4. Gauss elimination: вебсайт. URL: https://www.britannica.com/science/Gauss-elimination (дата звернення: 02.05.2024).

УДК 004.75:004.77: 004.8

Курдупов О. Л., *здобувач 1 курсу спеціальності 122 Комп'ютерні науки,*
Комаров В. Ф., *канд. техн. наук, старший викладач кафедри інформаційних технологій*

ВИКЛИКИ КІБЕРБЕЗПЕКИ У РОЗУМНИХ МЕДИЧНИХ СИСТЕМАХ

Донецький національний університет імені Василя Стуса, м. Вінниця

Сучасні технології, як-от штучний інтелект (AI) та інтернет речей (IoT), революціонізують медичну галузь, втілюючи концепцію смарт-медицини. Однак інтеграція цих технологій приносить нові виклики у сфері кібербезпеки. Дослідження зосереджується на аналізі викликів безпеки в системах, що використовують технології штучного інтелекту та інтернету речей (AIoT), і методах захисту даних у смарт-медицині.

Труднощі, з якими стикається медичний бізнес, впливають на стандарти лікування пацієнтів. Штучний інтелект у поєднанні з IoT може автоматизувати моніторинг стану здоров'я, оптимізувати роботу медичного персоналу та вдосконалити управління обслуговуванням пацієнтів. AIoT обіцяє трансформувати охорону здоров'я, забезпечуючи точнішу діагностику та персоналізоване лікування.

Для вирішення проблем, підвищення надійності та ефективності системи охорони здоров'я починають використовуватись технології Internet of Medical Thing (IoMT). Наприклад, носимі пристрої можуть надсилати дані про серцевий ритм та активність пацієнта безпосередньо до хмарної платформи для аналізу. Інформація про пацієнтів зберігається в хмарному центрі обробки даних або базі даних. До того ж хмара забезпечує доступ до численних медичних спеціалістів, наприклад до тих, хто проводить медичну діагностику для лікування пацієнтів [1]. Також додатки для охорони здоров'я дають змогу здійснювати віддалений моніторинг за допомогою інтелектуальних пристроїв, як-от смартфони та переносні сенсорні пристрої [2]. Традиційні способи догляду за пацієнтами швидко змінюються завдяки смарт-технологіям.

Однак із розширенням мережі IoT та збільшенням обсягу чутливих медичних даних зростає й потенціал кібератак. Відтак головною проблемою стає забезпечення надійності та конфіденційності медичних даних у розумних медичних системах. Без адекватних заходів безпеки така інтеграція вразлива до порушень даних.

Типовими задачами кібербезпеки у галузі застосування є:

1. Доступність даних: забезпечення безперервного доступу до медичних даних у разі кібератаки є критично важливим для здоров'я пацієнтів.

2. Конфіденційність: неавторизований доступ до медичних даних може призвести до порушення приватності та довіри пацієнтів.

3. Цілісність даних: неправдива інформація внаслідок злому може призвести до неправильного лікування, наражаючи пацієнтів на ризик.

Функції зберігання даних включають зберігання структурованих даних, відеоданих, даних зображень і напівструктурованих даних. Основними проблемами управління даними є індексація, об'єднання, аналіз і візуалізація даних. Важливо відокремлювати та шифрувати конфіденційні дані, а також контролювати доступ, керувати дозволами, робити резервні копії, відновлювати дані та зберігати журнали аудиту [3].

Забезпечити конфіденційність і безпеку даних складно, коли в системі наявний великий обсяг чутливої інформації. Переважна більшість медичного обладнання є вразливою до хакерських атак. IoMT може зберігати записи пацієнтів, контакти та інші клінічні записи, а це безліч пристроїв, наповнених клінічними даними. Медична карта пацієнта вразлива до можливості розголошення через недостатній або неактуальний рівень заходів безпеки.

Рішення IoMT повинні також враховувати загрози, які вони несуть не тільки пацієнтам, але й фінансовій підсистемі медичних установ [4].

Питання спільного використання даних завжди серйозні та мають всебічний вплив на конфіденційність і безпеку як системи, так і всіх зацікавлених сторін. Розмежування та спільне використання даних у смарт-системах є складною задачею в екосистемі AIoT через обсяг даних, що генерується сенсорними пристроями, постійний зв'язок між пристроями в системі та потребу в поєднанні інформації від пацієнтів для розкриття потенціалу смарт-систем [5].

Перспективною є рекомендація використання сучасних криптографічних методів, як-от шифрування даних, у поєднанні з технологіями блокчейн. Це може значно підвищити безпеку систем AIoT та IoMT. Імплементація стандартів і протоколів може вирішити багато зазначених проблем. Важливим в умовах швидкого розвитку смарт-технологій є також впровадження регулярних аудитів безпеки та навчання й актуалізація знань персоналу.

AIoT представляє величезні можливості для смарт-медицини, але супроводжується ризиками у сфері кібербезпеки. Розробка і реалізація комплексних стратегій захисту даних є ключовими для забезпечення успіху цих технологій у майбутньому.

Список використаних джерел

1. Privacy in the internet of things for smart healthcare / D. He, R. Ye, S. Chan, M. Guizani, and Y. Xu. *IEEE Communications Magazine*. 2018. Vol. 56, № 4.

2. Enabling Artificial Intelligence of Things (AIoT) / A. A. Pise, K. K. Almuzaini, T. A. Ahanger, A. Farouk, K. Pant, P. K. Pareek. *Healthcare Architectures and Listing Security Issues.* 2022. DOI: 10.1155/2022/8421434.

3. Artificial Intelligence of Medical Things for Medical Information Systems Privacy and Security / M. Abdulraheem, E. A. Adeniyi, J. B. Awotunde, A. L. Imoize, R. G. Jimoh, I. D. Oladipo, P. B. Falola. 2023. eBook ISBN9781003370321.

4. Al and IoT Enabled Smart Hospital Management Systems / M. K. Gourisaria, R. Agrawal, V. Singh, S. S. Rautaray, M. Pandey. 2022.

5. Ghosh A., Chakraborty D., Law A. Artificial intelligence in Internet of Things. *CAAI Trans.* Intell. Technol. 2018.