігти їй. Відповіді оцінюються за шкалою 1–5, що дозволяє кількісно нормалізувати оцінку контрольного середовища.

Ключовим елементом запропонованої методики є матриця релевантності W, яка відображає відносну важливість кожного питання Q_i для виявлення конкретного сценарію соціальної інженерії S. Формування матриці W здійснюється заздалегідь на основі методу попарних порівнянь, що дозволяє формалізувати експертну оцінку релевантності контрольних та форензичних індикаторів у контексті кожного сценарію атаки.

Для визначення ваг використовується шкала попарних порівнянь Сааті, яка застосовується для експертного оцінювання важливості критеріїв якості системи захисту інформації. Згідно з цією шкалою, значення 1 відповідає рівній важливості двох критеріїв, 3 – помірній перевазі одного критерію над іншим, 5 – суттєвій перевазі, 7 – значній перевазі, а 9 – дуже сильній перевазі. Допускається використання проміжних значень або співвідношень виду «в N разів важливіше» для точнішого відображення експертної думки. У процесі оцінювання критерії

порівнюються попарно, а результати таких порівнянь заносяться до матриці у вигляді простих дробів.

Після формування матриці попарних порівнянь прості дроби переводяться у десяткові значення, обчислюються суми елементів по кожному рядку, після чого виконується нормалізація отриманих сум. У результаті такого перетворення отримуються вагові коефіцієнти $W_{i,S}$:

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18
Q1	1	1	0,111	1	1	0,333	0,111	1	1	1	0,333	0,333	1	1	1	1	0,111	0,333
Q2	1	1	0,111	1	1	0,333	0,111	1	1	1	0,333	0,333	1	1	1	1	0,111	0,333
Q3	9	9	1	9	9	5	1	9	9	9	5	5	9	9	9	9	1	3
Q4	1	1	0,111	1	1	0,333	0,111	1	1	1	0,333	0,333	1	1	1	1	0,111	0,333
Q5	1	1	0,111	1	1	0,333	0,111	1	1	1	0,333	0,333	1	1	1	1	0,111	0,333
Q6	3	3	0,2	3	3	1	0,2	3	3	3	1	1	3	3	3	3	0,2	0,5
Q7	9	9	1	9	9	5	1	9	9	9	5	5	9	9	9	9	1	3
Q8	1	1	0,111	1	1	0,333	0,111	1	1	1	0,333	0,333	1	1	1	1	0,111	0,333
Q9	1	1	0,111	1	1	0,333	0,111	1	1	1	0,333	0,333	1	1	1	1	0,111	0,333
Q10	1	1	0,111	1	1	0,333	0,111	1	1	1	0,333	0,333	1	1	1	1	0,111	0,333
Q11	3	3	0,2	3	3	1	0,2	3	3	3	1	1	3	3	3	3	0,2	0,5
Q12	3	3	0,2	3	3	1	0,2	3	3	3	1	1	3	3	3	3	0,2	0,5
Q13	1	1	0,111	1	1	0,333	0,111	1	1	1	0,333	0,333	1	1	1	1	0,111	0,333
Q14	1	1	0,111	1	1	0,333	0,111	1	1	1	0,333	0,333	1	1	1	1	0,111	0,333
Q15	1	1	0,111	1	1	0,333	0,111	1	1	1	0,333	0,333	1	1	1	1	0,111	0,333
Q16	1	1	0,111	1	1	0,333	0,111	1	1	1	0,333	0,333	1	1	1	1	0,111	0,333
Q17	9	9	1	9	9	5	1	9	9	9	5	5	9	9	9	9	1	3
Q18	3	3	0,333	3	3	2	0,333	3	3	3	2	2	3	3	3	3	0,333	1
Q19	1	1	0,111	1	1	0,333	0,111	1	1	1	0,333	0,333	1	1	1	1	0,111	0,333
Q20	1	1	0,111	1	1	0,333	0,111	1	1	1	0,333	0,333	1	1	1	1	0,111	0,333
Q21	1	1	0,111	1	1	0,333	0,111	1	1	1	0,333	0,333	1	1	1	1	0,111	0,333
Q22	9	9	1	9	9	5	1	9	9	9	5	5	9	9	9	9	1	3
Q23	1	1	0,111	1	1	0,333	0,111	1	1	1	0,333	0,333	1	1	1	1	0,111	0,333
Q24	1	1	0,111	1	1	0,333	0,111	1	1	1	0,333	0,333	1	1	1	1	0,111	0,333
Q25	3	3	0,333	3	3	2	0,333	3	3	3	2	2	3	3	3	3	0,333	1

Рисунок 3.1 – Демонстрація методу попарних порівнянь на прикладі сценарію фішинг (неповна версія)[31]

Q19	Q20	Q21	Q22	Q23	Q24	Q25	Сума по рядку	Вага
1	1	1	0,111	1	1	0,333	18,109	0,0146181
1	1	1	0,111	1	1	0,333	18,109	0,0146181
9	9	9	1	9	9	3	169	0,1364215
1	1	1	0,111	1	1	0,333	18,109	0,0146181
1	1	1	0,111	1	1	0,333	18,109	0,0146181
3	3	3	0,2	3	3	0,5	52,8	0,0426216
9	9	9	1	9	9	3	169	0,1364215
1	1	1	0,111	1	1	0,333	18,109	0,0146181
1	1	1	0,111	1	1	0,333	18,109	0,0146181
1	1	1	0,111	1	1	0,333	18,109	0,0146181
3	3	3	0,2	3	3	0,5	52,8	0,0426216
3	3	3	0,2	3	3	0,5	52,8	0,0426216
1	1	1	0,111	1	1	0,333	18,109	0,0146181
1	1	1	0,111	1	1	0,333	18,109	0,0146181
1	1	1	0,111	1	1	0,333	18,109	0,0146181
1	1	1	0,111	1	1	0,333	18,109	0,0146181
9	9	9	1	9	9	3	169	0,1364215
3	3	3	0,333	3	3	1	57,332	0,04628
1	1	1	0,111	1	1	0,333	18,109	0,0146181
1	1	1	0,111	1	1	0,333	18,109	0,0146181
1	1	1	0,111	1	1	0,333	18,109	0,0146181
9	9	9	1	9	9	3	169	0,1364215
1	1	1	0,111	1	1	0,333	18,109	0,0146181
1	1	1	0,111	1	1	0,333	18,109	0,0146181
3	3	3	0,333	3	3	1	57,332	0,04628
							1238,808	1

Рисунок 3.2 – Демонстрація кінцевого результату виконання методу попарних порівнянь [31]

Сам алгоритм реалізації методики складається з таких кроків:

1. Збір вхідних даних: Експерт проходить опитування, що складається з 25 питань, кожне з яких оцінюється за п’ятибальною шкалою відповідно до рівня реалізації контрольних заходів та наявності форензичних індикаторів. Отримані значення позначаються як $\mathrm{Score}(\mathrm{Q_i})$.
2. Нормалізація експертних оцінок: Для уніфікації шкали оцінювання всі значення переводяться у нормалізований вигляд:

$$\mathrm{Norm\_score_i} = \frac{\mathrm{Score(Q_i)}}{5} \qquad (3.8)$$

що забезпечує приведення показників до діапазону [0;1].

3. Обчислення показника Detection Probability: Нормалізовані оцінки множаться на відповідні вагові коефіцієнти з матриці W, отриманої методом попарних порівнянь ($W_{i,S}$, де i – номер питання, S – сценарій). Після цього виконується агрегування значень для всіх питань:

$$\mathrm{DP_S} = \sum_{\mathrm{i=1}}^{25} \mathrm{Norm\_score_i} \times \mathrm{W_{i,S}} \qquad (3.9)$$

4. Формування ймовірнісної складової ризику пропуску (P_{nd}):

$$\mathrm{Pnd_S} = 1 - \mathrm{DP_S}\ , \qquad (3.10)$$

для кожного сценарію.

5. Кваліметрична інтерпретація рівня ризику: На основі значення P_{nd} формується якісний показник рівня ризику пропуску інциденту шляхом порівняння з заданими пороговими значеннями:
   - $P_{nd} > 0.7$ = Критичний – системні «сліпі зони» у виявленні, потребує негайних заходів.
   - $0.5 < P_{nd} \leq 0.7$ = Високий – значний дефіцит контрольних заході.
   - $0.3 < P_{nd} \leq 0.5$ = Середній – часткова спостережуваність інцидентів.

- $P_{nd} \leq 0.3$ = Низький - достатній рівень виявлення.

Такий підхід дозволяє організації не лише визначити слабкі місця у процесі виявлення атак, але й пріоритезувати їх згідно з потенційним впливом на загальну модель ризику. У результаті методика дає змогу формувати зрозумілі, числово обґрунтовані рекомендації щодо оптимізації захисних заходів у SCADA-системах.

3.2 Програмна реалізація методики

У межах даного дослідження була створена програмна реалізація розробленої методики оцінювання ризику пропуску атак соціальної інженерії. Програмний модуль забезпечує централізоване опитування відповідальних осіб, автоматизований розрахунок ймовірнісної складової ризику пропуску (P_{nd}) та формування підсумкової оцінки рівня ризику для кожного з п’яти розглянутих сценаріїв соціальної інженерії.

За описаним у попередньому підрозділі алгоритмом, спочатку програма ініціалізує список із двадцяти п’яти питань, які оцінюють здатність системи виявляти атаки, та нормалізовану матрицю ваг:

1. Q1: Чи ведеться повне журналювання email-транзакцій (метадані, IP, вкладення, спроби доставки)?
2. Q2: Чи впроваджено регулярне навчання персоналу з розпізнавання фішингу та соціальних маніпуляцій?
3. Q3: Чи ведеться журналювання браузерної активності на робочих станціях та проводиться її аналіз на підозрілі URL?
4. Q4: Чи налаштовано моніторинг аномальних подій входу (Logon Events) на Domain Controller?
5. Q5: Чи фіксуються всі підключення зовнішніх пристроїв (USB, portable media) на робочих станціях та Engineering Workstation?

6. Q6: Чи ведеться аудит ARP/DHCP/Network Discovery журналів для виявлення підозрілих змін у мережевих призначеннях?

7. Q7: Чи здійснюється моніторинг та аналіз журналів OPC Server для виявлення нетипових запитів?

8. Q8: Чи забезпечено контроль фізичного доступу до HMI, операторських та робочих станцій (камери, карткові системи)?

9. Q9: Чи проводиться аудит конфігураційних змін на PLC/RTU та IED з журналюванням усіх модифікацій?

10. Q10: Чи ведеться журналювання команд, виданих через HMI, з аналізом на аномальні послідовності?

11. Q11: Чи реалізовано механізми виявлення аномалій на мережевому рівні L2/L3 (MAC, ARP, VLAN)?

12. Q12: Чи ведеться журналювання та аналіз подій на маршрутизаторах для виявлення нетипового трафіку?

13. Q13: Чи проходить персонал навчання щодо виявлення фізичних соціальних атак та інформує про інциденти?

14. Q14: Чи існують процедури фіксації та розслідування підозрілих телефонних/голосових звернень?

15. Q15: Чи ведуться журнали виконання програм/скриптів на Engineering Workstation (Program Execution Logs)?

16. Q16: Чи моніторяться Security Events на Domain Controller щодо нетипових дій користувачів?

17. Q17: Чи виконується моніторинг Session Data на веб-серверах для виявлення підозрілих або скомпрометованих сесій?

18. Q18: Чи налаштовано IDS/IPS або інші системи аналізу аномального трафіку (signature & anomaly-based)?

19. Q19: Чи ведеться журналювання доступу до критичних системних файлів, конфігурацій та скриптів (File Integrity Monitoring)?

20. Q20: Чи здійснюється аналіз Alarm та Alert Data на IED з фіксацією підозрілих тригерів?

21. Q21: Чи ведеться моніторинг історії змін у базі даних Historian (DB logs, modification logs)?
22. Q22: Чи перевіряється браузерна історія та дані кешу на предмет ознак watering-hole атак?
23. Q23: Чи існує політика верифікації зовнішніх запитів про допомогу (helpdesk validation policy)?
24. Q24: Чи корелюються журнали різних систем у SIEM для централізованого виявлення інцидентів?
25. Q25: Чи ведеться журналювання подій на Firewall/IDS/IPS з аналізом заблокованих або підозрілих запитів?

Вони стали основою для формування загалом всього опитувальника. Питання складені на основі вимог і рекомендацій міжнародних стандартів із кібербезпеки, зокрема NIST SP 800-53, ISO/IEC 27001, а також практик MITRE ATT&CK for ICS. При їх формуванні також був використаний чекліст джерел цифрової форензики представлений у другому розділі дипломної роботи. Це дозволило забезпечити відповідність реальним контрольним точкам, які можуть відігравати роль у процесі фіксації та форензичному аналізу інцидентів.

Кожне питання оцінюється відповідальною особою за шкалою від 1 до 5, де 1 означає відсутність відповідного контролю або його незадовільний стан, а 5 – повну реалізацію та належну ефективність. Програма передбачає ручний ввід оцінок, і контролює допустимий діапазон вводу. Наприклад:

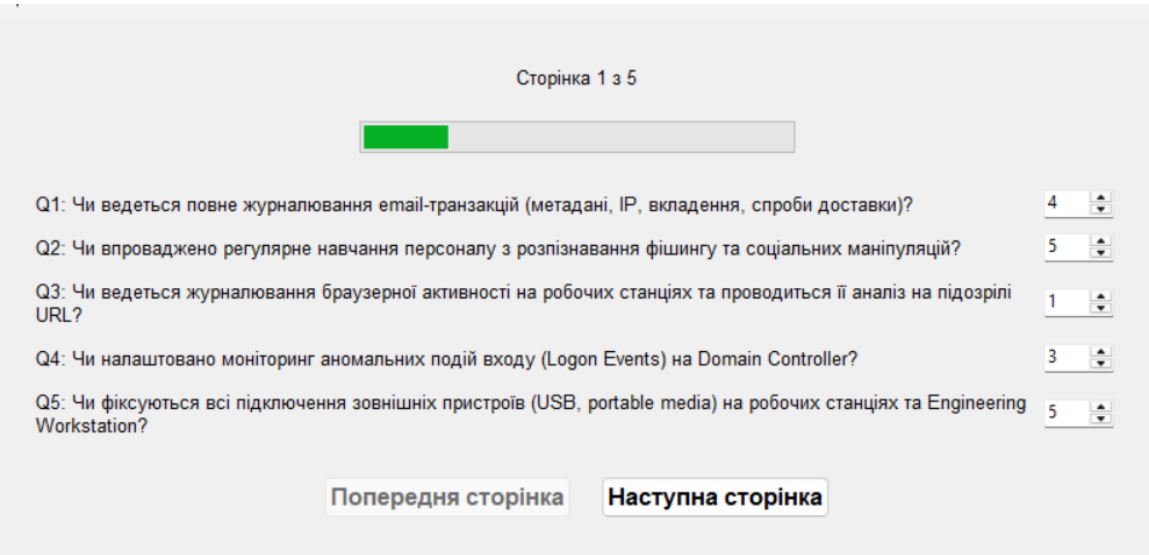

Рисунок 3.3 – Демонстрація вікна оцінювання питань

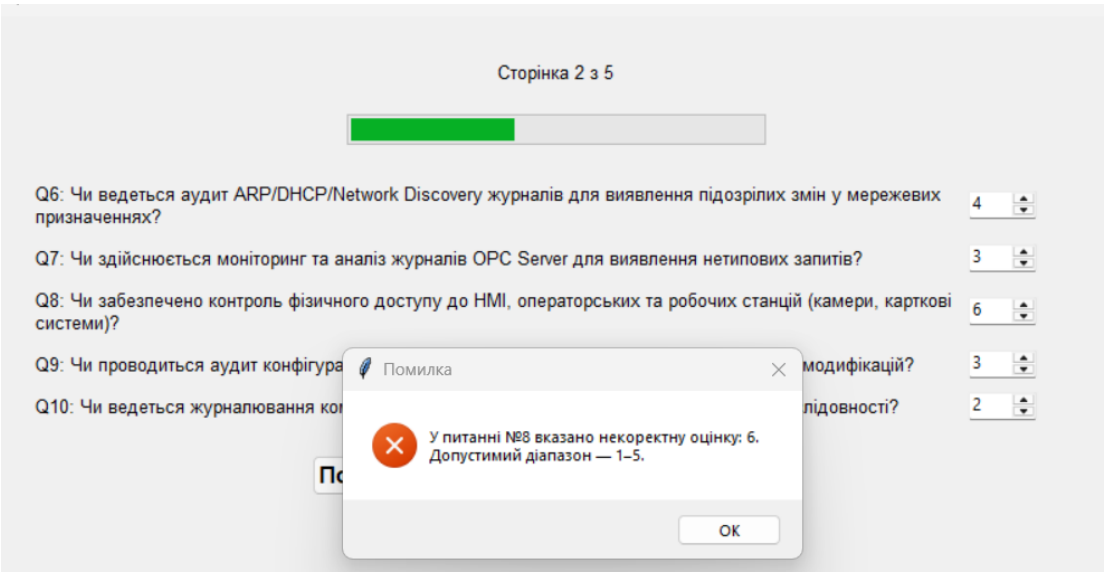

Рисунок 3.4 – Демонстрація вікна помилки при оцінюванні

На практиці такі оцінки можуть виставлятися адміністраторами SCADA/ICS, спеціалістами служби інформаційної безпеки, операторами SOC або внутрішнім аудитом – залежно від того, які підрозділи мають доступ до форензичних даних та відповідають за функціональні області безпеки. Таким чином, опитувальник реалізує процес експертного оцінювання стану системи виявлення аномалій і контролів, що впливають на здатність фіксувати атаки.

Після отримання відповідей код нормалізує значення оцінок та перемножає на значення вагових коєфіцієнтів з попередньо сформованої матриці:

Таблиця 3.1 – Матриця релевантності питанньь

Питання	Phishing (Email/Website)	Spear-phishing	Baiting	Water-Holing	Pretexting
Q1	0,1074	0,1036	0,0351	0,0146	0,0337
Q2	0,1031	0,1036	0,0351	0,0146	0,0337
Q3	0,0437	0,0351	0,0198	0,1364	0,0116
Q4	0,0742	0,0829	0,0198	0,0146	0,0116
Q5	0,0095	0,0119	0,1337	0,0146	0,0337
Q6	0,0107	0,0128	0,0721	0,0426	0,0116
Q7	0,0095	0,0119	0,0389	0,1364	0,0116
Q8	0,0095	0,0119	0,0389	0,0146	0,1113
Q9	0,0095	0,0119	0,0389	0,0146	0,1113
Q10	0,0437	0,0340	0,0214	0,0146	0,1113
Q11	0,0095	0,0119	0,0389	0,0426	0,0116
Q12	0,0437	0,0340	0,0214	0,0426	0,0116
Q13	0,0437	0,0343	0,0214	0,0146	0,0601
Q14	0,0095	0,0119	0,0107	0,0146	0,1113
Q15	0,0095	0,0119	0,1337	0,0146	0,0116
Q16	0,0742	0,0821	0,0235	0,0146	0,0116
Q17	0,0095	0,0119	0,0235	0,1364	0,0116
Q18	0,0723	0,1020	0,0235	0,0463	0,0116
Q19	0,0274	0,0119	0,0235	0,0146	0,0116
Q20	0,0095	0,0119	0,0235	0,0146	0,1113
Q21	0,0095	0,0340	0,0235	0,0146	0,0601
Q22	0,0437	0,1003	0,0351	0,1364	0,0116
Q23	0,0723	0,0614	0,0600	0,0146	0,0601
Q24	0,0723	0,0614	0,0235	0,0146	0,0116
Q25	0,0723	0,0613	0,0600	0,0463	0,0116

Коефіцієнти варіюються в межах від 0 до 1, де 1 відповідає максимально сильному впливу питання на виявлення певного сценарію, а 0 означає повну відсутність зв’язку. Таким чином, ваги дозволяють врахувати, що окремі контролі критично важливі для певних атак (наприклад, логування електронної пошти для фішингу або контроль USB-носіїв для baiting), тоді як інші контролі мають лише непряме або мінімальне значення.

Далі для кожного сценарію розраховується ймовірнісна складова (P_{nd}) за вище наведеними формулами. На основі порогових значень реалізується оцінка ризику на низький, середній, високий(>1,5) та критичний рівні(>1,7), що дозволяє користувачу отримати зрозумілий підсумковий висновок. Наприклад:

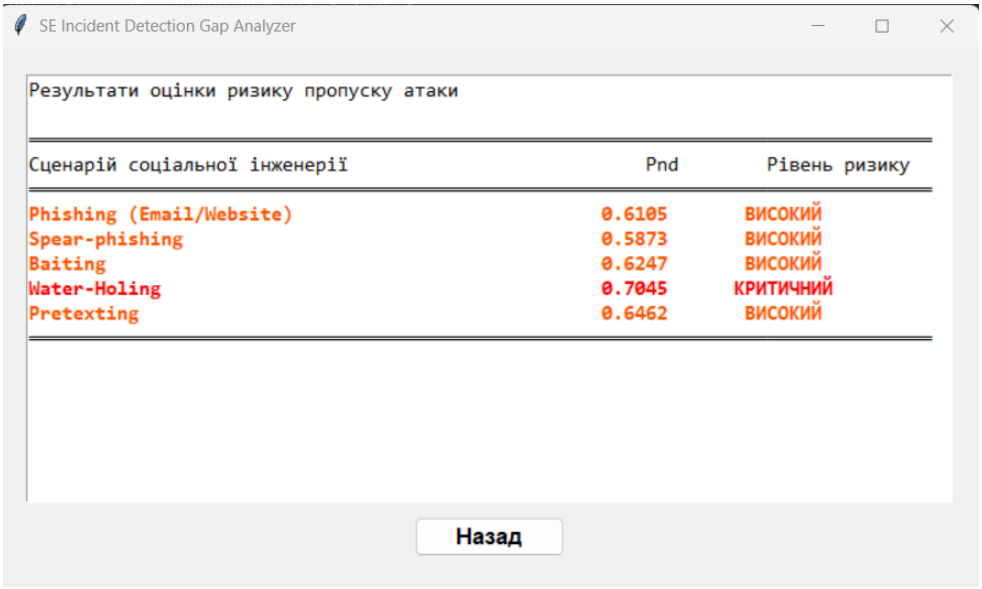

Рисунок 3.5 – Демонстрація виводу результатів виконання програми

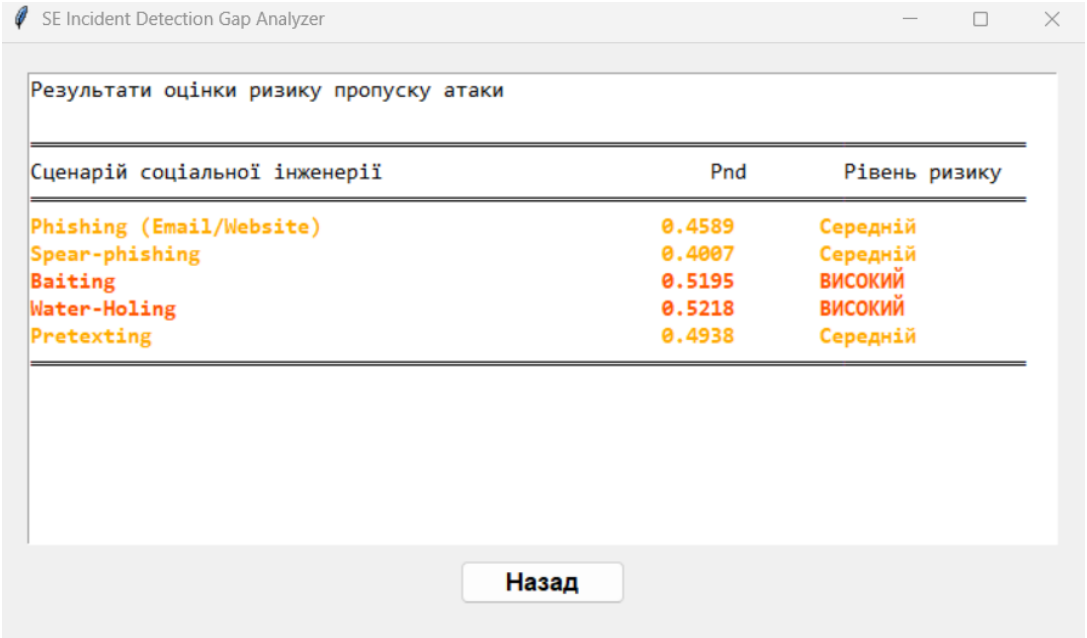

Рисунок 3.6 – Демонстрація виводу результатів виконання програми

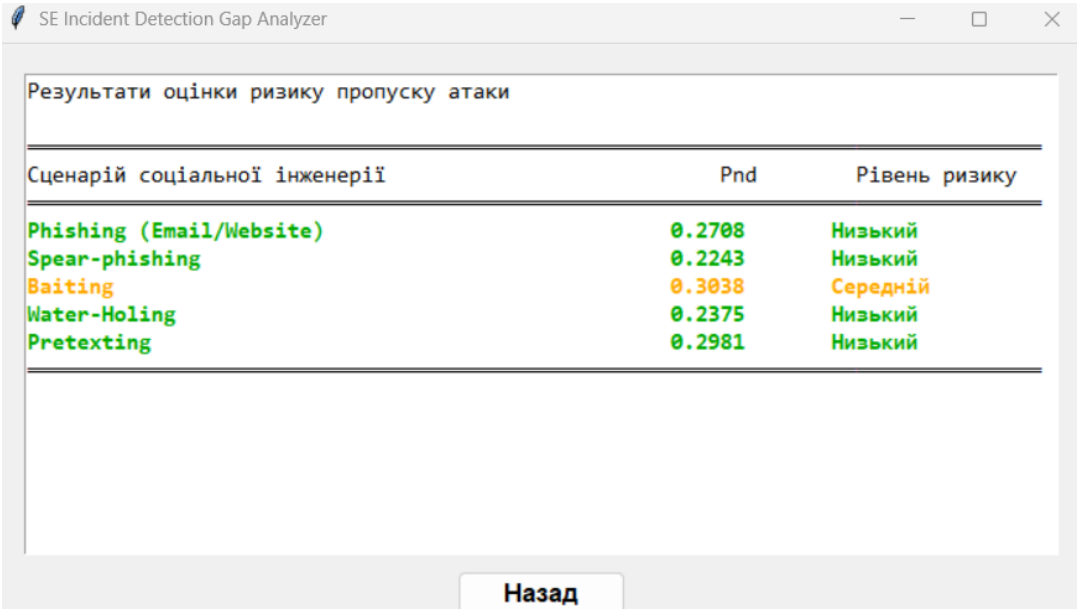

Рисунок 3.7 – Демонстрація виводу результатів виконання програми

Також передбачене логічне повернення до вже оцінених питань та зміну своїх відповідей для отримання іншого результату.

Програма забезпечує швидке оцінювання вразливостей SCADA-систем до атак соціальної інженерії, допомагаючи адміністраторам виявляти слабкі місця та планувати заходи для їх усунення.

3.3 Підсумковий аналіз розробленого підходу

Розроблена методика спрямована на формалізацію процесу кваліметричного оцінювання ризику пропуску інцидентів соціальної інженерії у SCADA-системах з урахуванням специфіки ОТ-середовища, рольової структури персоналу та доступних джерел цифрової форензики. Її ключовою особливістю є можливість системно оцінювати дефіцит контрольних заходів у частині виявлення інцидентів, незалежно від того, чи обумовлений він технічними, організаційними або людськими чинниками. Методика агрегує інформацію з різнорідних джерел, структуруючи її у вигляді стандартизованого опитування та матриці релевантності,

що забезпечує прозорість, відтворюваність та обґрунтованість отриманих результатів.

Важливою властивістю методики є її адаптивність. Матриця релевантності та перелік питань розглядаються як базовий кваліметричний шаблон, придатний для застосування у різних OT-архітектурах. На практиці склад питань, їхні вагові коефіцієнти та перелік сценаріїв соціальної інженерії можуть змінюватися залежно від технологічних особливостей об’єкта, архітектури мережевої взаємодії, рівня автоматизації, результатів аудитів безпеки або актуальної інформації про загрози. Процес адаптації доцільно здійснювати власником ризику або керівником служби інформаційної безпеки у взаємодії з OT-інженерами, SOC-командою та внутрішнім аудитом. Внесення змін до структури методики рекомендовано виконувати в межах формалізованої процедури керування версіями, що забезпечує узгодженість і порівнюваність результатів у часі.

Запропонована методика також створює основу для інтеграції з кількісними моделями ризику, зокрема з моделлю FAIR. Отриманий показник P_{nd} використовується як ймовірнісна складова ризику пропуску інцидентів або як індикатор дефіциту Control Strength у частині виявлення. Це дозволяє застосовувати результати методики як вхідні параметри для більш загальних ризик-орієнтованих моделей, у межах яких можуть враховуватися активи, потенційні втрати та економічні наслідки інцидентів. Таким чином, методика не замінює повноцінні кількісні моделі ризику, а доповнює їх, забезпечуючи формалізовану оцінку слабких місць детекції.

Водночас, як і будь-який підхід, що ґрунтується на експертних оцінках і вагових коефіцієнтах, запропонована методика є чутливою до якості вихідних даних та компетентності експертів. Це не розглядається як недолік, а підкреслює необхідність регулярного перегляду параметрів методики та залучення профільних фахівців до процесу оцінювання. Для підвищення об’єктивності результати можуть

бути доповнені даними SOC, журналами SIEM, інформацією про фактичні інциденти та зовнішніми джерелами розвідки загроз.

Серед перспективних напрямів розвитку методики доцільно відзначити автоматизацію збору вхідних даних з технічних систем моніторингу, поглиблену інтеграцію з інструментами цифрової форензики, використання методів машинного навчання для уточнення вагових коефіцієнтів, а також адаптацію методики до нових і еволюційних сценаріїв соціальної інженерії. Реалізація цих напрямів дозволить зменшити суб'єктивність оцінок і розширити застосовність методики в реальних промислових середовищах.

Висновки до розділу 3

У цьому розділі було представлено методику кваліметричного оцінювання ризику пропуску інцидентів соціальної інженерії на об'єктах критичної інфраструктури, яка дозволяє формалізувати аналіз здатності SCADA-систем до виявлення атак і перевести його у структуровану та відтворювану форму. Показано, що поєднання принципів цифрової форензики, ризик-орієнтованої логіки та математичної нормалізації експертних оцінок створює підхід, здатний відобразити реальний стан спостережуваності інцидентів в OT-середовищі незалежно від конкретної реалізації атаки.

Розроблений алгоритм обчислення показника P_{nd} дозволив переосмислити поняття Control Strength у контексті OT-систем, інтерпретуючи його з позиції дефіциту контрольних заходів у частині виявлення соціально-інженерних атак. Використання стандартизованого переліку питань, системи вагових коефіцієнтів та процедури нормалізації забезпечує логічну узгодженість і прозорість результатів. Це створює можливість ідентифікувати сегменти інфраструктури та сценарії атак, для яких ризик пропуску є найбільш критичним, і відповідно визначати пріоритети підсилення систем безпеки.

Реалізована програмна підтримка методики підвищує її прикладну цінність, забезпечуючи автоматизацію ключових етапів оцінювання – від збору експертних даних до формування якісного рівня ризику пропуску інцидентів. Завдяки цьому процес оцінювання набуває властивостей повторюваності та незалежності від окремих виконавців, що дозволяє інтегрувати методику у регулярні аудити безпеки та внутрішні процедури контролю в організаціях критичної інфраструктури.

Таким чином, запропонована методика може використовуватися як практичний інструмент для виявлення слабких місць у системах детекції соціально-інженерних атак на ОКІ та формує основу для подальшої інтеграції з повноцінними кількісними моделями ризику. Вона дозволяє не лише зафіксувати поточний рівень готовності системи до виявлення інцидентів, а й обґрунтовано планувати заходи з її подальшого зміцнення.

ВИСНОВКИ

У результаті виконання даної роботи були вирішені наступні завдання:

1. Узагальнення сучасних підходів до соціальної інженерії в контексті критичної інфраструктури та систематизація реальних кейсів атак дозволили розкрити соціальну інженерію як домінуючий вектор первинного проникнення в OT/SCADA-середовища. Аналіз практичних інцидентів показав, що успішність таких атак зумовлюється поєднанням психологічного впливу на персонал і специфіки промислових процесів, де пріоритет безперервності роботи часто обмежує глибину контролю безпеки. Це дало змогу виокремити ключові напрями атак (фішинг, таргетований pretexting, зловживання довірою до підрядників) та обґрунтувати необхідність фокусування захисних заходів не лише на технічних, а й на поведінкових чинниках.
2. Дослідження процесу цифрової форензики в OT-контексті показало, що виявлення наслідків соціально-інженерних атак можливе лише за умови комплексного використання різнорідних джерел даних, таких як журнали автентифікації, події віддаленого доступу, зміни конфігурацій PLC/HMI та аномалії взаємодій між компонентами SCADA. Водночас встановлено, що реальні OT-архітектури мають суттєві обмеження щодо повноти логування та централізованого зберігання даних. Виділення ключових індикаторів соціально-інженерного впливу дозволило сформувати практичну основу для реконструкції сценаріїв атак навіть за умов нестачі форензичних слідів.
3. Побудова чеклісту відповідностей між сценаріями атак, індикаторами та пристроями фіксації дала змогу формалізувати взаємозв’язок між поведінковими діями зловмисника та технічними артефактами, доступними для аналізу в OT-середовищі. Розроблена матриця та графік важливості активів наочно продемонстрували, які компоненти інфраструктури є критичними з точки зору накопичення форензичних доказів, а які створюють

«сліпі зони» для виявлення інцидентів. Отримані результати можуть бути використані для оптимізації архітектури моніторингу та пріоритезації заходів захисту з урахуванням реальних можливостей фіксації подій.

4. Адаптація окремих елементів моделі FAIR до завдань оцінювання ризику пропуску інцидентів у OT-контексті дозволила переосмислити класичні підходи до ризик-менеджменту з фокусом не на ймовірність реалізації атаки, а на дефіцит контрольних заходів у частині її виявлення. Запропонований підхід інтегрує структуровані експертні оцінки, вагові коефіцієнти форензичних індикаторів та рівень реалізації контрольних заходів, формуючи кількісну оцінку ймовірнісної складової ризику пропуску та забезпечуючи відтворюваність і порівнюваність результатів. Така інтерпретація розширює можливості застосування логіки FAIR у середовищах, де повноцінні статистичні дані є обмеженими або відсутніми.
5. Реалізація програмного прототипу методики підтвердила її прикладну придатність для використання в реальних умовах експлуатації об’єктів критичної інфраструктури. Автоматизація обчислень забезпечує систематичний аналіз різних сценаріїв соціальної інженерії та підтримує формування якісної оцінки рівня ризику пропуску інцидентів для прийняття управлінських рішень щодо підсилення систем моніторингу й реагування. Запропонований інструмент може бути інтегрований у SOC/SIEM-процеси, застосований під час внутрішніх аудитів безпеки або використаний як допоміжний засіб оцінювання кіберстійкості OT-середовищ.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Social engineering: A survey of the state of the art [Електронний ресурс] // ScienceDirect. – 2017. – Режим доступу до ресурсу: https://www.sciencedirect.com/science/article/abs/pii/S0167404817302249
2. Towards an Ontological Model Defining the Social Engineering Domain [Електронний ресурс] // ResearchGate. – 2014. – Режим доступу до ресурсу: https://www.researchgate.net/publication/263588276_Towards_an_Ontological_Model_Defining_the_Social_Engineering_Domain
3. NIST SP 800-53 Rev. 5: Awareness and Training (AT-2, AT-2(3)) [Електронний ресурс] // NIST Cybersecurity Framework. – 2020. – Режим доступу до ресурсу: https://csf.tools/reference/nist-sp-800-53/r5/at/at-2/at-2-3/
4. A survey of social engineering attacks [Електронний ресурс] // ScienceDirect. – 2016. – Режим доступу до ресурсу: https://www.sciencedirect.com/science/article/abs/pii/S0167404816300268
5. What is Social Engineering? [Електронний ресурс] // Cisco. – 2023. – Режим доступу до ресурсу: https://www.cisco.com/site/us/en/learn/topics/security/what-is-social-engineering.html
6. Social engineering attacks: Techniques and countermeasures [Електронний ресурс] // IEEE Xplore. – 2020. – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/9312039
7. Мітникк К. Мистецтво обману: керування людським фактором у безпеці [Електронний ресурс]. – Режим доступу до ресурсу: https://scispace.com/pdf/the-art-of-deception-controlling-the-human-element-of-2m3u2hus21.pdf
8. Social Engineering Attacks Explained [Електронний ресурс] // Splunk Blog. – 2023. – Режим доступу до ресурсу: https://www.splunk.com/en_us/blog/learn/social-engineering-attacks.html

9. Social Engineering Attacks Prevention: A Systematic Literature Review [Електронний ресурс] // ResearchGate. – 2022. – Режим доступу до ресурсу: https://www.researchgate.net/publication/359528837_Social_Engineering_Attacks_Prevention_A_Systematic_Literature_Review
10. Digital forensics and social engineering data analysis [Електронний ресурс] // MDPI. – 2023. – Режим доступу до ресурсу: https://www.mdpi.com/2306-5729/8/10/156
11. Закон України «Про критичну інфраструктуру» [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/1882-20#Text
12. Critical Infrastructure Protection: Securing Essential Systems Against Cyber Threats [Електронний ресурс] // The SSL Store Blog. – 2023. – Режим доступу до ресурсу: https://www.thesslstore.com/blog/critical-infrastructure-protection-securing-essential-systems-against-cyber-threats/
13. KnowBe4 Report: Critical Infrastructure Under Siege [Електронний ресурс] // KnowBe4. – 2023. – Режим доступу до ресурсу: https://www.knowbe4.com/press/knowbe4-report-reveals-critical-infrastructure-under-siege-with-cyber-attacks-increasing-30-percent-in-one-year
14. Security Considerations for Critical Infrastructure [Електронний ресурс] // Government of Canada. – 2022. – Режим доступу до ресурсу: https://www.cyber.gc.ca/en/guidance/security-considerations-critical-infrastructure-itsap10100
15. ICS/SCADA Social Engineering Attacks [Електронний ресурс] // InfoSec Institute. – 2023. – Режим доступу до ресурсу: https://www.infosecinstitute.com/resources/scada-ics-security/ics-scada-social-engineering-attacks/
16. Social Engineering Attacks: A Survey [Електронний ресурс] // ResearchGate. – 2019. – Режим доступу до ресурсу: https://www.researchgate.net/publication/332151597_Social_Engineering_Attacks_A_Survey

17. Significant Cyber Incidents [Електронний ресурс] // CSIS. – 2024. – Режим доступу до ресурсу: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
18. IBM X-Force Threat Intelligence Index 2025 [Електронний ресурс] // IBM Institute for Business Value. – 2025. – Режим доступу до ресурсу: https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/2025-threat-intelligence-index
19. Security threats to critical infrastructure: the human factor [Електронний ресурс] // Academia.edu. – 2020. – Режим доступу до ресурсу: https://www.academia.edu/43047571/Security_threats_to_critical_infrastructure_the_human_factor
20. The persuasion and security awareness experiment [Електронний ресурс] // Academia.edu. – 2013. – Режим доступу до ресурсу: https://www.academia.edu/12174718/The_persuasion_and_security_awareness_experiment_reducing_the_success_of_social_engineering_attacks
21. Cyber Insights 2025: Social Engineering Gets AI Wings [Електронний ресурс] // SecurityWeek. – 2025. – Режим доступу до ресурсу: https://www.securityweek.com/cyber-insights-2025-social-engineering-gets-ai-wings
22. Social Engineering Attacks: A Clearer Perspective [Електронний ресурс] // Academia.edu. – 2021. – Режим доступу до ресурсу: https://www.academia.edu/88638180/Social_Engineering_Attacks_A_Clearer_Perspective
23. Social Engineering Attacks: Common Techniques and How to Prevent Them [Електронний ресурс] // Digital Guardian. – 2023. – Режим доступу до ресурсу: https://www.digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack
24. Understanding the Dangers of Social Engineering [Електронний ресурс] // U.S. Department of State. – 2023. – Режим доступу до ресурсу: https://www.state.gov/understanding-the-dangers-of-social-engineering

25. NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response [Електронний ресурс]. – 2006. – Режим доступу до ресурсу: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf
26. ДСТУ та нормативні вимоги з технічного захисту інформації [Електронний ресурс]. – Режим доступу до ресурсу: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=74978
27. NIST IR 8428: Cybersecurity Framework Profile for the Responsible Use of AI [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8428.pdf
28. D4I – Digital Forensics Framework for Investigating Cyber Attacks [Електронний ресурс] // ResearchGate. – 2019. – Режим доступу до ресурсу: https://www.researchgate.net/publication/338184597_D4I_-_Digital_forensics_framework_for_reviewing_and_investigating_cyber_attacks
29. Use of Digital Forensic Technology to Reveal the Identity of Social Engineering Crimes [Електронний ресурс] // ResearchGate. – 2024. – Режим доступу до ресурсу: https://www.researchgate.net/publication/383829875_Use_Of_Digital_Forensic_Technology_To_Reveal_The_Identity_Of_Social_Engineering_Crimes
30. Phishing (MITRE ATT&CK Technique T1566) [Електронний ресурс] // MITRE ATT&CK. – 2024. – Режим доступу до ресурсу: https://attack.mitre.org/techniques/T1566/
31. Social Engineering Detection Project Repository [Електронний ресурс] // GitHub. – 2024. – Режим доступу до ресурсу: https://github.com/alkovaalina/Social-engineering-detection
32. ІТ-простір сьогодення: тенденції, інновації та перспективи розвитку : збірник тез доповідей ІІ Міжнародної науково-практичної студентської конференції (15 жовтня 2025 року, м. Харків, Україна) [Електронний ресурс]. – Харків, 2025. – С. 19–22. – Режим доступу до ресурсу: https://ekhnuir.karazin.ua/items/616ed73d-24cf-4327-a988-dcd100a94afe

ДОДАТОК А

main.py

```
import tkinter as tk
from tkinter import ttk, messagebox
import numpy as np
import math
import pandas as pd

with open('questions.txt', 'r', encoding='utf-8') as f:
    questions = [line.strip() for line in f if line.strip()]

df = pd.read_excel('weight_matrix.xlsx', sheet_name='norm_weight_matrix')
W = df.iloc[:, 1:].values

scenarios = [
    "Phishing (Email/Website)",
    "Spear-phishing",
    "Baiting",
    "Water-Holing",
    "Pretexting"
]

class App:
    def __init__(self, root):
        self.root = root
        self.root.title("SE Incident Detection Gap Analyzer")
        self.root.geometry("800x400")

        self.questions_per_page = 5
        self.total_pages = math.ceil(len(questions) / self.questions_per_page)
        self.current_page = 0
        self.score_vars = [tk.IntVar(value=1) for _ in questions]

        style = ttk.Style()
        style.configure("TLabel", font=("Arial", 10))
        style.configure("TButton", font=("Arial", 12, "bold"))

        self.question_frame = ttk.Frame(root, padding=20)
        self.question_frame.pack(fill="both", expand=True)

        self.progress_label = ttk.Label(self.question_frame, text="")
        self.progress_label.pack(pady=10)
```

```
        self.progress = ttk.Progressbar(
            self.question_frame, orient="horizontal",
            length=300, maximum=self.total_pages
        )
        self.progress.pack(pady=10)

        self.page_frame = ttk.Frame(self.question_frame)
        self.page_frame.pack(fill="x", pady=10)

        self.buttons_frame = ttk.Frame(self.question_frame)
        self.buttons_frame.pack(pady=10)

        self.prev_button = ttk.Button(self.buttons_frame, text="Попередня сторінка",
command=self.prev_page)
        self.prev_button.grid(row=0, column=0, padx=10)

        self.next_button = ttk.Button(self.buttons_frame, text="Наступна сторінка",
command=self.next_page)
        self.next_button.grid(row=0, column=1, padx=10)

        self.result_frame = ttk.Frame(root, padding=20)
        self.result_text = tk.Text(self.result_frame, height=15, wrap="word",
font=("Consolas", 11))
        self.result_text.pack(fill="both", expand=True)
        self.result_text.config(state="disabled")

        self.back_button = ttk.Button(self.result_frame, text="Назад",
command=self.back_to_questions)
        self.back_button.pack(pady=10)

        self.build_page()

    def validate_scores(self):
        for idx, var in enumerate(self.score_vars, start=1):
            val = var.get()
            if not (1 <= val <= 5):
                messagebox.showerror(
                    "Помилка",
                    f"У питанні №{idx} вказано некоректну оцінку: {val}.\n"
                    "Допустимий діапазон – 1–5."
                )
                return False
        return True
```

```
    def build_page(self):
        for widget in self.page_frame.winfo_children():
            widget.destroy()

        start = self.current_page * self.questions_per_page
        end = min(start + self.questions_per_page, len(questions))

        for i in range(start, end):
            ttk.Label(self.page_frame, text=questions[i], wraplength=700, justify="left")\
                .grid(row=i - start, column=0, padx=5, pady=5, sticky="w")

            ttk.Spinbox(self.page_frame, from_=1, to=5, textvariable=self.score_vars[i], width=5)\
                .grid(row=i - start, column=1, padx=5, pady=5)

        self.progress['value'] = self.current_page + 1
        self.progress_label.config(text=f"Сторінка {self.current_page + 1} з {self.total_pages}")

        self.prev_button.config(state="disabled" if self.current_page == 0 else "normal")
        self.next_button.config(text="Обчислити" if self.current_page == self.total_pages - 1 else "Наступна сторінка")

    def prev_page(self):
        if self.current_page > 0:
            self.current_page -= 1
            self.build_page()

    def next_page(self):
        if not self.validate_scores():
            return
        if self.current_page < self.total_pages - 1:
            self.current_page += 1
            self.build_page()
        else:
            self.calculate()

    def calculate(self):
        if not self.validate_scores():
            return

        scores = np.array([v.get() for v in self.score_vars])
        norm_scores = scores / 5.0
```

```
        DP = np.clip(np.dot(norm_scores, W), 0, 1)
        Pnd = 1 - DP

        result = "Результати оцінки ризику пропуску атаки\n\n"
        result += "═" * 82 + "\n"
        result += f"{'Сценарій соціальної інженерії':<48} {'Pnd':>10} {'Рівень ризику':>20}\n"
        result += "═" * 82 + "\n"

        risk_levels = []
        for scenario, p in zip(scenarios, Pnd):
            if p > 0.7:
                risk = "КРИТИЧНИЙ"
                tag = "critical"
            elif p > 0.5:
                risk = "ВИСОКИЙ"
                tag = "high"
            elif p > 0.3:
                risk = "Середній"
                tag = "medium"
            else:
                risk = "Низький"
                tag = "low"

            result += f"{scenario:<48} {p:>9.4f} {risk:^12}\n"
            risk_levels.append((scenario, tag))

        result += "═" * 82 + "\n\n"

        self.question_frame.pack_forget()
        self.result_frame.pack(fill="both", expand=True)

        self.result_text.config(state="normal")
        self.result_text.delete(1.0, tk.END)
        self.result_text.insert(tk.END, result)

        colors = {
            "critical": "#FF0000",
            "high": "#FF5500",
            "medium": "#FFAA00",
            "low": "#00AA00"
        }
        for tag, color in colors.items():
```

```
            self.result_text.tag_configure(tag, foreground=color, font=("Consolas", 11, "bold"))

        for scenario, tag in risk_levels:
            pos = "1.0"
            while True:
                pos = self.result_text.search(scenario, pos, tk.END)
                if not pos:
                    break
                line_end = pos.split('.')[0] + ".end"
                self.result_text.tag_add(tag, pos, line_end)
                pos = line_end

        self.result_text.config(state="disabled")

    def back_to_questions(self):
        self.result_frame.pack_forget()
        self.question_frame.pack(fill="both", expand=True)
        self.build_page()


if __name__ == "__main__":
    root = tk.Tk()
    App(root)
    root.mainloop()
```