УДК 004.056

Гнєдова В.О., Вінковська І.С.

Національний університет «Одеська політехніка»

КРИПТОГРАФІЧНИЙ ЗАХИСТ DICOM–ЗОБРАЖЕНЬ: ПРОБЛЕМИ, РИЗИКИ ТА НАПРЯМИ РОЗРОБКИ ПРОГРАМНИХ ЗАСОБІВ

Вступ. Сучасна медицина активно використовує цифрові технології для діагностики, зокрема медичні зображення, які зберігаються та передаються у форматі DICOM (Digital Imaging and Communications in Medicine). Цей стандарт забезпечує обмін результатами різних обстежень – комп'ютерної томографії, магнітно-резонансної томографії, ультразвукових досліджень та інших. Зростання обсягів медичних даних підвищує ефективність діагностики та лікування, але водночас створює серйозні ризики для конфіденційності та цілісності інформації. Несанкціонований доступ до медичних зображень може призвести до порушення прав пацієнтів, маніпуляцій із результатами досліджень і юридичних наслідків для медичних установ.

Мета: Проаналізувати проблеми криптографічного захисту медичних зображень у форматі DICOM. У роботі досліджуються вразливості медичних зображень під час зберігання та передачі, сучасні методи забезпечення конфіденційності, цілісності та автентичності DICOM–файлів, а також виявляються ключові проблеми й ризики для медичних закладів і пацієнтів.

1. Проблематика зберігання та передачі DICOM–зображень

Файли DICOM містять не лише медичні зображення, але й метадані пацієнта, які включають особисту інформацію та діагностичні відомості. Це робить їх особливо цінними й водночас уразливими до різного роду загроз. Однією з ключових проблем є несанкціонований доступ: у деяких медичних системах відсутні ефективні засоби шифрування, що дозволяє стороннім особам переглядати конфіденційні дані. Витік інформації може відбутися під час передачі DICOM-файлів через мережі з низьким рівнем захисту, створюючи ризик перехоплення або підміни даних. Крім того, можливі спроби модифікації файлів, коли зміни в зображеннях або метаданих спотворюють діагностичну інформацію, що критично для точності медичних висновків. Тому забезпечення надійного захисту DICOM–зображень є надзвичайно актуальним завданням у сучасній електронній медицині [1].

2. Методи криптографічного захисту

Криптографічні методи відіграють ключову роль у забезпеченні безпеки медичних даних, гарантують їх конфіденційність, цілісність та автентичність. Конфіденційність досягається шляхом шифрування даних, цілісність – контролем змін після створення чи передачі, а автентичність – підтвердженням походження даних від надійного джерела [2].

Серед сучасних підходів виділяють симетричне шифрування (AES, DES), що є швидким і ефективним, але вимагає безпечного обміну ключами, і асиметричне шифрування (RSA, ECC), яке забезпечує безпечну передачу ключів, але має меншу швидкодію при великих обсягах даних. Цифрові підписи та хеш–

функції (SHA–256) дозволяють перевіряти цілісність файлів і підтверджувати їх достовірність [2]. Водночас багато медичних систем досі не інтегрують повноцінні криптографічні засоби, що створює реальні ризики для безпеки даних пацієнтів.

У подальших дослідженнях планується розробити програмний застосунок, який реалізовуватиме комбінований підхід до шифрування DICOM–зображень, забезпечуючи безпеку та швидкість одночасно.

3. Аналіз проблем та ризиків

Основними проблемами безпеки DICOM–зображень є:

– недостатня стандартизація криптографічного захисту у DICOM–системах, що призводить до різного рівня безпеки серед виробників;

– складність інтеграції криптографічних засобів у медичні процеси, адже лікарі потребують швидкого доступу до зображень;

– людський фактор – помилки персоналу при керуванні ключами або налаштуванні систем;

– відсутність контролю автентичності при передаванні файлів через відкриті мережі, що може призвести до непомітної підміни даних [3].

Отже, існує потреба у комплексному підході до захисту DICOM–зображень, який поєднує технічні та організаційні заходи безпеки. Особливо важливо забезпечити створення програмних інструментів, здатних автоматизувати процеси шифрування, перевірки цілісності та автентифікації файлів, мінімізуючи вплив людського фактора.

Висновок. Аналіз проблем криптографічного захисту медичних зображень показує, що забезпечення конфіденційності, цілісності та автентичності DICOM–файлів є ключовим завданням сучасної електронній медицині. Виявлені проблеми – недостатня стандартизація шифрування, складність інтеграції криптографії у медичні процеси, ризики, пов'язані з людським фактором, та відсутність контролю автентичності при передачі даних – свідчать про високий рівень потенційних загроз. Це підкреслює необхідність комплексного підходу, який включає впровадження криптографічних технологій, політик управління доступом і навчання персоналу. Такий підхід підвищить рівень захисту медичних даних, зменшить ризики витоку інформації та сприятиме достовірності діагностичних процесів.

Перелік використаних джерел.

1. Medcrypt. "Чому захищений DICOM погано впроваджується: аналіз проблем." 2021. [Електронний ресурс]. – Режим доступу: https://www.medcrypt.com/blog/why-secure-dicom-is-poorly-accepted-understanding-the-challenges

2. Рахман, А. А. Т., Іслам, М. М., & Хоссайн, М. А. "Захист медичних зображень у телемедицині: систематичний огляд." 2022. [Електронний ресурс]. – Режим доступу: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8938747/

3. Бернс, Е. С., & Брейнінг, Р. Дж. "Безпека даних пацієнта та досліджень у DICOM-зображеннях." 2010. [Електронний ресурс]. – Режим доступу: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3043670/