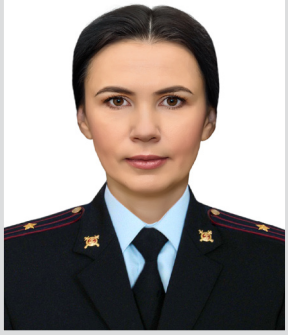
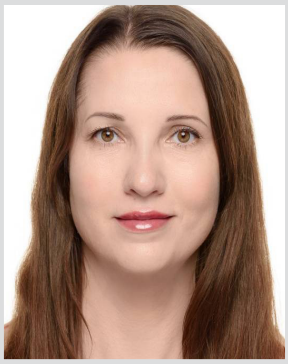
УДК 34.09
DOI: 10.24412/1998-5533-2025-3-409-413

Проблемные аспекты применения искусственного интеллекта в медицинской деятельности



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

Развитие технологий искусственного интеллекта в здравоохранении сопровождается новыми правовыми вызовами, связанными с безопасностью, ответственностью и защитой данных. Отсутствие целостной нормативной базы, фрагментарность регулирования и слабое урегулирование ответственности за ошибки интеллектуальных систем создают серьезные риски для пациентов и препятствуют эффективной интеграции искусственного интеллекта в клиническую практику. Целью работы является выявление проблемных аспектов правового регулирования применения искусственного интеллекта в медицинской деятельности и разработка предложений по их устранению. Практическая значимость исследования заключается в разработке конкретных рекомендаций по регулированию оборота медицинских интеллектуальных систем, распределению ответственности между участниками, защите медицинских данных и обеспечению информационной безопасности.

В ходе исследования обнаружены значительные пробелы в регулировании защиты персональных медицинских данных при обучении и эксплуатации интеллектуальных систем. Сделан вывод о необходимости разработки комплексного законодательного акта или включения специальных норм в действующие законы о здравоохранении и персональных данных, создания стандартов качества и безопасности для медицинских интеллектуальных систем. Исследование формирует основу для дальнейшей законодательной работы в данной области, ориентированной на баланс между развитием инноваций и защитой прав пациентов.

Ключевые слова: *искусственный интеллект, здравоохранение, медицинская деятельность. правовое регулирование, информационная безопасность, персональные данные*

Для цитирования: *Волченко А.В., Когтева А.Н., Тимохина Г.В. Проблемные аспекты применения искусственного интеллекта в медицинской деятельности // Вестник экономики, права и социологии. 2025. № 3. С. 409–413. DOI: 10.24412/1998-5533-2025-3-409-413.*

На сегодняшний день правовое регулирование использования искусственного интеллекта в медицине сталкивается с несколькими существенными вызовами.

Во-первых, отсутствует целостная нормативная правовая база, что порождает неопределенность статуса подобных технологий и фрагментарность регулирования, когда используются лишь общие нормы, не учитывающие специфику самообучающихся алгоритмов.

Во-вторых, не урегулирована ответственность за результаты работы искусственного интеллекта: в случае диагностической ошибки или сбоя алгоритма отсутствуют правовые нормы распределения риска между разработчиком программного обеспечения и медицинским работником. Такая неопределенность создает ситуацию, когда ни один из участников не несет явной ответственности за причиненный пациенту вред, что чревато юридическими коллизиями и феноменом «безликой» (размытой) ответственности.

В-третьих, существуют пробелы в регулировании использования больших массивов медицинских данных. Действующее законодательство о персональных данных настолько строго регулирует обращение сведений о здоровье (требуя явного согласия пациента либо полной деперсонизации информации), что без специального механизма практически невозможно легально применять большие обезличенные базы данных для обучения медицинских интеллектуальных моделей. Это, с одной стороны, тормозит разработку и повышение точности алгоритмов, а с другой – попытки обхода указанных ограничений несут риск нарушения права на приватность.

Далее соответствующие проблемные аспекты будут рассмотрены более детально.

Отсутствие специального закона и дефиниций

В законодательстве РФ на текущем этапе нет легального определения понятий «искусственный интеллект» и «медицинская интеллектуальная система». Кроме того, отсутствует специальный закон, посвященный регулированию искусственного интеллекта в целом. Это приводит к размытости правового статуса подобных систем и неопределенности применимого режима.

Фактически применение искусственного интеллекта регулируется общими нормами (о медизделиях, о защите информации, об оказании медпомощи), которые не учитывают всей специфики самообучения алгоритмов и автономности решений.

Указанное подчеркивает актуальность разработки отдельного нормативного акта, регламентирующего обращение искусственного интеллекта в медицине, либо включения соответствующего раздела в Федеральный закон от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» [1].

Неурегулированность ответственности и правового статуса участников

Законом не решен значимый вопрос о том, кто должен отвечать в случае ошибки или сбоя интеллектуальной системы, повлекшей вред пациенту. В стандартных условиях ответственность за диагностические и лечебные решения несет врач или медицинская организация. Использование алгоритма искусственного интеллекта размывает причинно-следственную связь: ошибка может быть вызвана некорректной работой программы.

С одной стороны, врач не должен полностью полагаться на подсказки искусственного интеллекта и обязан критически оценивать их, с другой – разработчики и поставщики интеллектуального продукта должны нести долю ответственности за качество алгоритма.

В действующем законодательстве отсутствуют нормы о распределении ответственности между медицинским работником (исполнителем услуги) и разработчиком (производителем) интеллектуальной системы. Это создает «зону неопределенности», которая может приводить к юридическим коллизиям. Существует риск так называемой «безликой ответственности», когда ни один субъект не признается прямо виновным.

Более того, как отмечает А.А. Шутова, существующий правовой механизм может вызывать у медицинских организаций опасения применять искусственный интеллект из-за страха привлечения к административной, а у сотрудников – к уголовной ответственности [2, с. 96]. Подобная ситуация тормозит внедрение инноваций.

Таким образом, требуется нормативно закрепить распределение рисков: либо через введение презумпции ответственности разработчика при доказанном дефекте алгоритма, либо через специальные условия освобождения врача от ответственности при добросовестном использовании сертифицированной интеллектуальной системы. Пока этого не

сделано, правоприменение будет опираться на общие нормы, которые могут оказаться неадаптированными к новым реалиям (например, предъявление претензий врачу за неверный диагноз, где реальную ошибку допустил алгоритм).

Недостатки механизмов контроля качества и безопасности искусственного интеллекта

Действующие процедуры оценки медицинских изделий (включая программные) во многом разрабатывались для традиционных, статичных по своим свойствам изделий. Алгоритмы машинного обучения могут изменяться со временем (при дополнительном обучении с учетом новых данных) и вести себя непредсказуемо вне заложенных сценариев.

Законодательство пока не содержит специальных требований к алгоритмической прозрачности, валидации данных и мониторингу эффективности интеллектуальных систем после их внедрения.

Первым прецедентом стала ситуация в 2023 г.: Росздравнадзор приостановил применение одного из уже зарегистрированных интеллектуальных сервисов для диагностики (системы *Botkin.AI*) из-за неоднократных сбоев и отсутствия заявленного клинического эффекта [3]. Это показало необходимость пострегистрационного надзора за работой интеллектуальных алгоритмов в реальных условиях.

Тем не менее, пока такой надзор носит реактивный характер, в связи с чем нужны проактивные механизмы:

– обязательная периодическая переоценка интеллектуальных систем, особенно самообучающихся, на предмет безопасности;

– требования по раскрытию разработчиком методик и данных обучения (в разумных пределах, без ущерба для коммерческой тайны);

– независимое тестирование на эталонных наборах данных.

Отсутствие требований к валидации данных и контролю качества алгоритмов на уровне регламента чревато проникновением на рынок потенциально неэффективных либо опасных решений. Разработанные стандарты (ГОСТы) пока носят добровольный характер.

Таким образом, существует пробел между быстрым техническим прогрессом и возможностями регулятора обеспечить должный контроль.

Проблемы конфиденциальности и правового режима медицинских данных

Для обучения моделей искусственного интеллекта требуются большие объемы данных о пациентах, часто представляющие персональные данные специальной категории (состояние здоровья). Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» [4] строго регулирует обращение таких сведений: как правило, нужно явное согласие субъекта либо данные должны быть обезличены до степени, исключающей идентификацию.

Пилотный проект 2020 г. в Москве показал возможность использования обезличенных данных без согласия субъекта [5], однако этот подход носит ограниченный характер эксперимента. В общероссийском масштабе до сих пор нет отдельной нормы, допускающей использование больших массивов медицинских данных в научно-исследовательских или аналитических целях без индивидуального согласия – даже если данные деперсонифицированы. Это существенно затрудняет разработку и улучшение медицинских интеллектуальных систем, поскольку получение согласия от миллионов пациентов практически невыполнимо.

С другой стороны, чрезмерное ослабление режима конфиденциальности чревато злоупотреблениями и нарушением прав на приватность. Найти баланс между доступностью данных для инноваций и защитой персональных данных – серьезный вызов.

Пока в законодательстве отсутствует механизм «управляемого доступа» к большим медицинским данным: например, через доверенные хранилища (*data trust*) или через специальные разрешительные процедуры. Кроме того, права пациентов на информацию об использовании их обезличенных данных не оформлены должным образом.

Исходя из указанного, правовая неопределенность приводит либо к риску нарушить закон при обучении искусственного интеллекта, либо к затруднениям в получении необходимых данных. Требуется внесение изменений в законодательство о персональных данных, чтобы легитимировать использование больших обезличенных медицинских данных в интересах развития искусственного интеллекта при условии соблюдения строгих мер защиты.

Информационная безопасность и защита данных при использовании искусственного интеллекта в медицине

Вопросы информационной безопасности занимают центральное место при правовом регулировании интеллектуальных систем, обрабатывающих медицинские данные. Медицинская информация традиционно отнесена к числу особо чувствительных: закон накладывает строгие требования на ее хранение, передачу и использование. С внедрением искусственного интеллекта происходит усложнение ландшафта угроз – помимо классических рисков несанкционированного доступа или утечки, добавляются специфические риски, связанные с работой алгоритмов. Необходимо разграничить два аспекта: защиту персональных данных пациентов и кибербезопасность самих интеллектуальных систем.

Защита персональных данных в контексте разрешения проблемы применения искусственного интеллекта в медицинской деятельности

Любая система искусственного интеллекта в медицине обучается и функционирует на основе ме-

дицинских данных, которые могут содержать персональную информацию о состоянии здоровья, диагнозах, результатах обследований и т.п. Положениями ФЗ № 152-ФЗ «О персональных данных» такие сведения отнесены к специальной категории персональных данных, обрабатываемых лишь с согласия субъекта или на основании отдельного закона. Как отмечено выше, экспериментальным путем был опробован подход с обезличиванием данных и их использованием без согласия (в Москве). Этот опыт показал, что при надлежащей деперсонификации можно обеспечить баланс интересов: с одной стороны, обезличенные данные уже не позволяют идентифицировать личность, с другой – сохраняют научную ценность для обучения моделей. Однако пока нет постоянных правил, распространяющих такой подход на всю страну.

Представляется необходимым на уровне федерального закона закрепить режим, при котором обезличенные в установленном порядке медицинские данные могут использоваться в научно-исследовательских и статистических целях (в том числе для разработки искусственного интеллекта) без получения индивидуального согласия пациентов.

Обязательным условием должно быть соответствие методике обезличивания, сертифицированной уполномоченным органом (в РФ такой методикой фактически является алгоритм, утвержденный приказом Минздрава № 341н [6]). Кроме того, целесообразно ввести для разработчиков обязанность использовать данные только в заявленных целях. Положительным примером является рекомендация Минздрава России, изложенная в письме № 18-6/И/2-471 от 16.01.2024 г.: использование медицинских данных, предоставляемых для работы интеллектуального сервиса, не допускается для иных целей, кроме как для функционирования самого медизделия, его дополнительного обучения или настройки.

Иными словами, данные пациентов, переданные интеллектуальной системе, не могут произвольно накапливаться разработчиком или третьими лицами и применяться вне контекста оказания медицинской помощи. Включение подобных норм в обязательные требования (например, в лицензии на софт или договоры) повысит уровень защиты конфиденциальности.

Также возможна реализация принципа минимизации данных: интеллектуальной системе должны передаваться только те сведения о пациенте, которые необходимы для выполнения конкретной задачи (диагноз, анализ снимка и т.п.), без избыточной информации. Для контроля за соблюдением этого принципа регулятору следует выработать методические указания.

С точки зрения пациентов важно обеспечить право на информированность: человек должен знать, что его (пусть даже обезличенные) данные могут использоваться в обучении алгоритмов, и иметь гарантии, что эти данные надежно защищены. Законодательство об охране здоровья пока не предусматривает обязанности медицинских организаций информировать пациентов о применении искусственного интеллекта, но в перспективе введение такой нормы выглядит оправданным – это повысит доверие и прозрачность.

В заключении следует отметить, что правовое регулирование в сфере защиты данных и инфобезопасности при внедрении искусственного интеллекта в медицине находится в стадии становления. Существующие нормы о персональных данных и о безопасности информационных систем должны быть уточнены применительно к интеллектуальным системам. Задача государства – создать условия, при которых инновации на основе искусственного интеллекта могут развиваться без ущерба для прав граждан на неприкосновенность частной жизни и при гарантированной надежности технологических решений.

Для успешной и эффективной интеграции искусственного интеллекта в медицину необходимо продолжить совершенствование законодательства.

Литература:

1. 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.
2. Шутова А.А. Применение технологий искусственного интеллекта в сфере здравоохранения: уголовно-правовые девиации // Правопорядок: история, теория, практика. 2023. №3 (38). С. 92–100.
3. Росздравнадзор приостановил использование системы с ИИ в клиниках. URL: https://www.vedomosti.ru/technology/news/2023/11/21/1006805-kommersant-roszdravnadzor
4. Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» (ред. от 08.08.2024) // СЗ РФ. 2006. № 31 (ч. 1). Ст. 3451.

5. 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.
6. Приказ Минздрава России от 14.06.2018 г. № 341н №Об утверждении Порядка обезличивания сведений о лицах, которым оказывается медицинская помощь, а также о лицах, в отношении которых проводятся медицинские экспертизы, медицинские осмотры и медицинские освидетельствования» (Зарегистрировано в Минюсте России 08.08.2018 г. №51822) // СПС КонсультантПлюс.

Problematic Aspects of the Use of Artificial Intelligence in Medical Practice

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

The development of artificial intelligence technologies in healthcare is accompanied by the emergence of new legal challenges related to security, responsibility, data protection and compliance with ethical standards. The lack of a coherent regulatory framework, fragmented regulation, and weak regulation of liability for errors in intelligent systems pose risks to patients and hinder the effective integration of artificial intelligence into clinical practice. The aim of the work is to identify problematic aspects of the legal regulation of the use of artificial intelligence in medical practice and to develop proposals for their elimination. The practical significance lies in the development of specific recommendations for regulating the turnover of medical intelligent systems, distributing the responsibility of participants, protecting medical data and ensuring information security. Significant gaps have been found in the regulation of the protection of personal medical data in the training and operation of intelligent systems. It is concluded that it is necessary to create a comprehensive legislative act or include special norms in existing laws on healthcare and personal data, develop quality and safety standards for medical intelligent systems. The study forms the basis for further legislative work in this area, focused on a balance between the development of innovation and the protection of patients' rights.

Keywords: artificial intelligence, healthcare, medical activity, legal regulation, information security, personal data