

Секція 1

**МЕТОДИ І ТЕХНОЛОГІЇ КІБЕРБЕЗПЕКИ ДЛЯ ЗАХИСТУ
ОНЛАЙН-СЕРВІСІВ ОБРОБКИ МЕДИЧНИХ ЗОБРАЖЕНЬ**

Рябко І. Б.

Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Харченко В.С.

Актуальність. Сучасні медичні онлайн-сервіси для обробки зображень (СОЗ) полегшують діагностику, але їхній розвиток супроводжується різноманітними загрозами кібербезпеки. Недоліком відомих публікацій є те, що вони зосереджуються на окремих аспектах кібербезпеки, не пропонуючи комплексних рішень для СОЗ.

Мета роботи. Оцінювання поточних методів і технологій кібербезпеки для захисту медичних онлайн-сервісів, виявлення основних загроз, аналіз контрзаходів та розроблення рекомендацій щодо підвищення рівня безпеки СОЗ.

Основні положення. Фішинг та соціальна інженерія. Фішинг-атаки на співробітників спрямовані на отримання доступу до конфіденційної інформації та ресурсів, що може призвести до масштабних витоків даних. DDoS-атаки. DDoS-атаки ускладнюють роботу онлайн-сервісів через перенасичення запитами, що може призвести до збоїв у роботі системи або її тимчасової недоступності для користувачів [1]. Вразливості програмного забезпечення. Уразливості, такі як SQL-ін'єкції та атаки типу XSS, часто використовуються для отримання несанкціонованого доступу до конфіденційних даних у недостатньо захищених системах [2]. Недостатній контроль доступу. Недостатньо налаштовані права доступу до чутливих даних або їхня відсутність створюють ризик несанкціонованого доступу до медичних даних, що може призвести до витоків інформації. Відсутність або недостатнє шифрування даних. Незашифровані дані під час передачі між серверами та клієнтами можуть бути перехоплені зловмисниками, що становить серйозну загрозу для конфіденційності медичної інформації [2]. Далі представлено методи захисту та рекомендації щодо їх вибору. Шифрування даних. Рекомендується використовувати AES для шифрування медичних даних, з можливістю застосування стеганографії для приховування інформації. Також слід використовувати SSL/TLS для захищених з'єднань, що знижує ризик перехоплення [3]. Моніторинг мережових аномалій. Штучний інтелект для аналізу трафіку допомагає виявляти загрози, як-от DDoS-атаки або фішинг, і забезпечує швидке

реагування [4]. Багатофакторна аутентифікація (2FA). Впровадження 2FA знижує ризик компрометації облікових записів [5]. Резервне копіювання і відновлення. Регулярне шифроване резервне копіювання та тестування відновлення знижують ризики втрати даних через кіберінциденти або технічні збої [2]. Впровадження політик доступу. Застосування принципу найменших привілеїв для доступу до даних та регулярне оновлення політик доступу знижує ризик внутрішніх загроз [5].

Висновки. Інтегровані методи захисту, такі як шифрування, стеганографія, багатофакторна аутентифікація та моніторинг загроз, знижують ймовірність витоків медичних зображень і забезпечують високий рівень кібербезпеки в онлайн-сервісах, відповідаючи міжнародним стандартам (GDPR, HIPAA).

Список літератури

1. DDoS Protection and Security Solutions. *Cloudflare*. URL – <https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack> (дата звернення 11.11.24).
2. National Institute of Standards and Technology (NIST). *Advanced Encryption Standard (AES)*. NIST FIPS PUB 197, Published November 26, 2001; Updated May 9, 2023.
3. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446. URL – <https://datatracker.ietf.org/doc/html/rfc8446> (дата звернення: 11.11.2024).
4. General Data Protection Regulation (GDPR). *GDPR*. URL – <https://gdpr-info.eu> (дата звернення: 11.11.2024).
5. Summary of the HIPAA Security Rule. *U.S. Department of Health and Human Services*. URL – <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html> (дата звернення: 11.11.2024).

Відомості про авторів

Рябко Іван Богданович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», i.b.ryabko@student.csn.khai.edu

Харченко Вячеслав Сергійович, завідувач кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., професор, v.kharchenko@csn.khai.edu