



Анализ рисков информационной безопасности в центрах медицинской реабилитации: проблемы и перспективы. Обзор

Зайцева Т.Н.* , Бараксанова К.М.

Российская медицинская академия непрерывного профессионального образования Минздрава России, Москва, Россия

РЕЗЮМЕ

ВВЕДЕНИЕ. В статье рассмотрены основные аспекты рисков информационной безопасности в медицинских организациях, в том числе в центрах медицинской реабилитации. Коллективом авторов отмечен ряд проблем, которые могут возникать в цифровом пространстве системы здравоохранения. Прежде всего речь идет о потере персональных данных пациентов, открытии несанкционированного доступа к результатам диагностики и анализов, а также неправомерного использования информации о методах лечения и медицинской реабилитации.

ЦЕЛЬ. Определить отдельные риски информационной безопасности в пространстве цифрового здравоохранения.

МАТЕРИАЛЫ И МЕТОДЫ. В качестве материала исследования использовались репрезентативные базы данных по поиску научных источников PubMed, Google Scholar, CyberLeninka, eLIBRARY.RU. В качестве инструментов поиска использовались следующие слова и сочетания: information security in medicine, information security in rehabilitation, personal data protection, информационная безопасность в здравоохранении, телемедицина, искусственный интеллект (ИИ) в медицине.

РЕЗУЛЬТАТЫ И ОБСУЖДЕНИЕ. Коллективом авторов выполнен обзор доступных научных источников, систематизированы и кратко представлены основные проблемы информационной безопасности, использования информационно-коммуникационных технологий и ИИ в цифровом здравоохранении, в том числе в центрах медицинской реабилитации. Проведенный анализ представленных научно-литературных данных позволяет сделать вывод о необходимости грамотной комбинация стратегий обеспечения безопасности пациентов как на уровне медицинской организации, так на региональном и федеральном уровнях.

ЗАКЛЮЧЕНИЕ. Сочетание стратегий по обеспечению безопасности пациентов зависит от особенностей оказания медицинских услуг. Формирование единой цифровой медицинской среды на национальном и затем международном уровне с разработкой стандартизированных автоматизированных рабочих мест для специалистов и соблюдением требований по защите конфиденциальности данных существенно повысит эффективность функционирования медицинских учреждений и может способствовать укреплению доверия пациентов к предоставляемым медицинским услугам.

КЛЮЧЕВЫЕ СЛОВА: информационная безопасность, цифровое здравоохранение, телемедицина, защита персональных данных, искусственный интеллект

Для цитирования: / For citation: Зайцева Т.Н., Бараксанова К.М. Анализ рисков информационной безопасности в центрах медицинской реабилитации: проблемы и перспективы. Обзор. Вестник восстановительной медицины. 2025; 24(1):112–119. <https://doi.org/10.38025/2078-1962-2025-24-1-112-119> [Zaytseva T.N., Baraksanova K.M. Risk Analysis of Information Security in Medical Rehabilitation Centers: Problems and Outlook. A Review. Bulletin of Rehabilitation Medicine. 2025; 24(1):112–119. <https://doi.org/10.38025/2078-1962-2025-24-1-112-119> (In Russ.).]

* **Для корреспонденции:** Зайцева Татьяна Николаевна, E-mail: zaytsevatn@rmapo.ru

Статья получена: 23.07.2024

Статья принята к печати: 26.09.2024

Статья опубликована: 16.02.2025

Risk Analysis of Information Security in Medical Rehabilitation Centers: Problems and Outlook. A Review

 Tatiana N. Zaytseva*,  Kristina M. Baraksanova

Russian Medical Academy of Continuous Professional Education, Moscow, Russia

ABSTRACT

INTRODUCTION. The article discusses the main aspects of information security risks in medical organizations, including medical rehabilitation centers. The team of authors noted a number of problems that may arise in the digital space of the health system. First of all the loss of personal data of patients, the unauthorized access to diagnostic, analytical results and the misuse of treatment and rehabilitation methods.

AIM. To identify particular risks to information security in the sector of digital healthcare.

MATERIALS AND METHODS. The research material included representative databases on PubMed, Google Scholar, CyberLeninka, eLIBRARY.RU. These phrases and words were used as search tools: information security in medicine, information security in rehabilitation, personal data protection, information security in health, telemedicine, and artificial intelligence in medicine.

RESULTS AND DISCUSSION. A team of authors reviewed available scientific sources, systematized and presented a concise overview of the key issues relating to the security of information, the use of information and communication technologies and artificial intelligence in digital healthcare, with particular reference to medical rehabilitation centers. The analysis of the presented scientific and literary data leads to the conclusion that a competent combination of strategies is required to ensure the safety of patients at the level of a medical institution and at the regional and federal levels.

CONCLUSION. The combination of patient safety strategies depends on the specifics of the provision of medical services. The formation of a unified digital medical environment at the national and then international level, with the development of standardized automated workplaces for specialists and compliance with data confidentiality requirements, will significantly enhance the performance of medical institutions. Additionally, it can help strengthen patient's confidence in the medical services provided.

KEYWORDS: information security, digital healthcare, telemedicine, personal data protection, artificial intelligence

For citation: Zaytseva T.N., Baraksanova K.M. Risk Analysis of Information Security in Medical Rehabilitation Centers: Problems and Outlook. A Review. Bulletin of Rehabilitation Medicine. 2025; 24(1):112–119. <https://doi.org/10.38025/2078-1962-2025-24-1-112-119> (In Russ.).

* **For correspondence:** Tatiana N. Zaytseva, E-mail: zaytsevatn@rmapo.ru

Received: 23.07.2024

Accepted: 26.09.2024

Published: 16.02.2025

ВВЕДЕНИЕ

Безопасность и конфиденциальность являются базовыми потребностями современного мира [1]. Построение надежной киберструктуры в диапазоне от коммерческих компаний до государственных учреждений является критически важным процессом. Использование информационных технологий позволяет значительно улучшить скорость, качество, точность и эффективность предоставляемой медицинской помощи. Информационная безопасность — это ключевой компонент для защиты имеющих ценность данных от вредоносного антропогенного воздействия [2]. При наличии уязвимостей в ИТ-периферии (ИТ — информационные технологии) такие угрозы, как несанкционированный доступ, шифрование и удаление данных, а также рассылки сообщений с подменных адресов могут являться причиной нанесения ущерба организации [3–5].

В настоящее время очень важными являются вопросы обеспечения безопасности пациентов и персонала при осуществлении медицинской деятельности [6, 7]. Оцифровывание медицинской документации позволяет проводить с ней различные автоматизированные операции. В лечебном процессе оцифрованная информация может оперативно передаваться всем сторонам, участвующим в предоставлении медицинских услуг, что в свою очередь обеспечивает получение

пациентами медицинской помощи более высокого качества при одновременном снижении затрат на администрирование этой деятельности. [8]. Большая часть клинической документации, подлежащей совместному использованию, собирается в картах пациентов. Более сложные подходы к электронным картам пациентов являются трансинституциональными или межнациональными [9].

Медицинские организации (стационары, поликлиники, диагностические центры, частные клиники, реабилитационные центры и др.) имеют особо чувствительные данные: истории болезней пациентов, содержащие персональные данные; методы профилактики и диагностики; результаты анализов и многое другое, представляющее собой медицинскую тайну [10]. Так, например, кража данных дает мошенникам возможность не только получить сведения о состоянии здоровья пациентов или манипулировать их медицинским страхованием, но и помешать процессу лечения и медицинской реабилитации. Следовательно, доступ к такой информации должен быть ограничен и строго контролироваться [11].

ЦЕЛЬ

Определить отдельные аспекты информационной безопасности в пространстве цифрового здравоохранения.

МАТЕРИАЛЫ И МЕТОДЫ

В качестве материала исследования использовались репрезентативные базы данных по поиску научных источников PubMed, Google Scholar, CyberLeninka, eLIBRARY.RU. В качестве инструментов поиска использовались следующие слова и сочетания: information security in medicine, information security in rehabilitation, personal data protection, информационная безопасность в здравоохранении, телемедицина, искусственный интеллект (ИИ) в медицине.

РЕЗУЛЬТАТЫ И ОБСУЖДЕНИЕ

Анализ рисков информационной безопасности, использования информационно-коммуникационных технологий и ИИ в цифровом здравоохранении может позволить определить основные проблемы и выстроить результативную стратегию обеспечения безопасности пациентов как на уровне медицинской организации, так и на региональном и федеральном уровнях.

На сегодня можно выделить наиболее значимые проблемы при обеспечении информационной безопасности в медицинской организации: недостаток собственного профессионального опыта, нехватка специалистов в сфере кибербезопасности и недостаток бюджета [12]. Все эти факторы в свою очередь могут приводить к различным утечкам данных. В 2022 г. из-за низкого уровня защиты конфиденциальной информации даркнет получил базу данных 30 млн клиентов медицинской лаборатории «Гемотест». Вследствие незаконного доступа мошенникам удалось распространить фамилии, имена, отчества, даты рождения, адреса электронных почт и номера телефонов клиентов. После данного случая Министерство цифрового развития, связей и массовых коммуникаций Российской Федерации (Минцифры России) совместно с Роскомнадзором выступило с инициативой вводить большие оборотные штрафы для организаций (за исключением государственных), допустивших утечку данных. Однако, как заявил глава Минцифры России Максут Шадаев, возможны смягчения наказаний в случае компенсации потерь пациентов. В 2023 г. был опубликован проект Федерального закона «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»¹ Нормативный правовой акт коррелирует ответственность в отношении количества субъектов персональных данных, подвергшихся хакерской атаке. Для юридических лиц повторное нарушение может повлечь штрафы до 500 млн рублей.

Подобные случаи встречаются и в зарубежной практике. В 2020 г. хакеры получили доступ к аккаунтам 2 млн клиентов компании EyeMed Vision Care, производящей контактные линзы премиум-класса. Данный инцидент обязал итальянскую компанию выплатить \$600 000 правительству США. Число кибератак может расти по причине не только недостаточного финансирования кибербезопасности медицинский учреждений, но и утечки информации из-за невнимательного

отношения сотрудников медицинских организаций к персональным данным.

Успешное использование различных облачных репозиторий для медицинской информации позволяет решить проблему масштабирования и защиты данных [13]. Целостность сведений, передаваемых на аутсорсинг в облачные информационные системы, является критически важной, поскольку только на основе полных данных можно поставить правильный диагноз, а составление протокола публичного аудита является ключевым решением этой проблемы [14]. По данным International Business Machine, в мире ежедневно создается около 3 экзабайт новой информации, значительная часть которой связана со сферой здравоохранения. Многие страны издают регламенты, регулирующие интеграцию медицинских информационных систем и облачных хранилищ. По этой причине, например, в 2018 г. Европейский Союз создал Общий регламент по защите данных (General Data Protection Regulation). Для обеспечения защиты консолидации к медицинским хранилищам (CSSM) специалисты устанавливают фиксированные требования (протокол аудита) для передачи информации третьим лицам по криптографическому ключу.

Модель системы с облачным хранилищем включает несколько фаз:

- запрос доступа к CSSM;
- бесшовная интеграция с DO (Data outsourcing);
- интерпелляция к TPA (Third party auditor);
- получение медицинским сотрудником запрашиваемой информации.

В данной модели используют билинейное криптографическое сопряжение и вычислительные дискретные логарифмы, которые формируют фазы настройки доступа (алгоритмы KeyGen, TagGen, HtGen) и верификации пользователя (алгоритмы Challenge, ProofGen, ProofVer). Также хеширование табличной структуры является важным звеном добавления, модификации и удаления данных с целью динамического обновления облачных функций [15, 16].

Организаторами здравоохранения, профессиональными медицинскими сообществами и юристами регулярно обсуждаются вопросы правового регулирования и обеспечения безопасности медицинской деятельности [8, 17–20]. Уже стало очевидно, что для модернизации ИТ в сфере здравоохранения необходимо создавать новые программы и нормативные правовые акты, помогающие снизить риски информационной безопасности. Так, в 2009 г. США приняли закон об информационных технологиях здравоохранения для экономики и клинического здравоохранения (The Health Information Technology for Economic and Clinical Health Act), или закон о HITECH. Данный нормативной правовой акт считался главной реформой в сфере медицинских услуг за последние 20–30 лет, так как позволил Министерству здравоохранения и медицинских служб США расширить внедрение электронных медицинских карт. Обмен медицинской информацией стал более доступен, однако обязал организации использовать только сертифицированные системы для анализа клинических показателей качества и назначения лекарственных препаратов. Также учреждения должны информировать Национальных координаторов ин-

¹ Проект Федерального закона № 502104-8 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях». Доступно на <https://sozd.duma.gov.ru/bill/502104-8> (Дата обращения: 17.06.2024)

формационной безопасности об утечках данных более 500 пациентов и учитывать требования по раскрытию информации о лечении, а также должны информировать о проводимых операциях и оплате медицинского обслуживания [21].

В 2020 г. 30 % мировых данных принадлежали индустрии здравоохранения. Медицинская информация экспоненциально увеличивается, что требует превентивных мер против киберпреступлений. Таким образом, учреждения пересматривали эффективность работы DLP-систем (Data Leak Prevention), предотвращающих утечку конфиденциальной корпоративной информации. Данные посетителей хранятся в репозиториях, называемых warehouse, где информация систематизируется для дальнейшего использования исследователями, медицинскими базами и учреждениями с целью улучшить процесс принятия решений медицинского обслуживания [22]. Также организации в сфере здравоохранения обладают статистическими и аналитическими индикаторами, которые способны предсказать изменение стоимости лекарств, возникновение эпидемий, происхождение новых препаратов и демографические тенденции.

Согласно прогнозам ВОЗ, к 2030 г. ожидается расширение и интеграция мер реабилитации в системы медицинского обслуживания. Особое внимание будет уделено комплексной терапии нарушений сердечно-сосудистой системы, а также реабилитации пациентов с поражениями спинного и головного мозга [23, 24]. При внедрении новых программ медицинской реабилитации будут широко применяться современные информационные технологии. Это означает, что в процессе восстановления (компенсации) нарушенных или утраченных функций организма активно будут задействованы различные цифровые решения и инструменты. Использование ИТ-технологий позволит сделать реабилитационные программы более эффективными и удобными как для специалистов, так и для самих пациентов. Например, в Австралии на базе Центра Джонса Хопкинса была создана лаборатория HabiТес — место нетворкинга для медицинских специалистов, разработчиков, исследователей и инвесторов, которые занимаются созданием и тестированием инструментов для реабилитации людей с различными нарушениями здоровья. Лаборатория HabiТес является инициативным объединением Университета Гриффита, корпорации Майкрософт и некоторых негосударственных организаций, поддерживающих сферу здравоохранения. Так, медицинские сотрудники используют технологию PEO (Person Environment Occupation), позволяющую сначала изучить общее нервно-мышечное состояние пациента, а затем назначать лечение на основе личностно-ориентированного подхода [25].

Появление современных способов оказания медицинской помощи и внедрение более совершенных технологий не только поднимает планку стандартов безопасности, но и может создавать новые риски. Роботы для медицинской реабилитации открывают уникальные возможности для сферы здравоохранения [26].

В настоящее время кибербезопасность становится все более важным аспектом для изучения внедрения и использования роботизированной медицинской техники с точки зрения как безопасности пациентов, так

и доступности, целостности и конфиденциальности их данных [27]. В основном медицинские роботы, используемые в процессе медицинской реабилитации, являются примерами взаимосвязанных медицинских устройств: им нужна линия связи для обмена и записи данных, для обновления и/или других функций. Их активно применяют в процессах психологической и когнитивной реабилитации пациентов с коммуникативными нарушениями. Таким образом, программное обеспечение роботизированной медицинской техники взаимодействует не только с персональными данными, но и с данными о состоянии здоровья пациента, а также собирает сведения об этапах его лечения и процессе медицинской реабилитации. Поэтому использование мошенниками данных, полученных от медицинских роботов, может иметь значительные негативные последствия для физического и психологического здоровья пациента.

Телемедицинские устройства обладают огромным потенциалом для телемониторинга и телереабилитации пациентов, страдающих хроническими инвалидизирующими заболеваниями. В частности, системы ИИ теперь могут обеспечить очень полезную поддержку в управлении и принятии решений во многих клинических областях [28, 29]. ИИ в сочетании с цифровизацией также может позволить осуществлять удаленный мониторинг состояния здоровья пациентов. Однако поводом для беспокойства является защита конфиденциальности и безопасности [30]. В этом контексте существует единогласное мнение, что внедрение ИИ должно сопровождаться тщательной проработкой вопроса со стороны законодательства, чтобы действительно гарантировать защиту прав граждан и пациентов. Например, стоит вопрос о согласии на обработку персональных данных о состоянии здоровья системами ИИ [31].

Развитие машинного обучения является стремительным процессом, обеспечивающим полезное применение и результат улучшения здоровья значимого процента населения. Однако ИИ может стать потенциальной детерминантой возникновения рисков в социальной, политической, экономической и медицинской сферах. Данная технология может оказывать пагубное влияние через манипулятивные процессы, имитацию голоса (система deep fake), регулирование автономным химическим оружием и воздействие на работу персонала. Необходимость эффективного регулирования и предотвращение возможного урона человечеству катализировало принятие «Регламента Европейского союза об искусственном интеллекте» 13 марта 2024 г. (регулирует все отрасли, кроме военной) [32]. В медицинской сфере данный нормативный правовой акт нацелен на исключение рисков информационной безопасности, приводящих к физическому или психологическому ущербу, а также неизбирательному использованию биометрической базы данных. Согласно регламенту системы ИИ, использующиеся в сфере медицинского обслуживания, маркируются как системы с высокой степенью риска и обязуются проходить специальную проверку соответствия поставщиком перед выпуском на рынок. Особо важное программное обеспечение для медицинского оборудования будет рассматриваться организацией, назна-

ченной национальным правительством страны-члена Европейского Союза в соответствии с зафиксированными требованиями в «Положении о медицинских устройствах».

Машинное обучение имеет потенциал революционизировать работу врачей, увеличивая точность диагнозов, разрабатывая новые лекарства и обеспечивая медицинскую помощь большему количеству людей. Положительное влияние, оказываемое за счет быстрого перевода ИИ семантики разговора специалистов, отразится на глобальном профессиональном сотрудничестве. Инструменты поддержки принятия решений, распознавание изображений клинических снимков, анализ больших данных могут уменьшить риск развития болезней. Не смотря на явные преимущества, известен случай пагубного влияния ИИ. Так пульсометр, управляемый программой машинного обучения, завывсил уровень кислорода в крови у пациентов с более темным цветом кожи, что привело к назначению мер, недостаточных для лечения гипоксии. В добавление к вышеобозначенному система распознавания лиц с большей вероятностью ошибочно определяет пол людей с более темной кожей [33].

В 2022 г. иранские исследователи из Департамента технологий здравоохранения и Мешхедского университета медицинских наук провели сравнительный анализ реабилитационных информационных систем в 8 странах: Канаде, США, Великобритании, Швеции, Австралии, Малайзии, России и Иране [34]. Исследователи сравнивали написанный код, используемые базы данных и категории реестров. Было выявлено, что реабилитационные системы Канады и США охватывают пациентов всех возрастов и собирают данные по всему миру. Австралия имеет национальный клинический реестр [35]. Швеция и Иран фокусируются на амбулаторной реабилитации взрослых, чтобы сохранить трудоспособность населения. Малайзия развивает технологии преимущественно для новорожденных (скрининг, вакцинация) с целью снижения младенческой смертности. Каждый год в этой стране умирает большое количество людей от инфекционных и хронических заболеваний, несмотря на крупный бюджет, выделяемый государством (22 млрд ринггитов в год). Главной целью Министерства здравоохранения Малайской Федерации является укрепление внешнеполитических связей с целью обмена профессиональным опытом и данными, которые помогут усовершенствовать цифровую отрасль и сделать медицинские услуги более доступными. Великобритания успешно внедряет медицинские сервисы, уделяя равное внимание лечению и реабилитации. Достижению высоких результатов способствует ежегодная миграция высококвалифицированных специалистов, увеличение спонсорских групп и многолетние исследования (в 1930 г. в Англии впервые была создана организация Medical Disability Society). Российская Федерация только создает траекторию запуска для информационных реабилитационных систем, и для ее развития необходима государственная поддержка медицинских работников, а также организация междисциплинарных коалиций [36]. Данный анализ может быть полезен для совершенствования реабилитационных практик и информационных систем в разных странах.

Глобально 1/3 пациентов после периода болезней или во время получения травм нуждается в предоставлении услуг реабилитационного сектора. Одной из наилучших мер доказать необходимость процесса реабилитационного лечения является фактическая регистрация данных, что сделает возможным определение всестороннего отношения причинности заболеваний и регионов. Соответственно, необходимо создание и развитие технологичных продуктов для интерпретации и анализа лучшего лечения. Однако не все страны могут себе позволить проектирование единой информационной системы анализа данных реадaptации и ее интеграцию с остальными прикладными системами в сфере здравоохранения [37]. Более 30 лет назад некоммерческой компанией UDSMR (Uniform Data System for Medical Rehabilitation) в Нью-Йорке были созданы аффилированные с университетом Буффало информационные продукты.

Наиболее популярным сервисом является The UDS-PRO System, инкорпорирующая медицинские и управленческие требования, обеспечивающая доступ к самой большой базе данных (более 13 млн пациентов) в медицинской сфере, охватывающая свыше 1400 стационарных реабилитационных учреждений по всему миру, около 900 которых находится в США [38]. В функционал The UDS-PRO System входят модуль предварительной регистрации персональных данных пациентов (имя, возраст, раса, гражданство, диагноз, программа лечения), содержащий необходимые элементы для Руководства по политике предоставления льгот программы Medicare, динамический экспорт, клинические исследования и информация о поставщиках оборудования (стандарт кодировочной системы — Uniform Data System Impairment Codes). Дата-инженеры и разработчики гарантируют нулевые риски взлома программного продукта, так как серверы находятся в здании, охраняемом правительством.

Канадская система NRS использует государственный стандарт программирования ICD10-CA и собирает информацию о лицах, нуждающихся в реадaptационных процессах из 9 провинций [39]. Защита персональных данных обусловлена законом о защите личной медицинской информации (2004) и технологий, утвержденным Международным сертификатом безопасности (ISO 27001) [40].

Великобритания и Швеция, страны-представители континентальной Европы, в качестве главных информационных сервисов используют UKROC и WebRehab со стандартизациями ICD 10 codes и ICF соответственно. Отличительной особенностью европейских стран от Северной Америки является сбор сведений об удовлетворенности стилем жизни, а также фиксация корреляции процесса выздоровления с рабочими и семейными условиями [41, 42]. Изначально WebRehab работала с данными пациентов, нуждающихся в восстановлении головного и спинного мозга, а UKROC анализировала неврологическую реадaptацию. Однако Великобритании, благодаря крупному финансированию, удалось построить лучшую в континентальной Европе программу реабилитации, где каждый год индекс Байреля увеличивается в 2 раза [43].

В 2022 г. Иранская информационная система Payment находилась в стадии развития, но в базах данных об-

следованных уже хранились ID-карты (ID — идентификатор), информация о финансовом благополучии, занятости и фиксация человека, удовлетворяющего роль «главы семейства». В период проведения исследования Малайзия не обладала достаточным финансовым, технологическим и кадровым ресурсом для создания информационной среды с целью улучшения медицинской реабилитации.

До настоящего времени в России не разрабатывалось программного обеспечения для анализа и прогнозирования процесса реабилитации на федеральном уровне. Акцент системы здравоохранения делается на лечение тяжелых нарушений в области сердечно-сосудистой хирургии, а также нарушений работы спинного и головного мозга, что не создает высокого спроса на создание единых глобальных сервисов в сфере реабилитации. Однако тенденция совершенствования узкоспециализированных программ, телемедицины и робототехники активно развивается. Результаты комплексного исследования реабилитационных информационных систем демонстрируют, что первенство в отношении создания технологической периферии сферы здравоохранения принадлежит Америке, Канаде и Великобритании [44].

ЗАКЛЮЧЕНИЕ

В настоящее время в нашей стране происходит активный переход к цифровой медицине, что позволяет поддерживать здоровье населения на новом качественном уровне. При этом мы находимся в ситуации, когда регулирование и надзор рискуют отставать от технологий, которыми они управляют. Регулирование должно поощрять более сложные методы анонимизации и защиты данных. Комбинация стратегий обеспечения безопасности пациентов зависит от специфики предоставления медицинских услуг. Руководители медицинских организаций могут разрабатывать и внедрять собственные внутренние правила, инструкции

и процедуры, направленные на соблюдение государственных стандартов и норм, обеспечивающих безопасность предоставляемой медицинской помощи. Контроль за обеспечением информационной безопасности данных пациентов и персонала должен происходить как внутри медицинской организации, так и со стороны региональных и федеральных контрольно-надзорных органов. Также медицинские учреждения должны своевременно информировать регулирующие органы обо всех случаях утечки персональных данных пациентов, включая сведения о проведенном лечении, операциях и оплате медицинских услуг.

Использование роботизированной техники, телемедицинских технологий и ИИ в медицинской реабилитации может представлять потенциальные риски для информационной безопасности. Этот аспект требует особого внимания и тщательной проработки для обеспечения надежной защиты данных пациентов и систем. Изучение опыта других стран в сфере обеспечения кибербезопасности может стать ценным источником для развития этого направления в нашей стране. Это позволит избежать ошибок, допущенных зарубежными коллегами, и внедрить у себя их наиболее эффективные практики.

Применение облачных хранилищ для медицинской информации позволяет решить проблемы масштабирования и защиты данных. Для обеспечения безопасности доступа к медицинским базам данных необходимо устанавливать четкие требования к передаче информации третьим лицам, включая использование криптографических ключей. Создание единой национальной, а затем и международной, цифровой медицинской среды с разработкой стандартизированных автоматизированных рабочих мест для специалистов, с соблюдением требований защиты конфиденциальных данных позволит значительно повысить эффективность работы медицинских учреждений и может способствовать росту доверия пациентов к медицинской деятельности.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Зайцева Татьяна Николаевна, кандидат медицинских наук, доцент кафедры физической терапии, спортивной медицины и медицинской реабилитации, заведующий отделом координации научной деятельности, Российская медицинская академия непрерывного профессионального образования Минздрава России.

E-mail: zaytsevatn@rmapo.ru;

ORCID: <https://orcid.org/0000-0001-7123-1568>

Бараксанова Кристина Михайловна, аналитик отдела поддержки и развития информационных систем, Управление информационных технологий, Российская медицинская академия непрерывного профессионального образования Минздрава России.

ORCID: <https://orcid.org/0009-0000-6749-4779>

Вклад авторов. Все авторы подтверждают свое авторство в соответствии с международными критериями ICMJE (все авторы внесли значительный вклад в концепцию, дизайн исследования и подготовку статьи, прочитали и одобрили окончательный вариант до публикации). Наибольший вклад распределен следующим образом: Зайцева Т.Н. — научное обоснование, анализ данных, проверка и редак-

тирование рукописи; Бараксанова К.М. — обеспечение материалов для исследования, написание черновика рукописи. Все авторы утвердили окончательный вариант статьи, несут ответственность за целостность всех частей статьи.

Источники финансирования. Данное исследование не было поддержано никакими внешними источниками финансирования. Исследование проведено на личные средства авторского коллектива.

Конфликт интересов. Авторы декларируют отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.

Благодарность. Авторы выражают признательность за ценные советы при планировании исследования и рекомендации по оформлению статьи доктору медицинских наук, профессору, заведующему кафедрой физической терапии, спортивной медицины и медицинской реабилитации ФГБОУ ДПО «Российская медицинская академия непрерывного профессионального образования» Минздрава России Герасименко М.Ю.

Доступ к данным. Данные, подтверждающие выводы этого исследования, можно получить по обоснованному запросу у корреспондирующего автора.

ADDITIONAL INFORMATION

Tatiana N. Zaytseva, Ph.D. (Med.), Associate Professor at the Department of Physiotherapy, Sports Medicine and Medical Rehabilitation, Head of the Department for the Coordination of Scientific Activities, Russian Medical Academy of Continuous Professional Education.

E-mail: zaytsevatn@mapo.ru;

ORCID: <https://orcid.org/0000-0001-7123-1568>

Kristina M. Baraksanova, Analyst, Department for Support and Development of Information Systems, Information Technology Directorate, Russian Medical Academy of Continuous Professional Education.

ORCID: <https://orcid.org/0009-0000-6749-4779>

Author Contributions. All authors confirm their authorship according to the international ICMJE criteria (all authors contributed significantly to the conception, study design and preparation of the article, read and approved the final version before publication). Special contributions: Zaytseva T.N. —

conceptualization, formal analysis, writing review and editing; Baraksanova K.M. — resources, writing original draft. All authors are responsible for the integrity of all parts of the manuscript and approval of the manuscript final version.

Funding. This study was not supported by any external funding sources. The study was conducted with personal funds from the author's team.

Disclosure. The authors declare no apparent or potential conflicts of interest related to the publication of this article.

Acknowledgments. The authors express their gratitude for valuable advice in the planning of the study and recommendations on the design of the article to M.Y. Gerasimenko, D.Sc. (Med.), Professor, Head of the Department of Physical Therapy, Sports Medicine and Medical Rehabilitation of the Russian Medical Academy of Continuous Professional Education.

Data Access Statement. The data that support the findings of this study are available on reasonable request from the corresponding author.

Список литературы / References

1. Брумштейн Ю.М., Захаров Д.А., Акишкин В.Г. Риски информационной безопасности медучреждений, их специалистов и пациентов. Информационная безопасность регионов. 2013; 1(12): 13–21. [Brumshtein Yu.M., Zakharov D.A., Akishkin V.G. Research into information security of medical institutions, their specialists and patients. Information security of regions. 2013; 1(12): 13–21 (In Russ.).]
2. Charles P. Pfleeger, Shari Lawrence Pfleeger. Analyzing Computer Security; A Threat/Vulnerability/ Countermeasure Approach. Pearson Education International; Upper Saddle River, N.J. 2012; 795 p.
3. Банк данных угроз безопасности информации. Доступно на: <https://bdu.fstec.ru/threat> (Дата обращения: 17.06.2024). [Data bank of information security threats. Available at: <https://bdu.fstec.ru/threat> (Accessed: 17.06.2024) (In Russ.).]
4. INFOWATCH. Аналитика отрасли информационной безопасности. Доступно на: <https://www.infowatch.ru/analytics/analitika?page=2> (Дата обращения: 03.06.2024). [INFOWATCH. Information security industry analytics. Available at: <https://www.infowatch.ru/analytics/analitika?page=2> (Accessed: 03.06.2024) (In Russ.).]
5. Datasets. Centre for Health Record Linkage. CHeReL Master Linkage Key. Available at: <https://www.cherel.org.au/datasets> (Accessed: 31.05.2024).
6. Демаков В.И., Рерке В.И., Портная Я.А. и др. Об обеспечении информационной безопасности в сфере медицины и актуальности ее изучения в ведомственных вузах. Человеческий капитал. 2021; 4(148): 83–89. <https://doi.org/10.25629/HC.2021.04.07> [Demakov V.I., Rerke V.I., Portnaya Y.A. et al. On ensuring information security in the field of medicine and the relevance of its study in departmental universities. Human capital. 2021; 4(148): 83–89. <https://doi.org/10.25629/HC.2021.04.07> (In Russ.).]
7. Sivarajkumar S., Gao F., Denny P. et al. Mining Clinical Notes for Physical Rehabilitation Exercise Information: Natural Language Processing Algorithm Development and Validation Study. JMIR Med Inform. 2024;12: e52289. <https://doi.org/10.2196/52289>
8. Сахаров Д.В., Пешков А.И. Нормативно-правовые проблемы безопасности территориально распределенных информационных систем в офтальмологии. Офтальмохирургия. 2022; 54: 132–137. <https://doi.org/10.25276/0235-4160-2022-45-132-137> [Sakharov D.V., Peshkov A.I. Regulatory and legal problems of security of geographically distributed information systems in ophthalmology. Ophthalmosurgery. 2022; 54: 132–137. <https://doi.org/10.25276/0235-4160-2022-45-132-137> (In Russ.).]
9. Knaup P., Benning N.H., Seitz M.W. et al. eHealth and Clinical Documentation Systems. Stud Health Technol Inform. 2020; 274: 174–188. <https://doi.org/10.3233/SHTI200676>
10. Carter A.B., Abruzzo L.V., Hirschhorn J.W. et al. Electronic Health Records and Genomics: Perspectives from the Association for Molecular Pathology Electronic Health Record (EHR) Interoperability for Clinical Genomics Data Working Group. J Mol Diagn. 2022; 24(1): 1–17. <https://doi.org/10.1016/j.jmoldx.2021.09.009>
11. Olorunsogo T.O., Ogugua J.O., Muonde M. et al. Environmental factors in public health: A review of global challenges and solutions. World Journal of Advanced Research and Reviews. 2024; 21(1): 1453–1466. <https://doi.org/10.30574/wjarr.2024.21.1.0176>
12. Варзин С.А., Матвеев В.В. Обеспечение информационной безопасности в системе здравоохранения. Национальная безопасность и стратегическое планирование. 2023; 3(43): 19–56. <https://doi.org/10.37468/2307-1400-2024-2023-3-19-56> [Varzin S.A., Matveev V.V. Ensuring information security in the healthcare system. National security and strategic planning. 2023; 3(43): 19–56. <https://doi.org/10.37468/2307-1400-2024-2023-3-19-56> (In Russ.).]
13. Africa Blog. An important next step on our AI journey. (Accessed: 17.06.2024). Available at: <https://blog.google/intl/en-africa/products/explore-get-answers/an-important-next-step-on-our-ai-journey/>
14. Majcherek D., Hegerty S.W., Kowalski A.M. et al. Opportunities for healthcare digitalization in Europe: Comparative analysis of inequalities in access to medical services. Health Policy. 2024; 139: 104950. <https://doi.org/10.1016/j.healthpol.2023.104950>
15. Li X., Liu S., Lu R. et al. An Efficient Privacy-Preserving Public Auditing Protocol for Cloud-Based Medical Storage System. IEEE J Biomed Health Inform. 2022; 26(5): 2020–2031. <https://doi.org/10.1109/JBHI.2022.3140831>
16. Huang K., Zhang X.-s., Mu Y. et al. Bidirectional and Malleable Proof-of-Ownership for Large File in Cloud Storage. In IEEE Transactions on Cloud Computing. 2022; 4(10): 2351–2365. <https://doi.org/10.1109/TCC.2021.3054751>
17. Орлова В.В. Оптимизация взаимодействия с пациентами медицинского учреждения на основе развития интернет-коммуникаций. Социальные аспекты здоровья населения. 2014; 6(40): 9. [Orlova V.V. Optimizing interaction with patients of a medical institution based on the development of Internet communications. Social aspects of public health. 2014; 6(40): 9 (In Russ.).]

18. Журавлев М.С. Правовые аспекты информационной безопасности в телемедицине. Диссертация на соискание ученой степени кандидата юридических наук. Москва. Высшая школа экономики. 2021; 191 [Zhuravlev M.S. Legal aspects of information security in telemedicine. Dissertation for the degree of Candidate of Legal Sciences. Moscow. HSE University. 2021; 191 (In Russ.).]
19. Марухленко А.Л., Чешин А.В., Алеева С.С. и др. Политика информационной безопасности в цифровом здравоохранении: организационно-правовые аспекты. Вопросы политологии. 2023; 12(100): 6612–6624. <https://doi.org/10.35775/PSI.2023.100.12.018> [Marukhlenko A.L., Cheshin A.V., Aleeva S.S. et al. Information security policy in digital health: organizational and legal aspects. Questions of political science. 2023; 12(100): 6612–6624. <https://doi.org/10.35775/PSI.2023.100.12.018> (In Russ.).]
20. Усенков И.А. Стабильность законодательства о телемедицине: актуальные проблемы. Право и политика. 2024; 3: 30–40. <https://doi.org/10.7256/2454-0706.2024.3.70044> [Usenkov I.A. Stability of telemedicine legislation: current issue. Law and politics. 2024; 3: 30–40. <https://doi.org/10.7256/2454-0706.2024.3.70044> (In Russ.).]
21. Cybersecurity Threats in Healthcare Organizations: Exposing Vulnerabilities in the Healthcare Information Infrastructure. Available at: <https://worldlibraries.dom.edu/index.php/worldlib/article/view/588/678> (Accessed: 31.05.2024).
22. Chidolue O., Iqbal T. System Monitoring and Data logging using PLX-DAQ for Solar-Powered Oil Well Pumping. 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC). 8–11 March 2023. Las Vegas. 2023; 0690–0694. <https://doi.org/10.1109/CCWC57344.2023.10099099>
23. World Health Organization. Rehabilitation in health system; guide for action. Available at: <https://www.who.int/publications/i/item/9789241515986> (Accessed: 31.07.2024).
24. Kleinitz P., Sabariego C., Llewellyn G. et al. Integrating rehabilitation into health systems: A comparative study of nine middle-income countries using WHO's Systematic Assessment of Rehabilitation Situation (STARS). PLoS One. 2024; 19(2): e0297109. <https://doi.org/10.1371/journal.pone.0297109>
25. Kendall E., Oh S., Amsters, D. et al. HabITec: A Sociotechnical Space for Promoting the Application of Technology to Rehabilitation. Societies. 2019; 9(4): 74. <https://doi.org/10.3390/soc9040074>
26. Martineau T., Ozano K., Raven J. et al. Improving health workforce governance: the role of multi-stakeholder coordination mechanisms and human resources for health units in ministries of health. Hum Resour Health. 2022; 20(1): 47. <https://doi.org/10.1186/s12960-022-00742-z>
27. Monoscalco L., Simeoni R., Maccioni G. et al. Information Security in Medical Robotics: A Survey on the Level of Training, Awareness and Use of the Physiotherapist. Healthcare (Basel). 2022; 10(1): 159. <https://doi.org/10.3390/healthcare10010159>
28. Cingolani M., Scendoni R., Fedeli P. et al. Artificial intelligence and digital medicine for integrated home care services in Italy: Opportunities and limits. Front Public Health. 2023; 10: 1095001. <https://doi.org/10.3389/fpubh.2022.1095001>
29. Jleli M., Samet B., Dutta A.K. Artificial Intelligence-driven Remote Monitoring Model for Physical Rehabilitation. Journal of Disability Research. 2024; 3(1). <https://doi.org/10.57197/JDR-2023-0065>
30. Прончев Г.Б. О проблемах информационной безопасности использования информационно-коммуникационных технологий и искусственного интеллекта в цифровом здравоохранении. Социально-гуманитарные знания. 2022; 2: 100–107. <https://doi.org/10.34823/SGZ.2022.2.51777> [Pronchev G.B. On the problems of information security in the use of information and communication technologies and artificial intelligence in digital health. Social and humanitarian knowledge. 2022; 2: 100–107. <https://doi.org/10.34823/SGZ.2022.2.51777> (In Russ.).]
31. Murdoch B. Privacy and artificial intelligence: challenges for protecting health information in a new era. BMC Med Ethics. 2021; 22(1): 122. <https://doi.org/10.1186/s12910-021-00687-3>
32. European Parliament. Available at: <https://www.europarl.europa.eu/portal/en> (Accessed: 14.06.2024).
33. Federspiel F., Mitchell R., Asokan A. et al. Threats by artificial intelligence to human health and human existence. BMJ Global Health. 2023; 8(5): e010435. <https://doi.org/10.1136/bmjgh-2022-010435>
34. Agboola S.O., Bates D.W., Kvedar J.C. Digital Health and Patient Safety. JAMA. 2016; 315(16): 1697–1698. <https://doi.org/10.1001/jama.2016.2402>
35. GitHub. CBDRH Health Data Science Datathon 2023. Available at: <https://cbdrh-hds-datathon-2023.github.io/> (Accessed: 14.06.2024).
36. Musselman K.E., Shah M., Zariffa, J. Rehabilitation technologies and interventions for individuals with spinal cord injury: Translational potential of current trends. J. Neuroeng. Rehabil. 2018; 15: 40. <https://doi.org/10.1186/s12984-018-0386-7>
37. Boot F.H., Owuor J., Dinsmore J. et al. Access to assistive technology for people with intellectual disabilities: a systematic review to identify barriers and facilitators. J. Intell. Disabil. Res. 2018; 62(10): 900–921. <https://doi.org/10.1111/jir.12532>
38. Uniform Data System. Available at: <https://www.udsmr.org/products/inpatient-rehab> (Accessed: 14.06.2024).
39. Canadian Institute for Health Information. (Accessed: 14.06.2024). Available at: <https://www.canada.ca/en/institutes-health-research/search.html?cdn=irscchir&st=s&num=10&langs=eng&st1rt=0&s5bm3ts21rch=x&q=NRS#wb-land>
40. Government of Canada. Public release of clinical information: guidance document. (Accessed: 14.06.2024). Available at: <https://www.canada.ca/en/health-canada/services/drug-health-product-review-approval/profile-public-release-clinical-information-guidance/document.html>
41. Brouns B., Meesters J.J.L., Wentink M.M. et al. Why the uptake of eRehabilitation programs in stroke care is so difficult-a focus group study in the Netherlands. Implement Sci. 2018; 13(1): 133. <https://doi.org/10.1186/s13012-018-0827-5>
42. Svenskt Register for Rehabiliteringsmedicin. Available at: <https://svereh.registercentrum.se/> (Accessed: 13.06.2024).
43. UK ROC. UK Rehabilitation Outcomes Collaborative. Available at: <https://www.ukroc.org/> (Accessed: 14.06.2024).
44. Mousavi Baigi S.F., Sarbaz M., Sobhani-Rad D. et al. Comparative Study of Rehabilitation Information Systems in 8 Countries: A Literature Review. Iranian Rehabilitation Journal. 2022; 20(4): 1–16. <http://dx.doi.org/10.32598/irj.21.1.1766.1>