КОНФІДЕНЦІЙНІСТЬ ДАНИХ У МЕДИЧНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ І ЗАСОБИ ЇЇ ЗАБЕЗПЕЧЕННЯ

Ковальчук В.І.[1], аспірант, vl.i.kovalchuk@gmail.com
[1] Національний Авіаційний Університет, Київ, Україна

Стрімкий розвиток інформаційних технологій, машинного навчання та Інтернету речей останніми роками значно вплинув на розвиток галузі охорони здоров'я. Нові технології та пристрої знаходять все більш широке застосування у клінічній практиці – настільки, що з'явилось визначення Інтернет медичних речей (IoMT). До нього входить широкий спектр приладів і застосунків: системи підтримки або функціональної заміни органів, електронні медичні картки і апарати віддаленого контролю на кшталт інсулінових помп та кардіостимуляторів. Пристрої для моніторингу та догляду все частіше використовують бездротові мережі та мають доступ до локальних мереж лікарень. Імплантовані медичні пристрої можуть підключатися бездротовим способом, щоб оновлюватися, збирати дані та передавати їх постачальнику медичних послуг для моніторингу здоров'я та динаміки пацієнта.

Процес модернізації сфери охорони здоров'я значно пожвавився останніми роками завдяки вищеописаним новаціям. Однак, разом із тим, перед галуззю постали нові виклики щодо конфіденційності і водночас доступності для дослідження великих обсягів персональних даних та біометричної інформації. Сучасна цифрова карта пацієнта містить величезну кількість інформації; від індивідуальних демографічних і контактних даних до конфіденційної медичної інформації, фінансових, страхових даних і деталей соціального забезпечення, документів, що посвідчують особу, і замовлень на рецепти. Очевидно, що такий обсяг інформації потребує багаторівневого захисту, оскільки її витік може призвести до різнопланових негативних наслідків як для пацієнта, так і для всієї галузі. [1]

Окрім фінансових витрат конкретної особи, чиї дані бути атаковані, існує також опосередкований вплив на здоров'я всього населення, яке обслуговує атакована система. Приклад цього впливу було продемонстровано під час атаки програми-вимагача WannaCry 12 травня 2017 року, яка вразила 230 000 систем у понад 150 країнах. У Великій Британії збій спричинив скасування майже 20 000 операцій і коштував майже £92 млн. Населення постраждало негайно і безпосередньо через скорочення доступу до медичної допомоги, скасування записів у клініку, скасування операцій і навіть закриття відділень невідкладної допомоги. [2]

Для протидії подібним інцидентам, а також для збільшення рівня захищеності медичних даних українськими науковцями було запропоновано створення системи захисту інформації в інформаційно-телекомунікаційних медичних системах. Для побудови такої системи необхідно ідентифікувати

загрози та вразливі місця елементів системи, проаналізувати та опрацювати інформаційні ризики з метою управління ними. Ризик інформаційної безпеки було визначено як числову функцію, яка описує ймовірність реалізації загроз інформаційній системі та величину збитків від їх потенційної реалізації внаслідок використання цими загрозами вразливостей елементів системи. В той же час управління ризиками розуміється як безперервний циклічний процес, що включає наступні етапи: ідентифікація ризиків (збір інформації про елементи системи, джерела загроз, класифікацію загроз і вразливих місць; ранжування ризиків); аналіз ризиків (якісний та кількісний підхід до оцінки ризиків); оцінка ризику (процес порівняння кількісно визначеного ризику із заданими критеріями ризику для визначення значущості); обробка та прийняття ризиків. На рис. 1 представлено алгоритм процесу управління ризиками в медичній інформаційній системі.

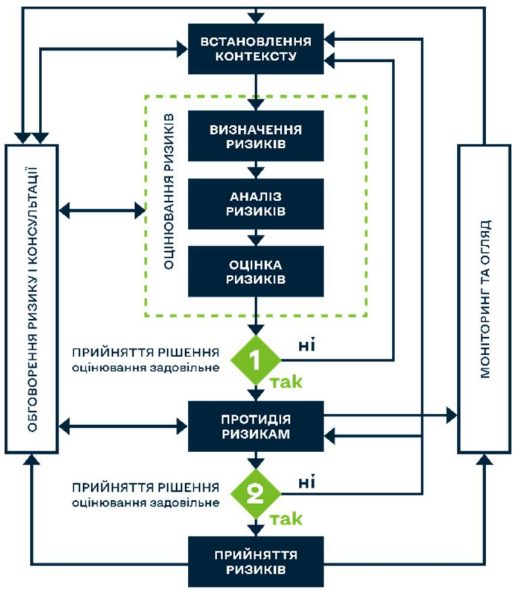

Рисунок 1. Алгоритм процесу управління ризиками медичної інформаційної системи

Від вірної оцінки ризиків суттєво залежить ефективність протидії цим ризикам. Виділяють якісний та кількісний підхід до встановлення значень ризику. Якісний підхід може бути здійснений за допомогою SWOT-аналізу, кількісний результат — статистичним методом, методом Монте-Карло або методом нечітких множин. Після визначення та оцінки конкретного ризику необхідно прийняти рішення щодо його подолання — вибору та впровадження заходів з мінімізації ризику. [3]

Оскільки ризики часто є складними і комплексними, слід окремо розглянути деякі стратегії протидії. Існує парадокс: добре деідентифіковані та очищені медичні дані можуть втратити багато значущої інформації, а збереження великої кількості ключових даних може мати високий ризик порушення конфіденційності. Тому потрібне цілісне рішення, або, інакше кажучи, єдина стратегія.

Для клінічних даних був запропонований підхід, що балансує між керуванням конфіденційністю та вторинним використанням даних – т.зв. «метод Мерфі». Він полягає в тому, щоб узгодити рівень деідентифікації даних із надійністю одержувачів даних. Простіше кажучи, чим більше ідентифікованих даних потрібно надати, тим більш «надійними» повинні бути одержувачі, і навпаки. Рівень довіри до одержувача даних стає критичним фак-

тором у визначенні того, які дані може бачити ця особа. Ця стратегія встановлює п’ять рівнів конфіденційності пацієнтів із трьома аспектами вимог: доступність даних, довіра до дослідника та дослідження та безпека технічних платформ. Рівням конфіденційності відповідають п’ять рівнів користувача: користувач захищених даних(точні дані не надаються), користувач агрегованих даних(дозволені точні цифри зі зведених результатів запиту), користувач даних LDS(доступ до визначених HIPAA LDS, тобто обмеженого набору даних без критичної інформації про пацієнтів), користувач даних LDS із підтримкою Notes (дозвіл на перегляд і зміну текстових нотаток), користувач даних (доступ до всіх даних пацієнта).

Що стосується геномних даних, двома потенційними загрозами конфіденційності є втрата конфіденційності даних про здоров’я пацієнтів через нелегітимний доступ до даних і повторна ідентифікація пацієнтів і, як наслідок, розкриття конфіденційних атрибутів через законний доступ до даних. На основі фреймворку i2b2 було запропоновано застосувати гомоморфне шифрування до першої загрози та диференціальну конфіденційність до другої загрози. Крім того, було розроблено модель системи, що складається з двох фізично розділених мереж, з точки зору архітектури. Ця мережева архітектура спрямована на ізоляцію та відокремлення даних, які використовуються для клінічної/медичної допомоги та які використовуються для дослідницької діяльності уповноваженими особами.

І найбільш новаторська на сьогодні стратегія включає в себе елементи машинного федеративного навчання. Ідея полягає в тому, щоб надавати спільний доступ лише до параметрів моделі замість вихідних даних. Таким чином, багато з цих ініціатив базуються на об’єднаних моделях, у яких фактичні дані ніколи не залишають установу походження, що дозволяє дослідникам обмінюватися моделями без обов’язкового обміну даними пацієнтів. Створення моделей такого типу використовувалося в реальних програмах, де конфіденційність користувачів є вирішальною, наприклад, для даних лікарень або застосунків на мобільних пристроях, і було зазначено, що оновлення моделі вважаються такими, що містять менше інформації, ніж вихідні дані, і завдяки агрегації оновлень з кількох точок даних вихідні дані вважаються неможливими для відновлення. [4]

Загалом, зазначені алгоритми і методи збереження конфіденційних даних в медичних телекомунікаційних системах є свідоцтвом активної участі наукової спільноти у розвитку системи охорони здоров’я. Нехтування інформаційною безпекою тотожне нівелюванню всіх переваги інформаційно-телекомунікаційних медичних технологій, оскільки ступінь інформаційної безпеки залежить від довіри громадян до цих технологій. Саме тому важливо збільшувати активність досліджування даної теми як в Україні, так і в усьому світі.

Література

1. Cartwright, A.J. The elephant in the room: cybersecurity in healthcare. J Clin Monit Comput 37, 1123–1132 (2023). https://doi.org/10.1007/s10877-023-01013-5

2. National Health Executive. WannaCry cyber-attack cost the NHS £92m: вебсайт. URL: https://www.nationalhealthexecutive.com/articles/wannacry-cyber-attack-cost-nhs-ps92m-after-19000-appointments-were-cancelled (дата звернення: 06.04.2023).

3. Shevchenko S., et al. Protection of Information in Telecommunication Medical Systems based on a Risk-Oriented Approach. CPITS 2023: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2023, Kyiv, Ukraine

4. Xiang D, Cai W. Privacy Protection and Secondary Use of Health Data: Strategies and Methods. Biomed Res Int. 2021 Oct 7;2021:6967166. doi: 10.1155/2021/6967166. PMID: 34660798; PMCID: PMC8516535.

Анотація

Представлено алгоритм роботи системи захисту інформації в інформаційно-телекомунікаційних медичних системах. Розглянуті також стратегії протидії ризикам і загрозам конфіденційності даних пацієнта в галузі охорони здоров'я. Серед них виокремлено метод Мерфі, застосування фреймворку i2b2 та метод федеративного навчання.

Ключові слова: конфіденційність, медичні дані, телекомунікації, охорона здоров'я.

Abstract

The algorithm of information protection system operation in information and telecommunication medical systems is presented. Strategies for countering risks and threats to the privacy of patient data in the healthcare industry are also considered. Among them, the Murphy method, the use of the i2b2 framework, and the method of federated learning are singled out.

Keywords: privacy, medical data, telecommunications, healthcare.