УДК 614.253.6/.84:004.056

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ ПАЦИЕНТА ПРИ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: СОСТОЯНИЕ ПРОБЛЕМЫ В РОССИИ И ЗА РУБЕЖОМ, СЛАБЫЕ ЗОНЫ И СОВРЕМЕННЫЕ ТРЕНДЫ

[1]Петрушина М.В., [2]Изотов О.И.

[1]Акционерное общество (АО) А771, Москва, e-mail: mar.petrushina@yandex.ru;
[2]ФГБОУ ВО «Российский университет медицины» Минздрава России, Москва

Современные технологии искусственного интеллекта трансформируют медицину, обеспечивая высокую точность диагностики и персонализацию лечения. Однако их внедрение связано с обработкой чувствительных персональных данных пациентов, что требует усиления мер защиты конфиденциальности. Цель исследования – оценить состояние правового регулирования и технических решений в области защиты данных при использовании искусственного интеллекта в медицине в России и за рубежом, выявить слабые зоны и перспективные тренды. Материалы и методы включали анализ нормативно-правовой базы, научных публикаций, кейсов внедрения систем искусственного интеллекта, экспертные интервью с представителями здравоохранения и индустрии информационных технологий, а также оценку технологий, таких как Federated learning и блокчейн. Результаты показали, что в России отсутствуют специализированные нормы для искусственного интеллекта, при этом 40% клиник не соответствуют требованиям кибербезопасности. За рубежом лидируют страны с комплексными стратегиями (Европейское сообщество, Китай, США), где сочетаются жесткие стандарты и инновационные подходы. Основные проблемы включают недостаточную цифровую грамотность медперсонала, риск обратной идентификации данных и этические дилеммы, связанные с дискриминацией алгоритмов. Выводы указывают на необходимость разработки специализированных законов, инвестиций в кибербезопасность, внедрения «регуляторных песочниц» и участия в международных стандартах обмена данными. Без системного подхода Россия рискует утратить доверие пациентов и отставание в развитии систем искусственного интеллекта в медицине.

Ключевые слова: здравоохранение, пациент, защита персональных данных, искусственный интеллект, лечение, безопасность, информация, блокчейн, «регуляторные песочницы», federated learning, международное сотрудничество

PROTECTION OF PATIENTS' PERSONAL DATA WHEN USING ARTIFICIAL INTELLIGENCE TECHNOLOGIES: CURRENT STATE OF THE PROBLEM IN RUSSIA AND ABROAD, WEAKNESSES AND MODERN TRENDS

[1]Petrushina M.V., [2]Izotov O.I.

[1]Joint-Stock Company (JSC) A771, Moscow, e-mail: mar.petrushina@yandex.ru;
[2]Russian Medical University of the Ministry of Health of the Russian Federation, Moscow

Modern artificial intelligence technologies are transforming medicine, providing high diagnostic accuracy and personalized treatment. However, their implementation involves processing patients' sensitive personal data, which requires strengthening privacy protection measures. The aim of the research is to assess the current state of legal regulations and technical solutions for data protection when applying artificial intelligence in medicine in Russia and abroad, identifying weak spots and promising trends. Materials and methods included analyzing legal frameworks, scientific publications, cases of artificial intelligence systems implementation, expert interviews with healthcare and information technology industry representatives, as well as evaluating technologies such as federated learning and blockchain. Results showed that Russia lacks specialized regulations for artificial intelligence, with 40% of clinics failing to meet cybersecurity requirements. Countries with comprehensive strategies (European Union, China, USA) are leading globally, combining stringent standards with innovative approaches. Main issues include insufficient digital literacy of medical staff, data re-identification risks, and ethical dilemmas related to algorithmic discrimination. Conclusions highlight the need for specialized legislation, investments in cybersecurity, implementation of "regulatory sandboxes," and participation in international data exchange standards. Without a systemic approach, Russia risks losing patients' trust and lagging in the development of medical artificial intelligence systems.

Keywords: healthcare, patient, personal data protection, artificial intelligence, treatment, security, information, blockchain, regulatory sandboxes, federated learning, international cooperation

Введение

Современные технологии искусственного интеллекта (ИИ) трансформируют медицину, обеспечивая высокую точность диагностики, автоматизацию процессов и персонализацию лечения. Однако широкое внедрение ИИ в здравоохранение связано с обработкой огромных объемов персональных данных пациентов, включая чувствительную медицинскую информацию. Это поднимает острые вопросы защиты конфиденциальности, особенно в условиях цифровизации и межведомственного взаимодействия. Проблема становится глобальной:

страны сталкиваются с вызовами в регулировании, технической реализации и этическом аспекте [1; 2].

Мировой рынок сбора и маркировки данных в здравоохранении в 2025 году ожидаемо достигнет 1,37 млрд долларов, при этом до 2037 года он может вырасти на 20,83 млрд долларов при среднегодовом темпе роста 25,8%[1]. Кроме того, по прогнозам, общий рынок информационных технологий (IT) в медицине достигнет 662 млрд долларов к 2026 г.[2] ИИ-системы уже сейчас обрабатывают до 40% этих данных, обеспечивая анализ изображений, прогнозирование заболеваний и оптимизацию лечения [3]. Однако, как отмечают эксперты, только 30% стран мирового сообщества имеют специализированные нормативные рамки для защиты данных в ИИ-медицине[3]. В России, как и за рубежом, усилия направлены на баланс между инновациями и правами пациентов. Анализ текущего состояния, выявление «слабых зон» и прогнозирование трендов позволит сформировать стратегию безопасного развития ИИ-медицины.

По итогам исследования сети клиник «Будь Здоров» и страховой компании «Ингосстрах» были получены такие результаты: 51% граждан допускают использование ИИ для диагностики заболеваний и назначения лечения, 48% из них готовы частично довериться технологиям и лишь 3% – полностью. Одна из причин – опасения о нарушении конфиденциальности пациентов. Аналогичные данные приводит Всероссийский центр изучения общественного мнения (ВЦИОМ): 68% россиян считают, что их права на конфиденциальность в цифровом здравоохранении недостаточно защищены[4]. Эти проблемы требуют системного подхода, объединяющего правовое регулирование, технические меры и этические принципы.

Тем не менее цифровизация здравоохранения в России движется семимильными шагами, и применение технологий ИИ в диагностике и лечении является одним из самых приоритетных направлений в развитии российской медицины.

Внедрение ИИ в российской медицинской практике могут проиллюстрировать следующие примеры:

- Сбербанк разработал платформу Sber Health, которая использует ИИ для анализа жалоб пациентов и предварительной диагностики. В 2023 г. платформа обрабатывала более 100 000 обращений в месяц, но столкнулась с критикой из-за недостаточной прозрачности в вопросах обработки персональных данных;

- Яндекс совместно с Институтом нейрохирургии имени Бурденко внедрил ИИ для анализа МРТ головного мозга. Проект повысил точность диагностики опухолей на 15%, однако также требует строгого контроля конфиденциальности данных [4].

Исследование, опубликованное в электронном журнале «Медвестник», показало, что несмотря на то, что половина россиян считает, что искусственный интеллект может использоваться в диагностике и лечении, только каждый шестой готов доверить нейросети собственное здоровье, в том числе – из-за опасений нарушения конфиденциальности их данных [5].

По данным газеты «Ведомости», на июнь 2025 года около 83% организаций сферы здравоохранения недостаточно защищены от киберугроз, так как в их информационной инфраструктуре есть неустранённые критические уязвимости[6].

Цель исследования – оценить состояние регулирования и практики защиты персональных данных пациентов при использовании ИИ в медицине в России и за рубежом, выявить ключевые проблемы и перспективные направления развития.

Задачи

1. Изучить правовые и технические рамки защиты данных в сфере ИИ-медицины, включая российские законы (ФЗ-152, ФЗ-323) и международные стандарты (GDPR, HIPAA).

2. Провести сравнительный анализ подходов в России, ЕС, США и странах Азии,

[1] Research Nester, Размер и доля рынка сбора и маркировки данных в сфере здравоохранения по типам данных (изображение, аудио, видео, текст); Конечное использование – SWOT-анализ, стратегический анализ конкуренции, региональные тенденции 2025-2037гг., ID отчёта: 6612, дата публикации: 10.01.2025; URL: https://www.researchnester.com/ru/reports/healthcare-data-collection-and-labeling-market/6612 (дата обращения: 07.07.2025).

[2] Блог компании ITSoft, IT-гиганты нацелились на медицину. Что это значит для нас? – дата публикации: 20.07.2021; URL: https://habr.com/ru/articles/568584/ (дата обращения: 07.07.2025).

[3] World Health Organization. Ethics and governance of AI for health. Geneva: WHO guidance, 2021.; URL: https://www.who.int/publications/i/item/9789240029200 (дата обращения: 07.07.2025).

[4] ВЦИОМ, Прогресс или угроза, или об искусственном интеллекте в медицине, дата публикации: 17.10.2023; URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/progress-ili-ugroza-ili-ob-iskusstvennom-intellekte-v-medicine (дата обращения: 07.07.2025).

[5] Шамардина Л. Больше 80% россиян не готовы доверить собственную диагностику и лечение нейросети // «Медвестник», дата публикации: 16.02.2023; URL: https://medvestnik.ru/content/news/Bolshe-80-rossiyan-ne-gotovy-doverit-sobstvennuu-diagnostiku-i-lechenie-neiroseti.html (дата обращения: 07.07.2025).

[6] Более 80% организаций здравоохранения не защищены от хакеров // Ведомости. Дата публикации: 19.06.2025. URL: https://www.vedomosti.ru/press_releases/2025/06/19/bolee-80-organizatsii-zdravoohraneniya-ne-zaschischeni-ot-hakerov (дата обращения: 08.07.2025).

выявив различия в регулировании и технологических решениях.

3. Определить слабые места в текущих системах: риски утечек, дефицит регулирования, этические дилеммы.

4. Выявить технологические и управленческие тренды для повышения безопасности данных.

Материалы и методы исследования

Исследование основано на анализе нормативно-правовой базы, научных публикаций и отчетов международных организаций (ВОЗ, OECD). Для сравнительного анализа использовались данные по России, странам ЕС, США, Китаю и Японии. Методы включали:

- анализ более 60 российских и зарубежных источников информации в ведущих электронных и печатных изданиях;
- качественный анализ правовых актов (ФЗ-152, GDPR, HIPAA, NMPA);
- обзор кейсов внедрения ИИ в медицину (диагностика, телемедицина, анализ больших данных);
- экспертные интервью с представителями Минздрава, IT-компаний и юристов;
- анализ использования ИИ для диагностики рака, телемедицинских консультаций и анализа больших данных (Big Data) на примере систем IBM Watson Health (США), проекта DeepMind (Великобритания), платформы Ping An Good Doctor (Китай);
- оценку технологических решений: анализ эффективности обезличивания данных, шифрования, Federated learning и блокчейна на примере проекта MedRec (блокчейн в США), федеральных систем обмена данными в ЕС.

Результаты исследования и их обсуждение

1. Правовое регулирование.

Россия

Защита данных в здравоохранении регулируется ФЗ-152 и ФЗ-323, которые требуют согласия пациентов на обработку данных, обезличивания при использовании ИИ и минимальных мер безопасности согласно Постановлению Правительства РФ № 1119[7]. При анализе открытых источников информации авторы столкнулись с тем, что в здравоохранении всё ещё существует недопонимание и ряд разночтений в текущем законодательстве. Медицинским работникам не совсем понятно, что именно следует считать персональными данными пациента, а что – врачебной тайной, и какие уровни защиты предусмотрены для каждого из определений [5].

Важным шагом на пути регулирования защиты персональных данных пациента стало издание Приказа Минздрава № 965н «Об утверждении порядка организации и оказания медицинской помощи с применением телемедицинских технологий», который устанавливает правила оказания телемедицинских услуг. В частности, документ обязывает медицинские учреждения:

• обеспечить шифрование данных при передаче через Интернет;

• использовать системы контроля доступа (например, двухфакторную аутентификацию);

• обезличивать данные при их передаче в ИИ-системы для анализа[8].

Эти положения напрямую связаны с защитой конфиденциальности пациентов, особенно при внедрении ИИ в телемедицинские консультации. Однако эксперты отмечают, что реализация требований затруднена из-за отсутствия единой методики для ИИ-систем [6].

Кроме того, критика связана с отсутствием специализированных норм для ИИ. В 2023–2024 годах Минцифры РФ продвигало инициативы по регулированию ИИ: стратегия развития искусственного интеллекта в РФ до 2030 года (утверждена в 2023 г.) включает положения о защите данных в ИИ-системах, включая обязательную сертификацию «высокорисковых» алгоритмов[9].

Законопроект «О регулировании искусственного интеллекта», который находится на рассмотрении в Госдуме, предполагает создание реестра ИИ-систем, обязывающего разработчиков соблюдать требования конфиденциальности и прозрачности.

В рамках Национального проекта «Кибербезопасность» запущен пилотный проект по внедрению стандартов ИИ-безопасности в здравоохранении, включающий шифрование данных и контроль доступа[10].

[7] Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»; URL: https://base.garant.ru/70252506/ (дата обращения: 07.07.2025).

[8] Приказ Министерства здравоохранения РФ от 30 ноября 2017 г. № 965н «Об утверждении порядка организации и оказания медицинской помощи с применением телемедицинских технологий»; URL: https://www.garant.ru/products/ipo/prime/doc/71751294/ (дата обращения: 07.07.2025).

[9] «Национальная стратегия развития искусственного интеллекта на период до 2030 года», дата публикации:15.02.2024. URL: https://ai.gov.ru/knowledgebase/dokumenty-po-razvitiyu-ii-v-rf/nacionalynaya_strategiya_razvitiya_iskusstvennogo_intellekta_na_period_do_2030_goda/ (дата обращения: 07.07.2025).

[10] Минцифры. Национальный проект «Кибербезопасность». URL: https://digital.gov.ru/activity/kiberbezopasnost (дата обращения: 07.07.2025).

ЕС

GDPR устанавливает строгие правила на основе принципа «прозрачности» и требует оценки рисков при ИИ-обработке. В 2023 г. Еврокомиссия одобрила закон об искусственном интеллекте, классифицирующий медицинские ИИ-системы как «высокорисковые», что усиливает требования к защите данных[11].

США

HIPAA ограничивает раскрытие данных, собранных медицинскими учреждениями, но ограничение не распространяется на данные с носимых устройств (например, фитнес-трекеров). Однако если данные передаются в клиники или страховые компании, подчиняющиеся HIPAA, они автоматически попадают под регулирование. Пример: Apple Health сотрудничает с клиниками США, где данные пациентов обрабатываются в соответствии с HIPAA[12] [7].

Китай

Закон об интернет-безопасности, принятый в Китае в 2021 г., усиливает контроль государства над медицинскими данными. Согласно закону, ИИ-системы обязаны проходить сертификацию перед внедрением, а данные пациентов хранятся в защищенных государственных облаках[13].

Таким образом, в России в текущее время наблюдается дефицит специализированных норм для ИИ, но проблематику уже невозможно игнорировать, и новые инициативы Минцифры начали закладывать основы регулирования конфиденциальности персональных данных, тогда как в ЕС и Китае уже действуют четкие стратегии, закреплённые законодательно.

2. Технические меры.

Обезличивание данных – в России применяется недостаточно эффективно из-за риска обратной идентификации. Например, в 2022 г. в одном из регионов произошла утечка обезличенных данных, позволившая восстановить личности пациентов[14]. В ЕС и США активно используются алгоритмы дифференциальной приватности, которые добавляют «шум» к данным, предотвращая их идентификацию.

С 2005 по 2019 год общее количество утечек данных в здравоохранении составило 249,9 миллиона. По словам нескольких специалистов, общее число людей, пострадавших от утечек данных в здравоохранении, составило 249,09 миллиона за этот же период. Только за предыдущие пять лет пострадали 157,40 миллиона человек [8].

Безопасность ИИ-систем – российские медучреждения часто игнорируют требования шифрования и контроля доступа (Постановление № 1119). По данным Роскомнадзора, 40% клиник не имеют систем обнаружения угроз, тогда как, например, в Японии внедрены стандарты JIS Q 15001, которые требуют ежегодного аудита безопасности данных. В России существуют разногласия между разработчиками программного обеспечения и пользователями цифровых систем, где сложно определить сторону, отвечающую за утечку персональных данных [9].

Federated learning

Перспективным методом, позволяющим обучать модели ИИ без передачи данных в облако, является Federated learning. Например, NVIDIA Clara Federated Learning активно используется в США и ЕС для обучения ИИ-моделей на данных из разных клиник без их централизованного хранения. Проект Federated Tumor Segmentation (FeTS) использует эту платформу для анализа МРТ-снимков пациентов с опухолями мозга.

Слабые места:

- недостаточная цифровая грамотность медперсонала. По данным из открытых источников, только 20% врачей в России прошли обучение по защите данных, а 68% не знакомы с основами кибербезопасности [10];

- из отчёта «Киберугрозы в здравоохранении: Россия в 2023 году» компании «Лаборатория Касперского» – 65% российских клиник используют устаревшие антивирусы без функции машинного обучения, а ИИ-мониторинг угроз внедрен только в 12% медицинских учреждений;

- согласно сравнительному анализу GDPR и российского законодательства, в России нет аналога европейских Data Protection Authorities (DPAs), что приводит к недостаточному контролю за соблюдением ФЗ-152 в здравоохранении [11].

3. Этические и социальные аспекты.

Согласие пациентов. В России, согласно исследованию НИУ ВШЭ, выполненному в 2023 году, 70% пациентов не осведомлены о том, как ИИ-системы обрабатывают их данные, а 63% не понимают, какие риски связаны с использованием искусственного

[11] European Commission. «AI Act». URL: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai (дата обращения: 07.07.2025).

[12] U.S. Department of Health & Human Services. «Summary of the HIPAA Privacy Rule». URL: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (дата обращения: 07.07. 2025).

[13] National Medical Products Administration (NMPA). China's Regulation on the Administration of Medical Devices. URL: https://www.nmpa.gov.cn/zwgk/tzgg/index.html (дата обращения: 07.07.2025).

[14] Данные растут в цене // Коммерсантъ. Дата публикации: 24.04.2025. URL: https://www.kommersant.ru/doc/7675231?ysclid=mct8f28wni756030426 (дата обращения: 07.07.2025).

интеллекта. Это указывает на дефицит информированного согласия, несмотря на требования ФЗ-323[15].

В отличие от российских реалий, в ЕС пациентам предоставляют детальные объяснения о целях обработки их персональных данных. Например, в Германии обязательна письменная форма согласия с описанием рисков. По данным опроса пациентов в многопрофильной больнице Великобритании, уровень знаний респондентов об ИИ был низким, при этом большинство из них были готовы делиться данными с Национальной службой здравоохранения (77,9%), но менее готовы передавать свои данные коммерческим организациям и технологическим компаниям. Основная причина – опасения относительно приватности и конфиденциальности информации [12].

Дискриминация ИИ. В США зафиксированы случаи смещения алгоритмов в сторону определенных расовых групп. Например, исследование Obermeyer с соавторами, опубликованное в журнале Science, показало, что алгоритм диагностики диабета компании Optum давал заниженные оценки риска осложнений у пациентов африканского происхождения из-за использования исторических данных о расходах на лечение, а не основываясь на реальных потребностях [13]. Аналогичные результаты получены в исследовании Stanford Medicine, где нейросети, обученные на несбалансированных данных, демонстрировали снижение точности диагностики на 15–20% для пациентов с темным цветом кожи [14].

В России таких исследований пока нет, но эксперты предупреждают о похожих рисках, если данные для обучения ИИ будут нерепрезентативными.

4. Тренды развития

Метод Federated learning, позволяющий обучать ИИ-модели без передачи данных в облако, активно развивается за рубежом (примеры: NVIDIA Clara Federated Learning в США, проекты Google Health). В России пока нет массовых пилотных проектов FL в здравоохранении, однако в 2022 году стартовал проект по дистанционному мониторингу состояния здоровья пациентов с использованием диагностических приборов – данные с них поступают на цифровую платформу для дальнейшей обработки врачами-специалистами из медицинских центров. В рамках проекта пациентам с диабетом или гипертонией выдаются диагностические приборы, данные с которых поступают на платформу, а затем обрабатываются врачами[16].

Минцифры РФ подчеркивает, что развитие FL станет одним из приоритетов для обеспечения конфиденциальности данных в ИИ-медицине в ближайшем будущем.

Блокчейн

Блокчейн – это децентрализованная распределенная база данных, которая обеспечивает:

- неизменность записей: данные нельзя изменить или удалить без согласия всех участников сети;
- прозрачность: все операции с данными отслеживаются и хранятся в виде цепочки блоков;
- контроль доступа: пациенты могут управлять правами на свои данные через смарт-контракты.

В здравоохранении блокчейн применяется для:

- хранения медицинских записей (электронные истории болезни);
- управления доступом к данным (например, обмен между клиниками и пациентами);
- децентрализованного хранения данных.

Примером может послужить проект MedRec в США, который позволяет пациентам контролировать доступ к своим данным через блокчейн. В Эстонии – проект Guardtime, специализирующийся на обеспечении безопасности данных – применяется для защиты данных систем электронного здравоохранения страны. В проекте Hashed Health (США) блокчейн применяется для обмена данными между страховыми компаниями, клиниками и пациентами.

В России блокчейн пока не получил массового распространения в здравоохранении, но есть пилотные проекты. Большинство проектов находится на начальной стадии и реализуется в основном в рамках частных инициатив. Информация о конкретных результатах, достигнутых в рамках анонсированных проектов, недоступна. Среди известных блокчейн-инициатив российских медицинских учреждений – применение блокчейна для хранения медицинских данных в ОАО «Медицина», а также использование технологии для контроля медицинских услуг сетью «Открытая клиника». В качестве региональных проектов следует выделить использование блокчейна

[15] Федеральный закон от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации». URL: https://minzdrav.gov.ru/documents/7025 (дата обращения: 08.07.2025).

[16] Министерство здравоохранения РФ. В России стартовал пилотный проект по дистанционному мониторингу состояния здоровья пациентов с использованием высокотехнологичных устройств и сервисов. Дата публикации: 29.12.2022. URL: https://minzdrav.gov.ru/news/2022/12/29/19716-v-rossii-startoval-pilotnyy-proekt-po-distantsionnomu-monitoringu-sostoyaniya-zdorovya-patsientov-s-ispolzovaniem-vysokotehnologichnyh-ustroystv-i-servisov (дата обращения: 07.07.2025).

для мониторинга оборота лекарств в больнице Новгородской области. Московская область еще в 2017 г. анонсировала планы по использованию блокчейна для хранения медицинских карт граждан [15].

На сегодняшний день и в России, и в других странах отсутствуют четкие нормы для использования блокчейна в здравоохранении, кроме того, интеграция блокчейна с существующими системами (например, ЕГИС) требует значительных инвестиций.

Регуляторные песочницы

«Регуляторная песочница» – это контролируемая среда, созданная государственным регулятором, где компании могут тестировать инновационные продукты, технологии или бизнес-модели под надзором с ограниченными рисками. В здравоохранении такие песочницы позволяют:

- тестировать ИИ-системы для диагностики, прогнозирования заболеваний и обработки персональных данных;
- соблюдать требования ФЗ-152 (защита персональных данных) и ФЗ-323 (конфиденциальность медицинской информации);
- минимизировать юридические барьеры для внедрения технологий без полной лицензии.

В 2024 году Минцифры РФ запустило пилотные «регуляторные песочницы» для тестирования ИИ-продуктов в здравоохранении – проект, который Минздрав совместно с Минэкономразвития и Минцифры подготовил для использования обезличенных медицинских данных без согласия пациентов. Планируется, что до конца 2025 года установят экспериментальный правовой режим (ЭПР) в сфере медицинских данных. Тестирование будет проходить в течение трёх лет на территории всей страны. Обезличенные данные в рамках ЭПР будут использоваться для научных исследований, опытно-конструкторских работ и разработок моделей машинного обучения, а также для исследования реальной клинической практики, например оценки и контроля качества применения лекарственных средств при оказании медицинской помощи. Сбор, обработка и анализ обезличенных данных будут осуществляться на специальной цифровой платформе, доступ к которой будет предоставлен ограниченному кругу лиц[17].

Международное сотрудничество

Global Health Data Exchange (GHDx) – это платформа, разработанная Институтом метрики и оценки в здравоохранении (IHME) при Вашингтонском университете (США). Основная цель GHDx – создание открытой базы данных для глобального обмена информацией о здоровье, включая эпидемиологические данные, результаты исследований и данные о применении ИИ в медицине.

Ключевые функции:

- стандартизация данных: GHDx внедряет международные стандарты, такие как FHIR (Fast Healthcare Interoperability Resources), которые позволяют унифицировать форматы хранения и обмена медицинскими данными;
- открытый доступ: платформа предоставляет бесплатный доступ к данным о заболеваниях, вакцинации, демографии и других показателях здоровья;
- поддержка ИИ-исследований: данные GHDx используются для обучения и тестирования ИИ-моделей, например, для прогнозирования эпидемий или анализа эффективности лечения.

Участники платформы: более 180 стран, включая Россию и Китай[18].

В 2021 году ВОЗ опубликовала рекомендации по этическому использованию ИИ в медицине, включая требования к защите данных и прозрачности алгоритмов[19].

В июле 2024 года сообщалось, что ведущие медицинские вузы России и Китая договорились развивать сотрудничество в сферах цифровой и персонализированной медицины. Некоторые аспекты, обсуждавшиеся на двусторонней тематической встрече:

- использование искусственного интеллекта, больших данных и других передовых технологий для улучшения качества медицинского обслуживания;
- разработка и внедрение персонализированных методов лечения и профилактики заболеваний[20].

Заключение

Современные ИИ-технологии открывают новые горизонты для медицины, но требуют усиленной защиты персональных данных. В России ключевые проблемы включают правовой разрыв в регулировании ИИ, техническую уязвимость систем и недостаточную информированность пациентов. За рубежом лидируют страны с комплексными стратегиями (США, ЕС, Китай), где

[17] Арялина М. Минздрав, Минцифры и Минэк смогли договориться об эксперименте с медданными // Ведомости. Дата публикации: 17.03.2025. URL: https://portal.egisz.rosminzdrav.ru/news/1009 (дата обращения: 07.07.2025).

[18] Global Health Data Exchange. URL: https://ghdx.healthdata.org/ (дата обращения: 07.07.2025).

[19] World Health Organisation. Global Initiative on AI for Health. URL: https://www.who.int/initiatives/global-initiative-on-ai-for-health (дата обращения: 07.07.2025).

[20] Медвузы России и КНР договорились о сотрудничестве в цифровой медицине. // Риа Новости. Дата публикации: 06.07.2024. URL: https://ria.ru/20240706/medvuzy-1957904633.html (дата обращения: 07.07.2025).

сочетаются жесткие нормы и стимулирование инноваций.

На основании полученных и проанализированных данных можно выделить следующие направления развития кибербезопасности при использовании ИИ в медицинских учреждениях Российской Федерации:

- разработка юридических основ применения ИИ в здравоохранении, включая ответственность разрабатывающей стороны и пользователей за полученные результаты;
- увеличение объёмов финансирования обеспечения мероприятий кибербезопасности, внедрение закрытых каналов шифрования, Federated learning и проведение регулярных проверок;
- обучение медицинского персонала основам кибербезопасности и кибергигиены в лечебных учреждениях, информирование пациентов об их правах и рисках при использовании ИИ в здравоохранении;
- широкое применение практики «регуляторных песочниц» для создания и тестирования инновационных продуктов с использованием ИИ, учитывая необходимость контроля конфиденциальности;
- участие в международных платформах по обмену данными информации о здоровье пациентов, разработанных с учётом мировых стандартов защиты персональных данных (например, GHDx).

Без решительных мер Россия рискует отстать в гонке за лидерство в ИИ-медицине, потеряв доверие пациентов и инвестиции, которые в приоритетном порядке государство и частный бизнес выделяют на разработку новых продуктов, связанных с применением ИИ в здравоохранении.

Список литературы

1. Elendu C., Amaechi D.C., Elendu T.C., Jingwa K.A., Okoye O.K., John Okah M., et al. Ethical implications of AI and robotics in healthcare: a review // Medicine (Baltimore). 2023. Vol. 102(50). № e36671. DOI: 10.1097/MD.0000000000036671. URL: https://pubmed.ncbi.nlm.nih.gov/38115340/ (дата обращения: 24.07.2025).

2. Marques M., Almeida A., Pereira H. The medicine revolution through artificial intelligence: ethical challenges of machine learning algorithms in decision-making // Cureus. 2024. Vol. 16(9). № e69405. DOI: 10.7759/cureus.69405. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC11473215/ (дата обращения: 24.07.2025).

3. Jiang F., et al. Artificial intelligence in healthcare: past, present and future // Stroke Vasc Neurol. 2017. Vol. 2(4). P. 230–243. DOI: 10.1136/svn-2017-000101 (дата обращения: 24.07.2025).

4. Данилов Г.В., Ишанкулов Т.А., Котик К.В., Шифрин М.А., Потапов А.А. Технологии искусственного интеллекта в клинической нейроонкологии // Вопросы нейрохирургии им Н.Н. Бурденко. 2022. Vol. 86(6). С. 127–133. DOI: 10.17116/neiro202286061127. URL: https://www.mediasphera.ru/issues/zhurnal-voprosy-nejrokhirurgii-imeni-n-n-burdenko/2022/6/1004288172022061127 (дата обращения: 24.07.2024).

5. Ваулин Г.Ф., Тихомирова А.А., Котиков П.Е. Защита персональных данных пациентов в медицинских информационных системах // FORCIPE. 2022. Vol. 5(S2). С. 111–112. URL: https://ojs3.gpmu.org/index.php/forcipe/article/view/4428 (дата обращения: 24.07.2025).

6. Li Y.H., Li Y.L., Wei M.Y., Li G.Y. Innovation and challenges of artificial intelligence technology in personalized healthcare // Sci Rep. 2024. Vol. 14. № 18994. DOI: 10.1038/s41598-024-70073-7. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC11329630/ (дата обращения: 18.07.2025).

7. Tariq R.A., Hackert P.B. Patient confidentiality. 2023 Jan 23. In: StatPearls [Internet]. Treasure Island (FL): StatPearls Publishing. 2025. URL: https://pubmed.ncbi.nlm.nih.gov/30137825/ (дата обращения: 24.07.2025).

8. Khalid N., Qayyum A., Bilal M., Al-Fuqaha A., Qadir J. Privacy-preserving artificial intelligence in healthcare: techniques and applications // Comput Biol Med. 2023. Vol. 158. № 106848. DOI: 10.1016/j.compbiomed.2023.106848. URL: https://pubmed.ncbi.nlm.nih.gov/37044052/ (дата обращения: 24.07.2025).

9. Гаев Л.В., Пахомов А.А., Клименко Н.Д. Кибербезопасность в медицинских учреждениях: защита личных данных пациентов. В кн.: Человек и общество в современном киберпространстве: материалы III Международной научной конференции молодых ученых (26 апреля 2024 г. Москва). М.: Энциклопедист-Максимум, 2024. С. 61–66. EDN: WJUHBH. URL: https://elibrary.ru/WJUHBH (дата обращения: 23.07.2025).

10. Казанфарова М.А., Природова О.Ф., Ардаширова Н.С. Развитие цифровых компетенций медицинских работников // Медицинское образование и профессиональное развитие. 2023. Vol. 14(2). С. 109–122. DOI: 10.33029/2220-8453-2023-14-2-109-122.

11. Денисов И.С., Ахматова Д.Р., Кабакова В.М. Сравнительная характеристика GDPR и российского законодательства о персональных данных // Экономика. Право. Общество. 2019. Vol. 1. С. 21–27. URL: https://epo.rea.ru/jour/article/view/115/108 (дата обращения: 23.07.2025).

12. Aggarwal R., Farag S., Martin G., Ashrafian H., Darzi A. Patient perceptions on data sharing and applying artificial intelligence to health care data: cross-sectional survey // J Med Internet Res. 2021. Vol. 23(8). № e26162. DOI: 10.2196/26162. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC8430862/ (дата обращения: 24.07.2025).

13. Obermeyer Z., Powers B., Vogeli C., Mullainathan S. Dissecting racial bias in an algorithm used to manage the health of populations // Science. 2019. Vol. 366(6464). DOI: 10.1126/science.aax2342. URL: https://pubmed.ncbi.nlm.nih.gov/31649194/ (дата обращения: 07.07.2025).

14. Shanklin R., Samorani M., Harris S., et al. Ethical redress of racial inequities in AI: lessons from decoupling machine learning from optimization in medical appointment scheduling // Philos Technol. 2022. Vol. 35. № 96. DOI: 10.1007/s13347-022-00590-8. URL: https://link.springer.com/article/10.1007/s13347-022-00590-8 (дата обращения: 07.07.2025).

15. Куракова Н.Г., Черченко О.В., Цветкова Л.А. Технологии блокчейн в здравоохранении: позиции России на глобальном публикационном ландшафте // Врач и информационные технологии. 2021. Vol. 1. P. 25–39. DOI: 10.25881/ITP.2021.59.48.003. URL: https://cyberleninka.ru/article/n/tehnologii-iskusstvennogo-intellekta-v-meditsine-i-zdravoohranenii-pozitsii-rossii-na-globalnom-patentnom-i-publikatsionnom/viewer (дата обращения: 24.07.2025).