УДК 004.056.5:614

Мельник М.О., Величканич Ю.Ю., Назарова І.М.

[1]Національний університет «Одеська політехніка»

МЕТОДИКИ ОЦІНКИ РИЗИКІВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ У МЕДИЦИНІ

Вступ. У сучасному цифровому середовищі система охорони здоров'я є однією з найуразливіших до кібератак галузей. Це зумовлено значним обсягом оброблюваних персональних і медичних даних, використанням розгалужених інформаційних систем, а також наявністю численного персоналу з різним рівнем цифрової компетентності. В останні роки спостерігається зростання кількості інцидентів, пов'язаних не з технічними вразливостями, а з людським фактором.

Соціальна інженерія (СІ) у сфері медицини - це сукупність методів психологічного впливу, які використовуються зловмисниками для отримання несанкціонованого доступу до даних або інформаційних ресурсів шляхом маніпуляції персоналом. До типових прикладів належать фішингові електронні листи, телефонні дзвінки від «постачальників» або «державних інспекторів», запити від імені адміністрації, підроблені вебпортали систем охорони здоров'я тощо. У результаті таких атак можуть бути порушені конфіденційність, цілісність і доступність медичної інформації, що створює не лише технічні, але й етичні та юридичні наслідки. Саме тому оцінка ризиків СІ є ключовим компонентом системи кіберзахисту медичних закладів

Мета: теоретичний аналіз існуючих методик оцінки ризиків СІ у сфері охорони здоров'я, виявлення їхніх переваг і недоліків, а також формування рекомендацій щодо впровадження комплексного підходу до управління цими ризиками у медичних організаціях.

1. Огляд існуючих рішень для оцінки та проведення тестів соціальної інженерії у медичній сфері

За даними звітів відкритих джерел IBM Security (2024) та Verizon Data Breach Investigations Report (2025), понад 80 % кібератак у сфері охорони здоров'я мають елемент СІ. Основними цілями зловмисників є отримання доступу до електронних медичних карток, облікових записів систем eHealth, лабораторних систем або фінансових даних. Найчастіше атаки здійснюються через фішингові повідомлення, телефонні дзвінки з проханням підтвердити логін або пароль, маніпуляції у месенджерах під виглядом екстрених запитів. Особливістю СІ є те, що основним вектором атаки виступає людський фактор, тому стандартні математичні або технічні моделі оцінки ризиків не є достатньо ефективними без урахування поведінкових характеристик персоналу.

За підходом до аналізу можна виокремити три групи методів:

1. Якісні методи – базуються на експертному аналізі, анкетуванні, самооцінюванні рівня обізнаності співробітників.

2. Кількісні методи – передбачають використання математичних моделей для оцінки імовірності атаки та потенційних втрат.

3. Комбіновані методи – поєднують поведінковий аналіз із кількісною оцінкою.

Далі представимо існуючі методичні підходи до оцінки ризиків у медичних закладах які складаються з наступних етапів:

– ідентифікації ризиків
– аналізу ризиків
– оцінювання рівня ризику
– розробки заходів по зниженню ризиків

Графіки загальної динаміка зростання фішингових/соціоінженерних атак у секторі медицини 2020-2024 рр на рисунку 1

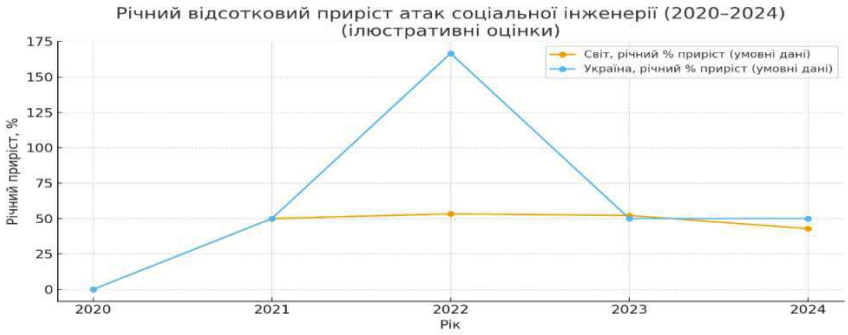

Рисунок 1 - Загальна динаміка зростання фішингових/соціоінженерних

2. Рекомендації щодо вдосконалення оцінки ризиків СІ у медичній сфері

З урахуваннням статистики та ризиків від СІ в медицині рекомендації щодо вдосконалення оцінки ризиків, а саме :

– Інтеграція психологічних індикаторів.
– Регулярне проведення симульованих атак (Phishing Simulation Program) для перевірки готовності персоналу.
– Створення єдиної бази інцидентів СІ, яка дозволяє аналізувати типові сценарії атак.
– Використання систем штучного інтелекту для аналізу листування та виявлення ознак маніпуляцій у реальному часі.
– Розробка національних рекомендацій з урахуванням специфіки медичної сфери України, аналогічних до NIST або NHS Digital Security Guidelines.

Висновок. Методики оцінки ризиків СІ у медицині, повинні враховувати не тільки технічні аспекти, та і психологічну складову, яка є визначальною у таких атаках. Вважаємо, що ефективна система управління ризиками СІ у медичних закладах повинна поєднувати наступне: стандартизовані підходи оцінки, поведінковий аналіз персоналу, постійне навчання і контроль через симуляції, моніторинг індикаторів ризику у динаміці. Застосування інтегрованої методики дозволить не лише зменшити кількість інцидентів, але й підвищити рівень кібергігієни медичного персоналу, сформувати культуру безпечної поведінки та забезпечити стійкість інформаційної інфраструктури медичних установ.

Перелік використаних джерел.

1.Венгерський П.С., Вишневська Н.С., Хохлачова Ю.Є., Хорошко В.О., Чобаль О.І., Кількісна оцінка кіберзахищеності інформації. Захист інформації. – 2023. – Т. 25, №2. – С. 53-61.

2. S.Yevseev, S.Pogasiv O.Shmatko, M. Melnyk Cybersecurity:security of linux operating system / Laboratory workshop, Kharkov, 2021