УДК 004.738

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ОРГАНІЗАЦІЇ ОБМІНУ ТА ЗАХИСТУ ПЕРСОНАЛЬНОЇ ІНФОРМАЦІЇ У МЕДИЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Зандер К.Ю., PhD аспірант, 8390983@stud.nau.edu.ua , НАУ
Гнатюк В.О., к.т.н, доцент, viktor.hnatiuk@npp.nau.edu.ua, НАУ, ДЕРЖНДІ ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

Впровадження медичних інформаційних систем (МІС) у лікарнях було обумовлено появою можливості отримання різноманітних даних про пацієнта в цифровому вигляді, а в подальшому для автоматизації процесу зберігання та доступу медичного персоналу лікарні до цих даних. Разом з цим з перших днів використання таких МІС, активна увага приділяється задачам надійного збереження інформації про пацієнтів, швидкого доступу та можливості взаємообміну даними для медичного персоналу лікарень, проведення статистичних аналізів зведених даних [1].

Починаючи з 2010 року стався активний розвиток МІС в наслідок чого до 2023 року було розроблено та впроваджено більше шести тисяч різноманітних МІС у світі. Також за останні роки суттєво збільшився обсяг даних, якими мають оперувати сучасні МІС.

Цей розвиток повністю змінив систему охорони здоров'я у більшості країн та став причиною розширення можливостей та функціоналу МІС, які на початку використовувалися для локальних потреб лікарні чи групи лікарень, а зараз потребують організацію обміну даних між лікарнями різних міст чи навіть країн. Паралельно у світі формувалися та гармонізувалися вимогти до технології передачі, захисту, анонімізації персональних даних.

На думку провідних розробників МІС, використання штучного інтелекту (ШІ) дає можливість значно прискорити та покращити процес безпечної інтеграції різних систем та пристроїв.

Побудована па платформі UNITY цифрова медична екосистема ALQNET, яку впроваджують з січня 2020 року у клініці Шаріте (Германія), використовує ШІ для забезпечення чіткого структурованого керування доступом. Така система надає диференційований доступ до персональних даних пацієнтів, враховуючи роль користувача (рис. 1 [2]).

Для підвищення надійності роботи системи, за допомогою ШІ, медичні дані перед завантаженням у хмарне сховище аналізуються, деідентифікуються та пов'язуються з пацієнтом за допомогою «псевдоніму». Завантаження та вивантаження даних відбувається за допомогою зашифрованих протоколів обміну між користувачами системи. Ця система сертифікована відповідно до стандартів управління інформаційною безпекою (ISO) 27001 та ISO 13485 та

відповідає вимогам регламенту ЕС із захисту персональних даних GDPR (General Data Protection Regulation), Google Cloud Platform (GCP) і Закону про перенесення та підзвітність медичного страхування (HIPAA).

Також використані алгоритми штучного інтелекту проходять регулярний внутрішній контроль щодо дійсності алгоритмів і цілісності отриманих даних [2].

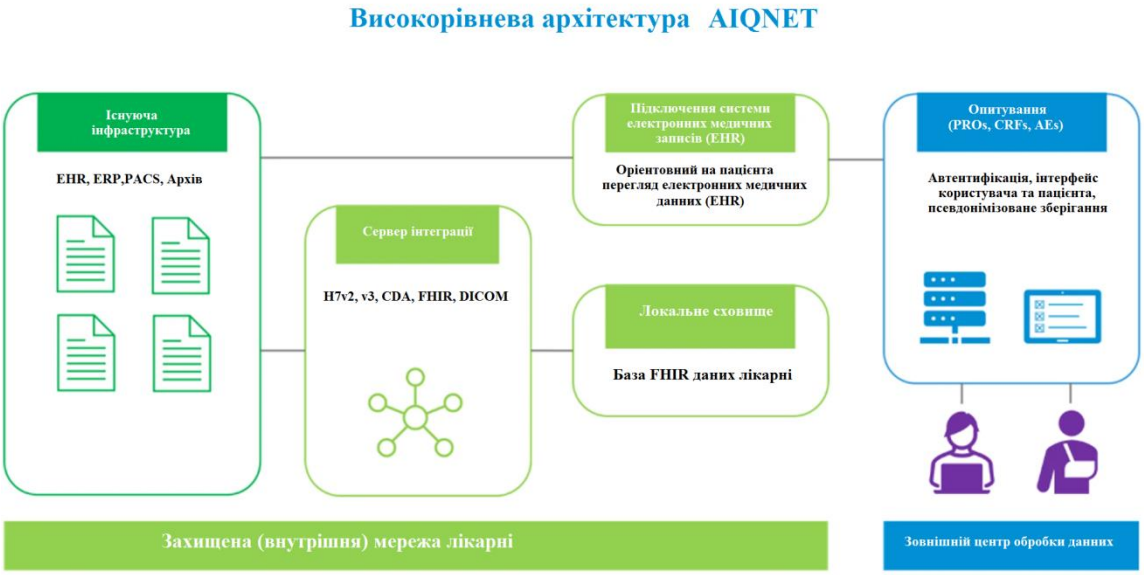

Рисунок 1 – Побудова архітектури медичної системи AIQNET

Як бачимо на прикладі ALQNET використання ШІ у МІС зараз як правило обумовлено необхідністю організації швидкого доступу різноманітних перевірених користувачів до даних про пацієнта, а також захисту даних при завантаженні-вивантаженні з системи. Для забезпечення надійності передачі та захисту даних зараз використовують різноманітні розроблені технології цифрового шифрування такі як Rivest-Shamir-Adleman (RSA), стандарт шифрування даних (DES) і розширений стандарт шифрування (AES) [3].

Метод RSA–це асиметричний алгоритм шифрування, у якому використовується велика довжина секретних ключів у двійковому форматі яка має вищій рівень безпеки, при цьому секретні ключі не потрібно передавати авторизованим користувачам з відкритими ключами. Такі схеми криптографії на основі RSA можуть застосовуватися наприклад, для автенфікації цифрового підпису. DES являє собою блочно-симетричний алгоритм шифрування, який шифрує та розшифровує цифрові данні за допомогою перестановки, заміни та транспонування даних. AES – також є симетричним алгоритмом шифрування, який застосовує операції підстановки, зміщення рядків змішування стовпців. Процес дешифрування для цього алгоритму діє у зворотному порядку.

Доповнення цих методів шифрування додатками ШІ з застосуванням алгоритмів машинного навчання та глибокого навчання роблять їх більш швидкими з точки зору обчислювальних операції, безпечним та ресурс ефективним [3].

Групою вчених Національного технологічного університету Chin-Yi, Тайвань, було створено модель медичної системи з використання ШІ для шифрування дешифрування персональних даних пацієнтів, а також отриманих діагностичних цифрових зображень з медичного обладнання.

Процес шифрування-дешифрування було реалізовано у два етапи:

Перший етап криптографічний – за допомогою комбінації хаотичної карти та генератора ключів на основі квантової системи. Це було необхідно для отримання дворaундних псевдовипадкових 256-бітних невпорядкованих та неповторюваних випадкових чисел, які використовували для вибору секретних ключів процесів шифрування та дешифрування.

Другий етап - використання алгоритмів машинного навчання і глибокого навчання шифратора та дешифратора на основі методу перестановки та методу заміни, для підвищення рівня складності протоколів криптографії.

Результати тестування такої моделі медичної системи показали, що при запропонованому методі шифрування та дешифрування медичної інформації, користувачі, після дешифрування отримували данні які відповідно до міжнародних вимог, майже на 100% були наближені до первинних цифрових зображень, чи інших цифрових даних отриманих з медичного обладнання [3].

Висновок. Використання штучного інтелекту у поєднанні з класичними методами та стандартами шифрування даних стає все більше поширеним явищем у медичних системах закладів охорони здоров’я, які оперують великими обсягами медичних персональних даних та мають надавати різнорівневий доступ до цих даних користувачам. Результати різноманітних досліджень та експериментів показують, що таке поєднання не призводить до критичних втрат інформації та може застосовуватися не тільки для зберігання чи передачі персональних даних пацієнта у зашифрованому вигляді, а і безпосередньо медичних зображень та даних отриманих від медичного обладнання в процесі діагностик стану пацієнта.

Список використаних джерел

1. Качмар В.О. "Медичні інформаційні системи – стан розвитку в Україні" Український журнал телемедицини та медичної телематики 8,№ 1 (2010): 12-17.
2. Putzier M , Khakzad T, Dreischarf M *et al.* Implementation of cloud computing in the German healthcare system. *Npj Digit. Med.* **7**, 12 (2024). https://doi.org/10.1038/s41746-024-01000-3.
3. P.Y. Chen *et al.*, "Information Security and Artificial Intelligence–Assisted Diagnosis in an Internet of Medical Thing System (IoMTS)," in *IEEE Access*, vol. 12, pp. 9757-9775, 2024, doi: 10.1109/ACCESS.2024.3351373.