KAPITEL 7 / *CHAPTER 7* [7]
METHODS FOR ASSESSING THE RISKS OF SOCIAL ENGINEERING IN MEDICINE

DOI: 10.30890/2709-2313.2025-45-02-029

В медичній галузі існують два варіанта рішень для оцінки та проведення тестів соціальної інженерії у медичній сфері:

– Платформи навчання та симуляції (Security Awareness + Phishing Simulation) – комерційні SaaS-продукти, що дозволяють робити масові або таргетовані симуляції фішингових атак, автоматизовану аналітику реакцій користувачів, навчальні модулі та звіти (приклади: KnowBe4, Cofense, Proofpoint). Такі рішення часто використовуються у Європі як частина комплексу заходів з управління людським ризиком. [2]

– Консалтингові послуги та «червоні команди» (penetration testing social engineering) – послуги локальних або регіональних компаній, що виконують спрямовані тестування персоналу (телефонні атаки, таргетований фішинг з використанням відкритої інформації), а також навчальні заняття та розробку політик. В Україні такі послуги надають як міжнародні партнери (через офіси або партнерів), так і локальні компанії-консультанти (наприклад, Berezha Security Group, Iterasec та інші консалтингові/кіберкоманди). Ринок кібербезпеки України значно зріс останні роки, що відобразилося й у розширенні локальних послуг у галузі соціальної інженерії. [3]

Крім комерційних рішень, на рівні політик і стандартів з'являються спеціалізовані вимоги, HIS2 (NIS2), які визначають більш жорсткі вимоги щодо управління кіберризиками, до яких належить і ризик через людський фактор у критичних секторах (серед яких — охорона здоров'я). Відповідність NIS2 стає важливою для європейських медичних установ та їх постачальників. [4]

На рис. 1.1 зображено загальну динаміку зростання фішингових/соціо-інженерних атак у секторі охорони здоров'я. На цих графіках зображено порівняння кількості атак соціальної інженерії у сфері медицині в Україні та в

[7] ***Authors:*** *Melnyk Marharyta, Velychkanych Yurii*
Author's sheets: *0,35*

світі (2020–2024). Індекс зростання (2020 = 100) для України й світу. Дані на графіках побудовані для візуалізації тенденцій (не є офіційною статистикою).

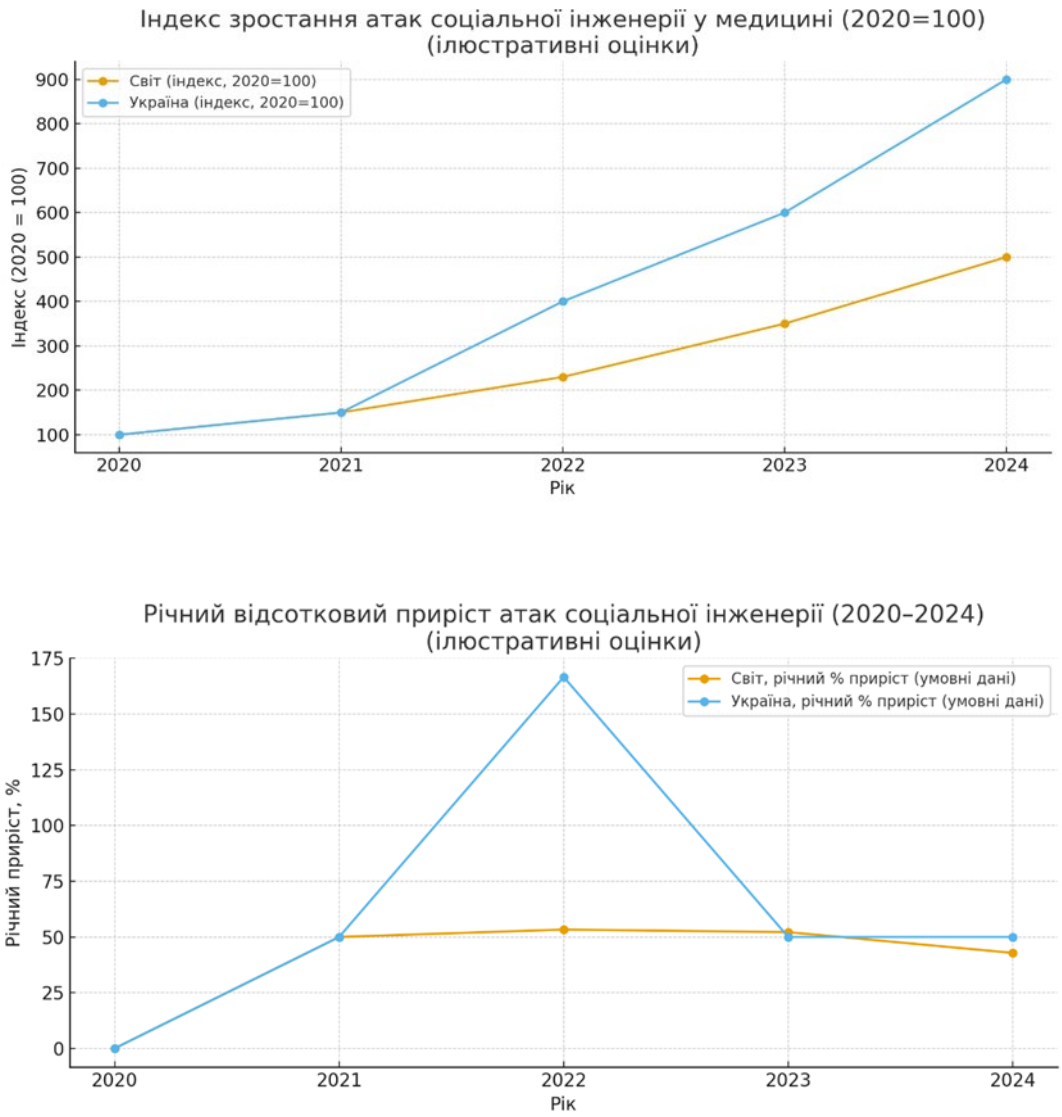

Рисунок 1.1. – Загальна динаміка зростання фішингових/соціоінженерних атак у секторі охорони здоров'я 2020-2024 рр

Вони відображають загальну динаміку, підтверджену оглядами та звітами зростання фішингових/соціо-інженерних атак у секторі охорони здоров'я, посилення активності в Україні під час війни тощо). Для побудови були розглянуті звіти HHS/HC3, HIPAA Journal, CERT-UA/SCPC, огляди 2023–2024 про зростання фішингу в healthcare. [5]

Для розуміння специфіки ринку медичних послуг, вважаю доцільним

навести табл 1.1 порівняння характеристик ринку порівняльна характеристика ринку досконалої конкуренції та ринку медичних послуг

Таблиця 1.1 – Порівняння характеристик ринку порівняльна характеристика ринку досконалої конкуренції та ринку медичних послуг

Критерій	**Ринок досконалої конкуренції**	**Ринок медичних послуг**
Кількість продавців	Велику кількість виробників і продавців, що забезпечує високий рівень конкуренції.	Кількість постачальників обмежена; існують бар'єри для входу на ринок, а в окремих випадках — умови, близькі до природної монополії.
Однорідність товару	Товари є однорідними та взаємозамінними.	Медичні послуги є неоднорідними, індивідуальними та унікальними для кожного пацієнта.
Інформованість споживачів	Покупці володіють повною та достовірною інформацією про товари й ціни.	Інформація споживачів є неповною або недосконалою через складність та специфічність медичних послуг.
Співвідношення ціни і якості	Існує можливість об'єктивно порівняти ціну товару з його якістю.	Порівняння ціни та якості медичних послуг часто є утрудненим або неможливим через їх індивідуальний характер.
Мета виробників	Основною метою є максимізація прибутку.	Значну частину ринку становлять державні та приватні медичні установи, які можуть працювати навіть зі збитками, виконуючи соціальні функції.
Форма реалізації	Реалізація продукції здійснюється безпосередньо між виробником і споживачем.	У більшості випадків необхідна участь «третьої сторони» — страхових компаній або інших посередників, які оплачують значну частину медичних послуг.

Оцінка ризиків соціальної інженерії в медичній сфері передбачає чітку послідовність етапів, що дозволяють виявити, проаналізувати й мінімізувати загрози, які ризики виникають через людський фактор, комунікації та організаційні процеси. Нижче наведені ключові етапи алгоритму оцінки ризиків соціальної інженерії у медичних закладах

Етап визначення об'єкту аналізу, визначення ресурсів, які можуть бути залучені для захисту (технічні, організаційні, людські).

На цьому етапі необхідно з'ясувати, що саме підлягає захисту:

- інформаційні системи, що зберігають / обробляють медичні дані пацієнтів;

- персональні дані співробітників;

- комунікаційні канали (електронна пошта, телефон, внутрішні месенджери);

- фізичні засоби та середовище (пристрої, доступ до серверних, робочі станції).

Етап ідентифікації потенційних загроз соціальної інженерії, встановлюються конкретні види соціальних інженерних атак, які можуть виникнути в медичному закладі:

- фішинг, spear-phishing, smishing, vishing;

- підробка особи (pretexting) та використання довіри (impersonation); [8]

- інсайдерські загрози (співробітники, які мають доступ до конфіденційної інформації та можуть бути соціально інженіровані або самі зловживати);

- маніпуляції через мобільні пристрої або пристрої IoMT (Internet of Medical Things), через слабкі місця у доступі та контролі; [8]

Етап оцінювання ймовірності реалізації кожної загрози, після ідентифікації загроз необхідно оцінити ймовірність того, що конкретна загроза реалізується в умовах даного закладу:

–Використання даних історичних інцидентів (якщо доступні) — скільки разів подібний інцидент вже траплявся.

–Оцінка рівня обізнаності персоналу, наявності захисних засобів (наприклад MFA, шифрування, політик доступу).

–Розгляд зовнішніх факторів: ступінь загроз з боку кібератак, соціально-економічного середовища, регуляторного тиску.

Цей етап може бути якісним (експертне опитування) або кількісним (рейтинг ймовірності в балах чи категоріях: низька, середня, висока).

Далі,визначаємо рівень впливу, на цьому кроці оцінюється, якою буде наслідки реалізації загрози: Вплив на конфіденційність пацієнтів — витік особистих чи медичних даних; Вплив на безпеку пацієнтів (наприклад, якщо інформація порушена, можуть бути помилки в лікуванні). Репутаційні наслідки – довіра пацієнтів, юридичні штрафи, нормативні наслідки. Фінансові витрати

такі як компенсації, штрафи, витрати на відновлення систем, аудит.

Наступним кроком є побудова матриці ризиків та пріоритезація ризиків та визначення критичних зон безпеки табл 2.1

Комбінування оцінок ймовірності та впливу для кожної загрози у матрицю ризиків, де:

- по горизонталі — рівень впливу (наприклад: низький, середній, високий);
- по вертикалі — ймовірність (рідко, можливо, часто).

Загрози, що потрапляють у квадранти з високою імовірністю та великим впливом, належать до критичних зон, які вимагають пріоритетного реагування. [8, 11]

Таблиця 1.1 – матриця ризиків

Ймовірність / Вплив	**Низький**	**Середній**	**Високий**
Рідко	Низький (🟢)	Низький (🟢)	Середній (🟡)
Можливо	Низький (🟢)	Середній (🟡)	Високий (🟠)
Часто	Середній (🟡)	Високий (🟠)	Критичний (🔴)

На основі матриці здійснюється, визначення, які загрози є найбільш небезпечними (високий вплив та висока ймовірність) – вони мають бути опрацьовані першочергово. Та зроблена оцінка, які заходи захисту можуть знизити ймовірність або вплив цих загроз. Наступним кроком є встановлення послідовності дій та ресурсів – реалізація заходів для критичних ризиків, підтримка менш пріоритетних.

Для оцінки ризиків рекомендовано використовувати наступну формулу:

$$R=P*A \quad (1.1)$$

де P– ймовірність настання події,

A– розмір збитку,

Для розрахунку пріоритету ризику (RPN) , рекомендуємо використовувати наступну формулу

$$RPN=S*O*D \quad (1.2)$$

де S– ступінь серйозності ризиків,

O– частота виникнення ризиків,

D– ймовірність виявлення ризиків.

Рекомендовано використовувати формулу для розрахунку частоти реалізації небезпеки:

$$R=n/N \quad (1.3)$$

де n— кількість реалізованих наслідків,

N— максимально можлива їх кількість

Розробка методики оцінки ризиків соціальної інженерії в медицині має свої особливості порівняно з іншими сферами через специфіку медичних даних, етичні аспекти та високий рівень довіри між пацієнтом і медичним персоналом.

Ці вимоги відображені у стандартних підходах до оцінки ризиків (наприклад, NIST SP 800-30 та ISO/IEC 27005), які задають процес – від встановлення контексту до ідентифікації, аналізу, оцінки та обробки ризиків – і є логічною опорою для адаптації до специфіки медичної сфери.

Пацієнти часто довіряють медичному персоналу, що може бути використано соціальними інженерами для отримання доступу до конфіденційної інформації. Це підвищує ризик успішних атак.

Чутливість даних та робота медичної сфери 24/7, медичні установи обробляють особисті та конфіденційні дані пацієнтів, що робить їх привабливою мішенню для соціальних інженерів. Невірне використання цих даних може призвести до серйозних наслідків для пацієнтів та медичних установ.

Етичні та правові аспекти, використання соціальної інженерії в медицині може порушувати етичні норми та законодавство щодо захисту персональних даних. Тому важливо враховувати ці аспекти при оцінці ризиків та розробці методик захисту.

Для практичного застосування у медичній установі доцільно поєднати змішаний підхід (semi-quantitative):

Кількісні елементи – використання, де доступні, вимірників (кількість

інцидентів/рік, частка співробітників, що натиснули в тестовому фішингу, фінансові втрати), а також, за потреби, кількісні моделі (наприклад, FAIR) для оцінки очікуваних втрат у грошовому еквіваленті.

Якісні / зрілісні елементи – п'ятибальні/шкальні оцінки рівня контролю (автентифікація, шифрування, навчання, політика BYOD тощо) і матриця «ймовірність × вплив» для візуальної пріоритизації. Цей підхід відповідає практикам ISO/IEC 27005 і NIST.

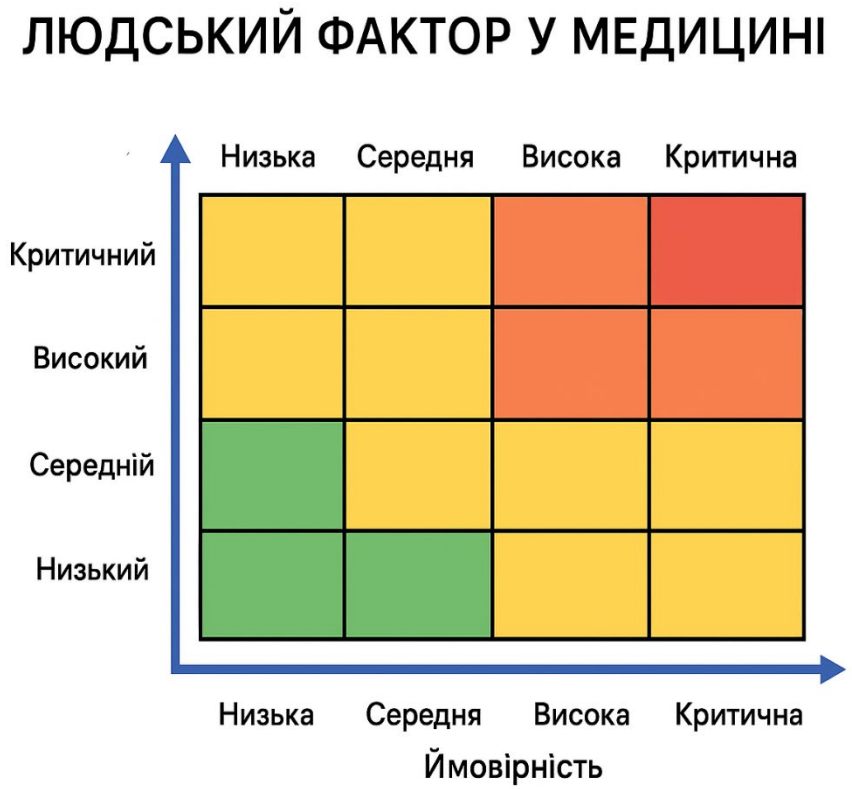

Рисунок 3.1 – Матиця «ймовірність х вплив» для ризиків соціальної інжереній в медицині

Також присутні особливості врахування людського фактору у медичних установах. Людський фактор у медицині має специфічні характеристики, що впливають на модель ризику і матрицю «ймовірність × вплив» для візуальної пріоритизації. Цей підхід відповідає практикам ISO/IEC 27005 і NIST.

На відміну від звичайних IT або корпоративних систем, у медицині вплив помилок має етичний і клінічний вимір, людський фактор посилюється емоційним навантаженням і стресом, соціальна інженерія може використовувати

співчуття або довіру медперсоналу. Тому захист має бути психологічно адаптований через тренінги, симуляції, контроль комунікацій.

Уразливість персоналу пов'язана з наступними факторами:

– Висока частота контактів з пацієнтами та сторонніми (адміністративні, клінічні, лабораторні підрозділи) – збільшена поверхня соціальної інженерії.

– Сильний стрес і робоче навантаження працівників (мінливі графіки, втома) підвищують шанс помилки або імпульсивної відповіді на фішинг-повідомлення.

– Різноманітність ролей і прав доступу (лікарі, медсестри, лабтехніки, адміністратори), які по-різному піддаються ризику (наприклад, фінансові відділи, клінічний персонал – при запитах на медичні дані).

Регуляторні наслідки (наприклад, витоки медичної інформації підпадають під жорсткі правила/штрафи) підвищують значущість навіть «незначних» інцидентів.

Дослідження показують, що фішинг і інші соціально-інженерні вектори є одними з найпоширеніших атак в охороні здоров'я; тому модель повинна ставити людський фактор у центр оцінки (навчання, симуляції, тестування) як ключовий контрольний механізм. [7]

Висновки

1 Дослідили специфіку соціальних атак і вразливостей у медичному середовищі

2 Для оцінки ризиків соціальної інженерії у медичній сфері доцільно застосувати змішану методику, яка поєднує процесні підходи ISO/IEC 27005 та NIST SP 800-30 з кількісними механізмами FAIR для окремих, критичних випадків.

3 Людський фактор є центральним елементом моделі ризику; ефективна методика має включати регулярні симуляції фішингу, цільові тренінги, процедури телефонної верифікації та політики BYOD. (Емпіричні дослідження підтверджують ефективність симуляцій у зниженні ризику).

4 Практичне впровадження має бути ітераційним: збір даних → оцінка → впровадження заходів → повторна оцінка. Для переконання керівництва рекомендується використовувати візуалізації (матриці, радарні діаграми) і, при можливості, числові оцінки втрат для обґрунтування інвестицій.