МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Казанский государственный энергетический университет»

ЦИФРОВЫЕ СИСТЕМЫ И МОДЕЛИ: ТЕОРИЯ И ПРАКТИКА ПРОЕКТИРОВАНИЯ, РАЗРАБОТКИ И ПРИМЕНЕНИЯ

Национальная (с международным участием)
научно-практическая конференция
(Казань, 10 – 11 апреля 2024 г.)

Электронный сборник статей по материалам конференции

Казань
2024

УДК 004.02+004.9
ББК 32.813 + 32.973
Ц75

Рецензенты:

д-р техн. наук, профессор, зав. кафедрой «Автоматизированные системы сбора и обработки информации» ФГБОУ ВО «КНИТУ» Р.Н. Гайнуллин;

д-р техн. наук, профессор кафедры «Системы информационной безопасности» ФГБОУ ВО «КНИТУ-КАИ» А.С. Катасёв

Ц75 Цифровые системы и модели: теория и практика проектирования, разработки и применения: материалы национальной (с международным участием) научно-практической конференции (Казань, 10-11 апреля 2024 г.) / под общ. ред. И.Г. Ахметовой. Казань: Казан. гос. энерг. ун-т, 2024. 1636 с.

ISBN 978-5-89873-660-6

В электронном сборнике представлены статьи по материалам национальной (с международным участием) научно-практической конференции «Цифровые системы и модели: теория и практика проектирования, разработки и применения» по следующим направлениям:

1. Цифровые технологии и решение прикладных задач. Программная инженерия.
2. Технологии искусственного интеллекта.
3. Информационная безопасность.
4. Цифровая экосистема в образовании и в формировании личности человека.

Предназначен для научных работников, преподавателей, студентов, магистрантов, аспирантов и специалистов, работающих в сфере информационных технологий, а также для всех интересующихся цифровыми технологиями.

Статьи публикуются в авторской редакции. Ответственность за содержание статей возлагается на авторов.

УДК 004.02+004.9
ББК 32.813 + 32.973

ISBN 978-5-89873-660-6

УДК 004.056: 614.2: 616-056.32

ЗАЩИТА ДАННЫХ В ЭПОХУ ЦИФРОВИЗАЦИИ ЗДРАВООХРАНЕНИЯ

Алина Николаевна Шиховцева, Ольга Юрьевна Янова
ФГБОУ ВО «КГЭУ», г. Казань, Россия
eryomenko.alina2016@yandex.ru

Аннотация. В статье обсуждается важность обеспечения информационной безопасности в сфере здравоохранения в условиях цифровизации. Подчеркиваются возможные риски утечек конфиденциальных медицинских данных и предлагаются методы их предотвращения. Отмечается роль законодательства и обучения персонала в данном процессе.

Ключевые слова: цифровизация здравоохранения, информационная безопасность, утечки данных, медицинские данные.

DATA PROTECTION IN THE ERA OF HEALTHCARE DIGITALIZATION

Alina N. Shikhovtseva, Olga I. Ianova
KSPEU, Kazan, Russia
eryomenko.alina2016@yandex.ru

Abstract. The article discusses the importance of ensuring cybersecurity in the healthcare sector in the context of digitalization. The possible risks of leaks of confidential medical data are emphasized and methods of their prevention are proposed. The role of legislation and staff training in this process is noted.

Keywords: digitalization of healthcare, information security, data leakage, medical data.

Цифровизация здравоохранения – это не просто технологический тренд, но и неотъемлемая часть эволюции современной медицины. Электронные медицинские записи, медицинские изображения, данные о пациентах, лабораторных исследованиях – всё это сейчас активно хранится и обрабатывается в цифровом формате. Внедрение информационных технологий в медицинскую практику приносит огромные преимущества: улучшение качества обслуживания пациентов, оптимизация медицинских процессов и расширение доступа к медицинской помощи. Однако, вместе с этим, оно приносит и серьезные вызовы в области безопасности данных.

По данным исследований, треть медицинских учреждений хотя бы раз сталкивалась с утечками конфиденциальных данных. Цифровизация медицинских учреждений, которая получила активное развитие в период пандемии, подстегнула эту проблему. Утечка информации в медицинских учреждениях приводит к целому набору рисков – репутационных и финансовых [1]. Утечка медицинской тайны может привести к негативным последствиям как

для организации с точки зрения регуляторных штрафов, уголовной ответственности, потери репутации (особенно когда речь идет о частной клинике), так и для самого пациента. Например, утечка сведений о том, что пациент болеет ВИЧ или СПИД, может стать поводом для преследований, буллинга, отчислений, увольнений и т. д.

Шифрование данных играет ключевую роль в защите конфиденциальности медицинских информационных ресурсов. Одним из наиболее распространенных алгоритмов шифрования является Advanced Encryption Standard (AES). Этот алгоритм применяется для зашифрования данных на уровне блоков и может использоваться с различными размерами ключей, такими как 128, 192 и 256 бит. Кроме того, для защиты ключей шифрования часто применяется асимметричный алгоритм RSA, который обеспечивает высокий уровень конфиденциальности [2]. Важно подчеркнуть, что правильная реализация шифрования данных включает в себя безопасное управление ключами и регулярное обновление шифрования с учетом современных стандартов безопасности.

Для контроля доступа пользователей к медицинским информационным системам применяются различные методы аутентификации и авторизации. Например, Lightweight Directory Access Protocol (LDAP) используется для аутентификации пользователей и доступа к их каталогам. Широко применяется протокол OAuth, который позволяет одному сервису предоставить доступ к своим данным третьей стороне без передачи пароля. Еще одним способом аутентификации является использование стандарта X.509, который основан на сертификатах и обеспечивает безопасное идентифицирование пользователей.

Обнаружение и предотвращение кибератак в здравоохранении осуществляется с помощью различных методов и технологий. Например, системы IDS/IPS (Intrusion Detection System/Intrusion Prevention System) используются для обнаружения и блокирования аномальной сетевой активности, которая может указывать на попытки вторжения или вредоносную активность. Также широко применяется система SIEM (Security Information and Event Management), которая анализирует данные безопасности из различных источников для обнаружения угроз безопасности и быстрого реагирования на них. Кроме того, межсетевые экраны (firewalls) фильтруют сетевой трафик и блокируют нежелательные или вредоносные соединения [3].

В России регулирование кибербезопасности медицинских данных осуществляется через ряд законодательных актов и нормативных документов, которые устанавливают требования к защите медицинской информации и наказывают за ее нарушение.

Одним из основных законодательных актов в этой области является Федеральный закон «О персональных данных» № 152-ФЗ, который устанавливает правила обработки и защиты персональных данных, включая

медицинские. Согласно этому закону, медицинская информация считается особым видом персональных данных и подлежит особой защите.

Кроме того, существует ряд нормативных документов, разработанных Федеральной службой по надзору в сфере здравоохранения и другими органами государственной власти. Дополнительно, кибербезопасность медицинских данных в России регулируется нормативами и стандартами информационной безопасности, такими как ГОСТ Р ИСО/МЭК 27001, который устанавливает требования к системам управления информационной безопасностью.

Для обеспечения кибербезопасности в здравоохранении нужно следовать лучшим практикам и рекомендациям. В первую очередь, важно проводить качественное обучение персонала здравоохранения основным принципам защиты данных, определению и предотвращению угроз, а также вырабатывать навыки по обеспечению безопасности при работе с медицинскими информационными системами [4, 5].

Таким образом, важно продолжать исследования для совершенствования практик защиты данных и адаптации к новым угрозам. Следует понимать, что защита медицинских данных в период цифровой трансформации здравоохранения требует совместных усилий со стороны медицинских учреждений, правительственных органов, индустрии информационной безопасности и других заинтересованных сторон. Только так можно обеспечить безопасность и конфиденциальность данных пациентов и обеспечить стабильное функционирование медицинских учреждений.

Источники

1. Вячина И.Н., Коврижных О.Е. К вопросу о финансовой безопасности и финансовых рисках предприятия / Вестник Академии знаний. 2023. №1 (54). С. 294-298.

2. Дадашова А.С., Николаева С.Г., Джабагова С.С. Информационная безопасность и системный анализ: стратегии защиты и анализ рисков / Научно-технический вестник Поволжья. 2023. № 12. С. 239-241.

3. Пырнова О.А. Культура информационной безопасности // Технологический суверенитет и цифровая трансформация. Международная научно-техническая конференция. Казань, 2023. С. 153-157.

4. Силкина О.Ю., Зарипова Р.С. Интеллектуальные системы в медицине / Интеллектуальные информационные системы: теория и практика: сборник статей по материалам II Всероссийской конференции. Курск, 2021. С. 94-101.

5. Филимонова Т.К., Овсеенко Г.А., Мустафаев Т.А. Разработка имитационной информационно-математической модели деятельности предприятия // Научно-технический вестник Поволжья. 2023. № 11. С. 127-130.