УДК 004.056.53

ПРОБЛЕМЫ АУТЕНТИФИКАЦИИ И ВОЗМОЖНЫЕ ПУТИ РЕШЕНИЯ В СИСТЕМАХ МЕДИЦИНСКИХ ДАННЫХ

Голованёв А.В. (ИТМО),
Научный руководитель – кандидат технических наук, доцент Коржук В. М. (ИТМО)

Введение. В современных условиях ускоряющейся цифровизации здравоохранения всё чаще обсуждается вопрос безопасности медицинских данных. С каждым годом растет количество устройств, взаимодействующих с медицинскими данными не только в медицинских учреждениях, но и за их пределами через сеть интернет. Возможность получения, использования и хранения информации в системах медицинских данных напрямую связано с аутентификацией пользователей. В статье не только обсуждаются актуальные проблемы аутентификации в системах обработки медицинских данных, такие как несанкционированный доступ, угрозы кибербезопасности и недостатки существующей законодательной базы как в РФ, так и в других странах. Но и предлагаются возможные пути решения, включающие внедрение многофакторной аутентификации, использование технологии блокчейн, биометрии, шифрования данных, технологии искусственного интеллекта и современных методов управления доступом. Предлагаемые решения направлены на повышение уровня безопасности и защиты медицинских данных в распределенных системах, обеспечивая надежную аутентификацию пользователей и предотвращение возможных угроз [1].

Основная часть. Не смотря на широкое распространение всевозможных технологий защиты информации, отрасль здравоохранения отстает и на технологическом [2], и на законодательном уровне. Для защиты конфиденциальности пациентов и предотвращения несанкционированного доступа к медицинской информации предлагается использовать многофакторную аутентификацию (МФА), включающую последние технологические инновации. Совместное использование двухфакторной аутентификации (например, пароля и временного кода) и биометрических методов (например, распознавание лица или сетчатки глаза) предоставляют большую защищенность при аутентификации в системах. Другие варианты внедрения МФА, объединяющие несколько методов проверки подлинности [3]. Хранение уникальных данных с применением технологии блокчейн. Передача данных должна осуществляться по зашифрованным каналам связи, рассматривается SHA-2 шифрование. Добавление в эту схему искусственного интеллекта (ИИ) для обнаружения аномалий в сетевом трафике и предсказывания потенциальных угроз усилит защиту всей системы. Аналитика данных искусственного интеллекта способна обрабатывать огромные объемы информации, что делает ее идеальной для выявления необычных и скрытых угроз.

Выводы. Представлены и проанализированы актуальные проблемы аутентификации и предложены современные пути их решения применимые к использованию в медицинских системах.

Список использованных источников:

1. Coventry L., Branley D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward //Maturitas. – 2018. – Т. 113. – С. 48-52.
2. Соболева С. Ю., Голиков В. В., Тажибов А. А. Информационные технологии в здравоохранении: особенности отраслевого применения //e-management. – 2021. – Т. 4. – №. 2. – С. 37-43.
3. Малафеевский В. Е. Защита персональных данных пациентов в медицинских учреждениях //кибербезопасность: технические и правовые аспекты защиты информации. – 2022. – С. 172-175.