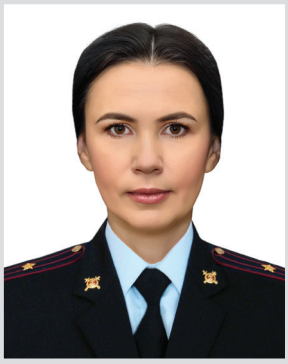
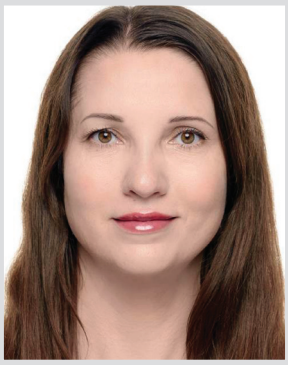
УДК 34.09
DOI: 10.24412/1998-5533-2025-2-139-144

Искусственный интеллект в медицине: проблемы кибербезопасности и этические аспекты



Волченко А.В.
Кандидат юридических наук,
старший преподаватель кафедры уголовного процесса
Белгородского юридического института МВД России
имени И.Д. Путилина, майор полиции

Когтева А.Н.
Кандидат экономических наук,
доцент кафедры информационной безопасности
Финансового университета при Правительстве РФ (Москва)



Тимохина Г.В.
Магистрант Юридического института
Белгородского государственного национального
исследовательского университета

Интеграция искусственного интеллекта в медицину открывает широкие возможности, но одновременно порождает принципиально новые риски для информационной безопасности. Интеллектуальные системы получают доступ к конфиденциальным данным пациентов и участвуют в принятии клинических решений; их уязвимость (например, к атакам с искажением входных данных) может привести к утечке персональной информации или выдаче ошибочных медицинских рекомендаций. Между тем на федеральном уровне отсутствуют специальные требования к кибербезопасности медицинских систем с искусственным интеллектом, а единые этические стандарты их применения в здравоохранении не закреплены нормативно. Это обуславливает актуальность настоящего исследования. Его цель – проанализировать возникшие киберугрозы и этико-правовые пробелы при внедрении искусственного интеллекта в здравоохранение и разработать предложения по совершенствованию нормативной базы и практических мер для обеспечения безопасного и ответственного использования искусственного интеллекта. В ходе работы проведен анализ действующих нормативных актов и стандартов, выявлены ключевые проблемы (отсутствие специальных норм ответственности за ошибки искусственного интеллекта, риск злоумышленных воздействий на алгоритмы, дефицит правил прозрачности и информирования пациентов) и предложены подходы к их устранению. Научная и практическая значимость заключается в том, что полученные результаты могут служить основой для разработки новых требований и рекомендаций по кибербезопасности и этике применения искусствен-

ного интеллекта в медицине. Научная новизна состоит в комплексном рассмотрении вопросов информационной безопасности медицинских интеллектуальных систем с учётом технических, правовых и этических аспектов, а также в обосновании необходимости интеграции специальных мер защиты и прозрачности в существующую нормативно-правовую систему здравоохранения.

Ключевые слова: *искусственный интеллект в медицине, кибербезопасность, информационная безопасность, этические аспекты, правовое регулирование, защита персональных данных, прозрачность алгоритмов*

Для цитирования: *Волченко А.В., Когтева А.Н., Тимохина Г.В. Искусственный интеллект в медицине: проблемы кибербезопасности и этические аспекты // Вестник экономики, права и социологии. 2025. № 2. С. 139–144. DOI: 10.24412/1998-5533-2025-2-139-144.*

Стремительная цифровизация здравоохранения посредством внедрения систем искусственного интеллекта сопровождается появлением новых киберугроз. Однако существующие нормативно-правовые и этические механизмы обеспечения информационной безопасности отстают от развития технологий и не гарантируют должного уровня защиты. Проблема настоящего исследования заключается в противоречии между возрастающими рисками для информационной безопасности при использовании искусственного интеллекта в медицине и отсутствием специальных правовых и этических мер для их предотвращения.

На современном этапе интеграция интеллектуальных систем в клинические процессы порождает новые векторы киберугроз. Алгоритмы имеют доступ к конфиденциальной информации пациентов и способны влиять на принимаемые решения, поэтому их уязвимость (например, к атакам, искажающим входные данные) может привести к утечкам данных или выдаче ошибочных рекомендаций. Тем не менее специальные требования к обеспечению кибербезопасности медицинских интеллектуальных систем пока не закреплены на федеральном уровне (существуют лишь единичные региональные инициативы по этому вопросу).

Наблюдается также дефицит этических регуляторов. В сфере здравоохранения отсутствуют обязательные этические стандарты использования искусственного интеллекта, гарантирующие прозрачность алгоритмов и информированное согласие пациентов. Недостаток четких этико-правовых ориентиров усиливает недоверие к новым технологиям, поскольку значительная часть пациентов настороженно относится к внедрению искусственного интеллекта без гарантий безопасности и ответственности.

Риски для информационной безопасности

Интеграция интеллектуальных систем в медицинские информационные процессы порождает новые векторы киберугроз. Искусственный интеллект в медицинской сфере обычно функционирует в связке с электронными медицинскими системами, получая доступ к чувствительным данным пациентов, а в некоторых случаях – влияя на принятие решений, затрагивающих жизнь и здоровье.

Таким образом, нарушение работы искусственного интеллекта или несанкционированный доступ к нему может привести к тяжким последствиям: от утечки большого объема конфиденциальной информации до выдачи ошибочных рекомендаций по лечению.

Действующие нормативы по защите информации в здравоохранении (приказы Федеральной службы по техническому и экспортному контролю и др.) распространяются на информационные системы персональных данных и государственные системы (типа ЕГИСЗ – Единой государственной информационной системы в сфере здравоохранения), но специально аспекты безопасности искусственного интеллекта не выделяют.

Существуют также риски манипулирования алгоритмами (например, так называемые *adversarial attacks* – внедрение во входные данные небольших искажений с целью ввести в замешательство алгоритм), против которых традиционные меры защиты не всегда эффективны. Кроме того, подключение внешних интеллектуальных сервисов (например, по модели *SaaS*) к медицинским информационным системам порождает угрозы на стыке сетевой безопасности и защиты данных.

Законодательство пока не устанавливает специальных требований к кибербезопасности медицинских интеллектуальных систем. Хотя общие нормы обязывают медицинские организации защищать обрабатываемые ими персональные данные и поддерживать безопасность инфраструктуры, отсутствуют конкретные указания для разработчиков искусственного интеллекта по обеспечению устойчивости алгоритмов к атакам, шифрованию встроенных моделей и т.п.

В ряде случаев региональные власти сами вводят требования: так, Постановление правительства Республики Татарстан от 19.04.2022 г. № 369 «Об использовании технологий искусственного интеллекта в Республике Татарстан» [1] прямо предпи-

сывает при внедрении интеллектуальных сервисов обеспечивать защиту информации и прозрачность принимаемых алгоритмами решений. Однако это единичный пример на региональном уровне. Общероссийские же правила информационной безопасности в контексте искусственного интеллекта пока находятся в стадии формирования.

Обработка данных и конфиденциальность

Персональные медицинские данные составляют основу для обучения и работы медицинских алгоритмов искусственного интеллекта, что обуславливает особую остроту вопросов конфиденциальности и информационной безопасности. Медицинская информация относится к категории специальных персональных данных, охраняется режимом врачебной тайны, установленным в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» [2], согласно требованиям которого сбор и использование персональных данных допустимы лишь для заранее определенных, законных целей и с согласия субъекта. Нарушение этих требований способно ущемить права на неприкосновенность частной жизни пациента.

Широкое внедрение электронных медицинских карт, телемедицины и устройств с интеллектуальным интерфейсом приводит к сбору колоссальных объёмов чувствительных данных (идентификационные сведения, история болезней, результаты анализов, генетическая информация и пр.) для нужд искусственного интеллекта [3, с. 16]. Это порождает существенные риски: несанкционированный доступ, утечки и взломы баз данных могут раскрыть конфиденциальную информацию.

Несанкционированный доступ к медицинским данным ставит под угрозу приватность пациента и его безопасность, подрывая доверие к системе. Пациенты вправе ожидать ответственной обработки своих данных, и нарушение этого доверия влечет далеко идущие негативные последствия как для отдельных лиц, так и для медицинских организаций [4, с. 42]. Кроме внешних киберугроз, существуют и внутренние риски – неправомерное использование данных медицинским персоналом, человеческий фактор [3]. Таким образом, обеспечение кибербезопасности и строгий контроль доступа становятся этическим императивом, дополняющим правовые нормы.

Другой проблемой является дефицит контроля пациентов над своими данными. В сложных экосистемах электронного здравоохранения данные нередко циркулируют между разными сервисами и учреждениями, а пациенты могут не знать, какие сведения собираются, передаются и как используются. Это ведет к ощущению уязвимости и утрате автономии [5, с. 13]. Кроме того, агрегирование разрозненных баз данных для обучения ИИ может непреднамеренно раскрыть личную информацию или привести к повторной идентификации пациентов, даже если данные обезличены, что создает новые риски для конфиденциальности. Эти этические соображения выходят за рамки простого соблюдения норм закона и затрагивают принципы уважения частной жизни и доверия. Пациент должен иметь возможность принимать осознанные решения о сборе и использовании своих медицинских сведений, а медицинские организации обязаны поддерживать высочайшие стандарты защиты данных.

В российском правовом поле защита персональных данных пациентов регламентируется уже упомянутым Федеральным законом № 152-ФЗ «О персональных данных», а также отраслевым законодательством, например, Федеральным законом от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» [6].

Появление искусственного интеллекта потребовало новых подходов. Для ускорения внедрения технологий были предприняты регуляторные эксперименты. Так, Федеральный закон от 24.04.2020 г. № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона № 152-ФЗ» [7] запустил особый правовой режим в городе Москве для испытания решений на основе искусственного интеллекта. Этим актом допущена обработка обезличенных медицинских данных пациентов без их согласия в ряде случаев. По сути, закон позволил использовать большие массивы данных для обучения алгоритмов, ослабив действие общего правила о необходимости предварительного согласия.

Данное нововведение получило неоднозначное восприятие. С одной стороны, выдача автоматических согласий недопустима, поскольку каждый человек имеет право знать, с какой целью используются его сведения. В то же время представляется возможным оборот надлежащим образом обезличенных данных ради общественного блага – ускорения прогресса искусственного интеллекта (при условии гарантированной защиты от деанонимизации).

Таким образом, перед законодателем стоит задача найти баланс между развитием технологий больших данных и защитой прав личности. Необходимо уточнить режим обезличивания данных, установить прозрачные требования к анонимизации, при которых риски идентификации сводятся к минимуму, а также обеспечить внешние проверки (аудит) соблюдения конфиденциальности.

Кроме того, следует усилить ответственность за утечки и неправомерное использование медицинской информации. В информационном праве уже

формируются подходы к информационным данным как к специфическому ресурсу, например, предлагается создание сертифицированных инфраструктур для безопасного обмена медицинскими данными. Без восстановления доверия пациентов к тому, что их данные не станут достоянием третьих лиц, масштабное внедрение искусственного интеллекта в медицине натолкнется на обоснованные этические возражения.

Этические и социальные аспекты

Помимо юридически значимых рисков, применение искусственного интеллекта в медицине ставит этические проблемы (прозрачность решений, возможность дискриминации, необходимость информирования пациента об участии искусственного интеллекта и получения согласия на это и др.). Пока эти вопросы слабо урегулированы нормативно.

В 2021 г. в РФ был принят Этический кодекс разработчиков искусственного интеллекта [8] (на уровне соглашения при поддержке Минэкономразвития), но он носит добровольный характер. Однако в сфере здравоохранения отсутствуют отраслевые этические рекомендации по использованию искусственного интеллекта. Это может приводить к недоверию со стороны пациентов. Например, нет разъяснений, должен ли врач информировать пациента, что при постановке диагноза он опирался на рекомендацию искусственного интеллекта, и нужно ли получать согласие на использование такого инструмента.

Отсутствие четких этико-правовых ориентиров в сочетании с названными выше проблемами (неопределенность ответственности, возможные ошибки алгоритма) в итоге может подорвать доверие к технологиям. По данным опросов, значительная часть людей испытывает настороженность к внедрению искусственного интеллекта без гарантий безопасности и ответственности [9]. Следовательно, в правовом регулировании следует учитывать и этическую составляющую – вводить нормы, обеспечивающие прозрачность и подотчетность использования искусственного интеллекта в отношениях врач – пациент.

Отмеченные проблемы взаимосвязаны: так, отсутствие специальных норм об ответственности и безопасности усложняет и защиту данных, и этическое сопровождение. В совокупности они указывают на необходимость совершенствования законодательства и ведомственных регламентов.

Кибербезопасность интеллектуальных систем в медицинской деятельности

Технологии искусственного интеллекта становятся частью медицинской информационной инфраструктуры и к ним применимы все базовые требования по защите информации, актуальные для здравоохранения. Медицинские организации обязаны соблюдать Приказ ФСТЭК от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [10], устанавливающий требования по защите персональных данных, и связанные регламенты, обеспечивать защиту сетей, шифрование каналов, контроль доступа.

Однако интеллектуальные системы могут иметь уязвимости и особенности, которые требуют дополнительных мер. Например, алгоритмы глубокого обучения подвержены «атакам путем внедрения данных»: злоумышленник, имея доступ, может слегка модифицировать медицинское изображение или запись таким образом, что для человека изменение незаметно, а для искусственного интеллекта приводит к ошибочному выводу.

Предотвращение подобных атак выходит за рамки стандартных методов информационной безопасности. Здесь необходима комбинация мер: регулярное обновление и тестирование моделей на устойчивость к внешним воздействиям, валидация входных данных, мониторинг аномалий в работе алгоритма.

В нормативном аспекте следует разработать руководства или стандарты кибербезопасности применительно к искусственному интеллекту. Всемирная организация здравоохранения в своих рекомендациях по искусственному интеллекту в здравоохранении отмечает, что для укрепления доверия к технологиям критически важна транспарентность и документирование всего жизненного цикла интеллектуальных систем, а также управление рисками, включая учет угроз кибербезопасности [11]. То есть каждый этап – от разработки до эксплуатации – должен сопровождаться мерами безопасности и фиксацией изменений (журналированием).

В российской практике уже делаются шаги: ГОСТ Р 59921.3-2021 и 59921.5-2022 устанавливают требования к управлению изменениями алгоритма и к набору данных, используемых для обучения, что косвенно относится и к безопасности (исключение некорректных данных, недопущение незадокументированных модификаций модели и т.д.). Однако этих технических мер недостаточно без организационной составляющей.

Необходимо, чтобы в каждой медорганизации, использующей искусственный интеллект, были регламенты информационной безопасности для таких систем: порядок обновления алгоритмов (только от доверенных источников и после проверки), разграничение доступа (кто может запускать/настраивать искусственный интеллект, кто имеет доступ к результатам), протоколирование случаев отказов или нестандартных рекомендаций, план действий при сбоях. Возможно, имеет смысл наделить Росздравнадзор или Минздрав полномочиями по утверждению отраслевых руководств по безопасному использованию искусственного интеллекта.

Также важно интегрировать интеллектуальные сервисы в общую систему защиты: если больница использует облачный интеллектуальный сервис, должен быть заключен договор, обязывающий поставщика соблюдать требования защиты данных по российскому законодательству (территориальное хранение, сертификация криптосредств и т.д.).

В целом, обеспечение информационной безопасности медицинских информационных систем с интеллектуальными компонентами должно рассматриваться как часть обеспечения качества медицинской помощи. Как и клинические риски, киберриски могут напрямую влиять на здоровье пациентов, поэтому их минимизация – зона ответственности как разработчиков программ, так и медицинских организаций и регуляторов.

Литература:

1. Постановление Кабинета Министров Республики Татарстан от 19.04.2022 г. № 369 «Об использовании технологий искусственного интеллекта в Республике Татарстан». URL: https://pravo.tatarstan.ru/npa_kabmin/post/?npa_id=977556
2. Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» (ред. от 08.08.2024) // СЗ РФ. 2006. № 31 (1 ч.). Ст. 3451.
3. Кошечкин К.А., Хохлов А.Л. Этические проблемы внедрения искусственного интеллекта в здравоохранении // Медицинская этика. 2024. № 1. С. 12–19.
4. Асеева И.А. Проблема приватности в цифровую эпоху // Науковедческие исследования. 2020. № 20. С. 36–50.
5. Вигель Н.Л., Меттини Э. Этические и культурные вызовы внедрения искусственного интеллекта в медицинских практиках: мультикультуральный анализ // Medical Ethics. 2024. № 3. С. 11–15.
6. Федеральный закон от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» (ред. от 28.12.2024) (с изм. и доп., вступ. в силу с 01.03.2025) // СЗ РФ. 2011. № 48. Ст. 6724.
7. Федеральный закон от 24.04.2020 г. № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» // СЗ РФ. 2020. № 17. Ст. 2701.
8. Приказ Минэкономразвития России от 02.07.2021 г. № 407 «Об утверждении отдельных методик расчета показателей федерального проекта «Искусственный интеллект» национальной программы «Цифровая экономика Российской Федерации» (ред. от 28.12.2021) // СПС Гарант.
9. Всероссийский центр изучения общественного мнения (ВЦИОМ) представляет результаты всероссийского опроса о применении искусственного интеллекта в здравоохранении. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/progress-ili-ugroza-ili-ob-iskusstvennom-intellekte-v-medicine
10. Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (ред. от 14.05.2020) (зарегистрировано в Минюсте России 14.05.2013 г. № 28375) // Российская газета. 2013. № 107.
11. 2023 Нормативно-правовое регулирование искусственного интеллекта в здравоохранении / Regulatory considerations on artificial intelligence for health // Всемирная организация здравоохранения. URL: https://ai.gov.ru/knowledgebase/mezhdunarodnye-dokumenty-po-razvitiyu-ii/2023_normativno-pravovoe_regulirovanie_iskusstvennogo_intellekta_v_zdravoohranenii_regulatory_considerations_on_artificial_intelligence_for_health_vsemirnaya_organizaciya_zdravoohraneniya

Artificial Intelligence in Medicine: Cybersecurity Issues and Ethical Aspects

Volchenko A.V.
Belgorod Law Institute of Ministry of the Internal of the Russian Federation named after I.D. Putilin
Kogteva A.N.
Financial University under the Government of the Russian Federation (Moscow)
Timokhina G.V.
Belgorod State National Research University

The integration of artificial intelligence into medicine opens up wide opportunities, but at the same time creates fundamentally new risks for information security. Intelligent systems gain access to confidential patient data and participate in clinical decision-making; their vulnerability (for example, to attacks with distorted input data) can lead to the leakage of personal information or the issuance of erroneous medical recommendations. Meanwhile, there are no special requirements for the cybersecurity of medical systems with artificial intelligence at the federal level, and uniform ethical standards for their use in healthcare are not legally fixed. This determines the relevance of this study. Its purpose is to analyze the emerging cyber threats and ethical and legal gaps in the implementation of artificial intelligence in healthcare and to develop proposals for improving the regulatory framework and practical measures to ensure the safe and responsible use of artificial intelligence. In the course of the work, an analysis of existing regulations and standards was carried out, key problems were identified (lack of special rules of responsibility for artificial intelligence errors, the risk of malicious attacks on algorithms, lack of rules for transparency and patient information) and approaches to their elimination were proposed. The scientific and practical significance lies in the fact that the results obtained can serve as a basis for the development of new requirements and recommendations on cybersecurity and ethics of the use of artificial intelligence in medicine. The scientific novelty consists in a comprehensive consideration of the issues of information security of medical intelligent systems, taking into account technical, legal and ethical aspects, as well as in substantiating the need to integrate special protection measures and transparency into the existing regulatory and legal system of healthcare.

Keywords: artificial intelligence in medicine, cybersecurity, information security, ethical aspects, legal regulation, personal data protection, transparency of algorithms