УДК 621.397

П.О. Яковишен
С.Є. Тужанський

СТРАТЕГІЇ ТА ТЕХНОЛОГІЇ ЗАХИСТУ ДАНИХ У ТЕЛЕМЕДИЧНИХ СИСТЕМАХ

Вінницький національний технічний університет

Анотація. *Телемедицина, яка об'єднує технології з медичною практикою, відкриває двері до нових можливостей у наданні медичної допомоги на відстані, зменшуючи географічні та часові обмеження. Проте перехід до дистанційного збирання, обробки, передавання та зберігання медичних даних створює нові виклики у забезпеченні безпеки та конфіденційності інформації. Захист даних в телемедичних системах є невід'ємною складовою у забезпеченні конфіденційності, цілісності та доступності медичної інформації. У роботі розглянуто типові загрози, яким піддаються дані в телемедичних системах, описуються стратегії та технології захисту, здійснено аналіз перспектив розвитку захисту даних у телемедицині, які охоплюють широкий спектр інноваційних технологій та стратегій.*

Ключові слова: телемедична система, передавання даних, захист інформації.

Abstract. *Telemedicine, which combines technologies with medical practice, opens the door to new opportunities in providing medical care at a distance, reducing geographical and time restrictions. However, this transition to remote collection, processing, transmission and storage of medical data also creates new challenges in ensuring the safety and privacy of this data. Protection of data in telemedicine systems is an integral part of the confidentiality, integrity and accessibility of medical information. This paper deals with the typical threats that are subject to data in telemedicine systems, describes data protection strategies and technologies, as well as analyze the prospects for data protection development in telemedicine, which cover a wide range of innovative technologies and strategies.*

Keywords: telemedicine system, data transmission, data protection.

Важливість захисту інформації у телемедицині не може бути переоцінена, оскільки ця сфера займає центральне місце в сучасній медичній практиці. По-перше, медична інформація є найбільш конфіденційною та особистою для пацієнтів [1]. Будь-яке порушення цілісності і конфіденційності таких даних може призвести до серйозних наслідків для пацієнтів, включаючи витік особистої та медичної інформації, можливість шантажу, порушення медичної приватності та навіть ідентифікаційну крадіжку. По-друге, захист даних у телемедицині має важливе значення для забезпечення довіри між пацієнтами та медичними працівниками. Пацієнти мають право на конфіденційність власної медичної інформації, будь-яке порушення такого права підриває довіру до медичної системи в цілому. Крім того, захист даних в телемедицині є ключовим елементом відповідності законодавчим та регулятивним вимогам у сфері зберігання та обробки медичної інформації, таким як Закони про захист персональних даних [2], Про схвалення Стратегії розбудови телемедицини в Україні [3], Закон про медичний резерв (HIPAA), який діє в США [4], та Загальний регламент про захист даних (GDPR), який діє в Європейському Союзі тощо [5].

Основні типи загроз. На сьогодні, найтиповішими загрозами безпеці даних в телемедичних системах є:

- кібератаки, які можуть здійснюватись з метою витягнення конфіденційної медичної інформації (наприклад, злам системи для доступу до медичних записів), порушення цілісності (модифікація медичної інформації) або знищення даних. Кібератаки можуть включати вірусне або шкідливе програмне забезпечення, фішинг, атаки відмови в обслуговуванні (DDoS) тощо;
- витік даних, що може бути результатом несанкціонованого доступу до системи або людського фактору (наприклад, втрата медичного пристрою або недбале використання інформації). Витік даних може призвести до серйозних порушень приватності пацієнтів та порушення законодавчих вимог щодо захисту особистої інформації;
- недостатня безпека мережі: несанкціонований доступ до мережі та недостатня захищеність мережевих пристроїв можуть призвести до порушення безпеки даних. Наприклад, не захищені Wi-Fi мережі можуть стати вразливими перед атаками зовнішніх зловмисників;
- несправність систем та програмного забезпечення: недоліки у програмному забезпеченні або обладнанні можуть призвести до ненавмисних витоків даних або їх втрати. Це може стати наслідком помилок у програмному коді, недостатньої тестування або використання застарілих версій програмного забезпечення;
- людський фактор, який може бути слабким місцем у захисті даних. Наприклад, атаки фішингу, коли зловмисник використовує маніпуляції для отримання доступу до конфіденційної інформації через соціальний інжиніринг або психологічний тиск на працівників [6].

Ці загрози підкреслюють важливість ретельного захисту даних у телемедицині та необхідність розроблення комплексної стратегії кібербезпеки для забезпечення безпеки та конфіденційності медичної інформації в усіх телемедичних системах.

Стратегії захисту даних в телемедицині. Основні стратегії, які потрібно використовувати для захисту даних у телемедицині:

- шифрування даних для перетворення інформації у криптографічно захищену форму, яка може бути розшифрована тільки з використанням спеціального ключа. Використання шифрування даних для збереження та передачі медичної інформації забезпечує додатковий рівень захисту від несанкціонованого доступу;
- мережеві заходи безпеки, до яких відноситься: застосування захищених мережевих протоколів, мережевого моніторингу та виявлення вторгнень (IDS/IPS), застосування брандмауерів та інших заходів для запобігання несанкціонованому доступу до медичних даних через мережу [7];
- аутентифікація та авторизація. Використання сильних методів аутентифікації, таких як двофакторна або біометрична аутентифікація, дозволяє переконатися, що тільки авторизовані користувачі мають доступ до медичної інформації. Крім того, системи повинні мати гнучкі механізми авторизації, щоб обмежити доступ користувачів до лише необхідної для них інформації;
- фізична безпека пристроїв, на яких зберігається та (або) обробляється медична інформація, що може включати в себе застосування захищених серверних приміщень, контроль доступу до пристроїв та моніторинг роботи обладнання;
- регулярне навчання персоналу: медичний персонал повинен усвідомлювати всі потенційні загрози безпеці даних та має бути навченим їх запобіганню завдяки регулярному навчанню з кібербезпеки, розумінню процедур роботи з конфіденційною інформацією та відповідальністю за захист даних.
- використання штучного інтелекту (AI) та машинного навчання (ML) для виявлення аномальних патернів у доступі до даних та розпізнавання підозрілих активностей, що допомагає вчасно виявляти та реагувати на потенційні загрози безпеки;
- використання блокчейн технологій, що можуть забезпечити безпеку та недоступність для змін даних, що зберігаються в телемедичних системах.

Ці стратегії є лише кількома засобами захисту даних та зображень у телемедицині. Щоб забезпечити повну захищеність медичних даних, важливо розробляти комплексні підходи до кібербезпеки, які враховують усі аспекти технічної, організаційної та людської безпеки даних.

Фізична безпека та контроль доступу. Фізична безпека даних та контроль доступу в телемедичних системах є критичними аспектами загальної стратегії безпеки даних, яким необхідно приділити окрему увагу. Ці заходи доповнюють технічні та організаційні заходи захисту, щоб забезпечити повну захищеність медичної інформації в цьому цифровому середовищі. Ключовими аспектами такого комплексу захисту даних є:

- захищене розташування серверних центрів: фізичне розташування серверних центрів, де зберігається медична інформація, повинно бути обладнане відповідними заходами безпеки. Це може включати в себе застосування біометричних систем контролю доступу, відеоспостереження, фізичні бар'єри та інші заходи захисту;
- контроль доступу до пристроїв: крім фізичної безпеки центрів обробки даних, важливо також контролювати доступ до конкретних пристроїв, на яких зберігається та (або) обробляється медична інформація. Це може бути досягнуто за допомогою аутентифікації, паролів, карток доступу або біометричних методів ідентифікації;
- захищені пристрої для доступу до даних: користувачам, які мають доступ до медичної інформації через телемедичні системи, повинні бути надані захищені пристрої, які відповідають вимогам безпеки. Наприклад, застосування шифрування даних на пристроях, використання безпечних мобільних платформ та обмеження можливостей зберігання даних на пристроях;
- моніторинг та аудит доступу до даних, що включає в себе ведення журналів доступу до даних, виявлення незвичайних або підозрілих активностей та вживання заходів для їх усунення;
- фізичні заходи безпеки під час передачі даних: Під час передачі медичної інформації через мережі важливо забезпечити фізичну безпеку цього процесу. Це може включати в себе використання шифрування даних, встановлення захищених мережевих тунелів та застосування протоколів безпеки мережі, таких як VPN (віртуальна приватна мережа) [8].

Перспективи і напрямки розвитку захисту даних в телемедичних системах охоплюють широкий спектр інноваційних технологій та стратегій, спрямованих на поліпшення захисту конфіденційності, цілісності та доступності медичної інформації. Основними ключовими напрямками розвитку захисту інформації в галузі телемедицини сьогодні є такі:

1) Інтеграція новітніх технологій. Розвиток і впровадження передових технологій, таких як штучний інтелект, блокчейн, квантові обчислення та інші, можуть зробити захист даних у телемедичних системах більш ефективним та надійним. Наприклад, застосування штучного інтелекту для аналізу поведінки користувачів та виявлення аномальних активностей може допомогти у вчасному виявленні потенційних загроз;

2) Посилення кіберзахисту медичних пристроїв IoT. З розвитком Інтернету речей (IoT) у сфері телемедицини стає критично важливим забезпечення безпеки цих пристроїв. Поглиблене дослідження та

розробка захисту для медичних пристроїв IoT, таких як медичні сенсори та зв'язані з ними мережі, є ключовим напрямком розвитку;

3) Створення глобальних стандартів та регуляцій. Розробка та впровадження єдиної нормативно-правової бази, що стосується захисту даних у телемедицині, може допомогти забезпечити єдність підходів до захисту інформації та зробити процес більш прозорим і передбачуваним;

4) Удосконалення процесів аутентифікації та авторизації. Розвиток нових методів аутентифікації, таких як біометричні технології та мультифакторна аутентифікація, може зробити процес входу в систему більш безпечним та зручним для користувачів;

5) Посилення свідомості про кібербезпеку. Важливим аспектом є навчання медичного персоналу та пацієнтів основам кібербезпеки, включаючи виявлення фішингових атак, збереження безпеки паролів та розпізнавання підозрілих активностей в мережі;

6) Розробка гнучких та масштабованих систем захисту для можливості їх ефективного впровадження в телемедичні системи різних конфігурацій та масштабів.

Висновки

Отже, захист даних в телемедичних системах є важливим аспектом забезпечення конфіденційності, цілісності та доступності медичної та персональної інформації. Зростання використання телемедицини вимагає посилення заходів безпеки для запобігання несанкціонованому доступу, зловживанню та кібератакам.

Здійснено аналіз типових загроз та стратегій захисту даних в телемедичних системах, на основі якого можна зробити висновок, що ефективний захист даних в телемедицині можна забезпечити шляхом комплексного підходу, який включає в себе як технологічні, так і організаційні аспекти. Також визначено напрямки розвитку безпеки даних в телемедичних системах, які включають в себе інтеграцію передових технологій, посилення кіберзахисту медичних пристроїв IoT, створення глобальних стандартів та регуляцій, удосконалення процесів аутентифікації та авторизації, а також підвищення свідомості про кібербезпеку. Розвиток гнучких та масштабованих систем захисту дозволить ефективно впроваджувати ці стратегії у телемедичні системи будь-яких конфігурацій.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. A. Gusarova. Data protection in telemedicine. SHS Web of Conferences, 2 (2012) 00013. Published online: 2012-10-17. URL: https://doi.org/10.1051/shsconf/20120200013

2. Про захист персональних даних. *Офіційний вебпортал парламенту України.* URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

3. Про схвалення Стратегії розбудови телемедицини в Україні. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/625-2023-р#Text

4. Стандарт конфіденційності інформації про здоров'я HIPAA. URL: https://whatishipaa.org/

5. Регламент ЄС про захист даних GDPR. URL: https://gdpr-text.com/uk/

6. Дудикевич В. Б., Хорошко В.О., Яремчук Ю.Є. Основи інформаційної безпеки: навч. пос. Вінниця : ВНТУ, 2018. 82-89 с.

7. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Інформаційна безпека в комп'ютерних мережах : навч. посіб. Кропивницький: Видавець Лисенко В. Ф., 2020. 138-152 с.

8. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. К.: КУБГ, 2019. 132 с.

Яковишен Павло Олександрович - аспірант кафедри біомедичної інженерії та оптико-електронних систем, Вінницький національний технічний університет, м. Вінниця, yakovishen3@gmail.com.

Тужанський Станіслав Євгенович – к.т.н, доцент кафедри біомедичної інженерії та оптико-електронних систем, Вінницький національний технічний університет, slavat@vntu.edu.ua.

Yakovyshen Pavlo Oleksandrovych - Postgraduate student, Department of Biomedical Engineering and Optoelectronic Systems, Vinnytsia National Technical University, Vinnytsia, yakovishen3@gmail.com.

Tuzhanskyi Stanislav Yevhenovych - Candidate of Technical Sciences, Associate Professor, Department of Biomedical Engineering and Optoelectronic Systems, Vinnytsia National Technical University, slavat@vntu.edu.ua.