

Дата поступления рукописи в редакцию: 20.04.2026 г.

DOI: 10.24412/2076-1503-2026-5-100-104

Дата принятия рукописи в печать: 27.05.2026 г.

КУННУЕВА Умузахи Магомедовна,
обучающаяся первого курса,
очной формы обучения, лечебного факультета,
ФГБОУ ВО «Дагестанский государственный медицинский университет»
Министерства здравоохранения Российской Федерации,
e-mail: uma.kunnuyeva@mail.ru

ХИЗРИЕВА Мадина Мусаевна,
обучающаяся первого курса,
очной формы обучения, лечебного факультета,
ФГБОУ ВО «Дагестанский государственный медицинский университет»
Министерства здравоохранения Российской Федерации,
e-mail: madina.khizrieva13@gmail.com

Научный руководитель:
ГАДЖИМАГОМЕДОВА Шумайсат Солеймановна,
Старший преподаватель кафедры «Философия и гуманитарные дисциплины»
ФГБОУ ВО «Дагестанский государственный медицинский университет»,
г. Махачкала, Россия,
e-mail: mail@law-books.ru

Соруководители:
ХАЛИКОВ Абдулхалик Султансаидович,
Кандидат философских наук,
доцент кафедры «Философия и гуманитарные дисциплины»
ФГБОУ ВО «Дагестанский государственный медицинский университет»,
г. Махачкала, Россия,
e-mail: mail@law-books.ru

ПАШАЕВА Аида Магомедхановна,
врач-кардиолог,
e-mail: mail@law-books.ru

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ВРАЧЕБНАЯ ТАЙНА: КАК В ИНТЕРНЕТЕ НАРУШАЕТСЯ КОНФИДЕНЦИАЛЬНОСТЬ ПАЦИЕНТОВ

Аннотация. Интенсивное развитие нейронных сетей повлекло за собой глобальные трансформации всех сфер жизни, в том числе медицины и права. И специалисты-медработники, и пациенты убеждены в многообещающем потенциале искусственного интеллекта: применение нейросетей в научных исследованиях и телемедицинских консультациях было признано чрезвычайно эффективным. Однако материалы для обучения ИИ, как и механизмы его функционирования, вызывают множество споров в обществе. Ставится под вопрос этичность использования конфиденциальной информации для получения знаний нейросетью, а зафиксированные случаи утечек данных поспособствовали эксплуатации уязвимостей интернет-систем злоумышленниками. Цель: выявление «слабых мест» в области ИИ-права, анализ нынешней Конституции РФ и законов о нейронных сетях, выдвижение способов повышения безопасности использования и обучения ИИ. Материалы и методы: системный анализ открытых литературных источников и исследований, сведений из авторитетных медиа-изданий, последующий синтез полученной информации. Результаты: формулирование методов повышения безопасности при использовании ИИ в здравоохранении. Заключение: составленные в ходе изучения темы рекомендации могут стать

ценным материалом для последующих правовых изменений относительно применения нейронных сетей и их обучения.

Ключевые слова: искусственный интеллект, интернет медицинских вещей, врачебная тайна, защита данных, частная жизнь, биоэтика, право.

KUNNUEVA Umuzahi Magomedovna,

first-year student,
full-time student, Faculty of General Medicine,
Dagestan State Medical University
Ministry of Health of the Russian Federation

KHIZRIEVA Madina Musayevna,

first-year student,
full-time student, Faculty of General Medicine,
Dagestan State Medical University
Ministry of Health of the Russian Federation

Academic Supervisor:

GADZHIMAGOMEDOVA Shumaysat Soleymanovna,
Senior Lecturer, Department of Philosophy and Humanities,
Dagestan State Medical University,
Makhachkala, Russia

Co-supervisors:

KHALIKOV Abdulkhalik Sultansaidovich,
PhD in Philosophy,
Associate Professor, Department of Philosophy and Humanities,
Dagestan State Medical University Dagestan State Medical University,
Makhachkala, Russia

PASHAEVA Aida Magomedkhanovna,
cardiologist

ARTIFICIAL INTELLIGENCE AND MEDICAL CONFIDENTIALITY: HOW PATIENT PRIVACY IS VIOLATED ON THE INTERNET

Annotation. The rapid development of neural networks has led to global transformations in all spheres of life, including medicine and law. Both healthcare professionals and patients are convinced of the promising potential of artificial intelligence: the use of neural networks in scientific research and telemedicine consultations has been recognized as extremely effective. However, the materials used to train AI, as well as its operating mechanisms, are the subject of considerable controversy. The ethics of using confidential information for machine learning process are being questioned and documented cases of data leaks have facilitated the exploitation of vulnerabilities in internet systems by attackers. Objective: identifying weaknesses in AI law, analyzing the current Constitution of the Russian Federation and laws on neural networks, proposing solutions for improving the security of using and training AI. Materials and Methods: A systematic analysis of open literature and research as well as information from reputable media outlets, followed by a synthesis of the obtained information. Results: The development of methods for improving the security of using AI in healthcare. Conclusion: The recommendations drawn up during the study of this topic may become valuable material for subsequent legal changes regarding the use of neural networks and their training.

Key words: artificial intelligence, internet of medical things, medical confidentiality, data protection, privacy, bioethics, law.

Искусственный интеллект (далее ИИ) по праву можно признать самой выдающейся инновацией первых двух десяти-

тилетий 21 века. Современные нейронные сети, не являясь искусственным сознанием в истинном смысле данного слова, представляют собой язы-

ковые модели, обученные понимать и распознавать смыслы слов, а также генерировать текст самостоятельно, основываясь на изученных материалах. На сегодняшний день ИИ активно применяется во всех возможных отраслях жизни и прогрессирует с огромной скоростью, формируя все более логичные и сложные по своей структуре рассуждения.

Тем не менее, у ИИ, как относительно новой разработки, существует множество уязвимостей. Его внедрение создает риски утечек информации и неправомерного использования деятельности нейросети, а также неспособность государства призвать к ответственности людей, создающих контент, противоречащий Конституции УК РФ. Являясь полезным инструментом для медработников, ИИ способен создать угрозу раскрытия сведений, составляющих врачебную тайну отдельных пациентов, что весьма опасно для социума в связи с нарушением врачебной этики, без которой медицинская практика невозможна на законодательном уровне. [1]

Целью данной статьи явилось изучение правовых нюансов взаимодействия с нейронными сетями в данный момент, в рамках действующего на территории Москвы 123-ФЗ, и теоретизирование о будущем искусственного интеллекта в России после вступления в силу законопроекта «Об основах государственного регулирования применения технологий искусственного интеллекта» в 2027 году и предложение возможных решений для создания безопасной информационной среды для врачей и пациентов. [2]

Наиболее важным аспектом данного вопроса является защита данных, недопущение их распространения вне медицинских систем и надежная охрана информационных здравоохранительных структур.

Для формулирования идей по правовому регулированию искусственного интеллекта в медицинской сфере следует ознакомиться с опытом других государств и обратить внимание на принятые там меры и законы.

В данный момент конституции многих стран мира претерпевают значительные изменения в связи с возникновением ИИ. Всемирная организация здравоохранения в 2021 году выпустила «Руководство по этике и управлению ИИ в здравоохранении», согласно которому законы о применении нейросетей обязаны придерживаться принципов защиты автономии человека, обеспечения благополучия и безопасности, прозрачности, ответственности и социального равенства. [3]

В США была разработана концепция «программного обеспечения в роли медицинского устройства» (SaMD). Суть этой концепции состоит в необходимости сертифицировать агентов искус-

ственного интеллекта аналогичным сертификации медицинского оборудования и услуг образом. [4]

В Европейском Союзе был представлен законопроект «Регламент об ИИ» (AI Act), ранжирующий системы нейронных сетей по уровню опасности: чем он выше, тем строже должен вестись мониторинг действий искусственного интеллекта, тем прозрачнее должно быть его устройство. [5]

В России правовое регулирование ИИ в медицине только начинает развиваться. 18 марта 2026 года впервые был опубликован проект ФЗ «Об основах государственного регулирования применения технологий искусственного интеллекта». В нем устанавливаются следующие требования к разработке и машинному обучению:

- Обязательная маркировка ИИ-контента (фотографий, текста, видео) при публикации в интернете;
- Каждый участник взаимоотношения с искусственным интеллектом в случае генерации нарушающих закон материалов понесет наказание соразмерное своей вине в создании контента;
- Разработчикам дозволено использовать защищенные авторским правом объекты без разрешения от непосредственного правообладателя в случае, если разработчик обладает законным доступом к объекту. [6]

Безусловно, законопроект еще будет доработан и откорректирован, поскольку в текущей версии не учитываются многие детали. К примеру, защита прав пациентов, ставшая причиной написания данной статьи, совершенно не освещена, несмотря на масштабные инциденты кражи приватной жизненно-важной информации: киберпреступникам, получившим доступ к исходному коду нейросети, открываются огромные базы данных, собранных со всей мировой сети и включающих в себя секретную документацию вместе с персональной информацией госпиталей, поликлиник и прочих медицинских учреждений. [7] Данные собираются даже из трекеров самочувствия, приложений для диабетиков и перехватываются с серверов радио- и видеонянь. ИИ облегчает планирование фишинг-схем, подбор паролей и поиск «уязвимостей нулевого дня» (т.е. ненадежные фрагменты программы, обнаруженные злоумышленниками сразу после релиза приложения; более того, ограничения и правила нейросетей можно обойти с помощью специальных «промптов» (указаний), в которые хакер может вложить инструкции правонарушения или добиться изъятия необходимой ему информации. [8] Всем этим атакам в первую очередь подвергается Интернет медицинских вещей. Самые часто атакуемые

устройства – это инфузионные насосы, аппараты КТ и МРТ, устройства для мониторинга состояния пациента и медицинские рабочие станции.

Среди последствий кибератак – задержки в проведении анализов и процедур, о чем сообщили 56% организаций, увеличение числа осложнений после процедур (53%), продолжительности пребывания пациентов (52%), числа переводов пациентов (44%) и даже более высокие показатели смертности (28%). [9]

Каким же образом можно обезопасить сферу здравоохранения и нивелировать негативные последствия использования ИИ?

В ходе изучения норм нейросетевого права разных стран, обзоров исследований кибер-инцидентов и нынешних стратегий цифрового развития РФ нами были выдвинуты следующие предложения:

- Создание отечественных агентов искусственного интеллекта специально для медицинских организаций, надежно защищенные и существующие в замкнутой интернет-сети здания соответствующих организаций;
- Разработка доктрины «Разделенная солидарная ответственность», предлагающая разделение субъектов медицинской помощи на медицинского оператора (клинику) и инфраструктурно-алгоритмического оператора (разработчика ИИ и провайдера телемедицины), закрепив их солидарную ответственность за раскрытие врачебной тайны вследствие утечки данных;
- Отслеживание согласия, т.е. замена статичного бумажного ИДС на цифровую контрактную форму, заполняемую в приложении Госуслуги и позволяющую пациенту отслеживать, какая именно нейросеть в данный момент обучается на его снимках или данных, и отзываться это согласие в один клик;
- Поправки к статье 13 ФЗ-323 «Врачебная тайна». Необходимо дополнить часть 3 указанной статьи положением, согласно которому «передача сведений, составляющих врачебную тайну, провайдерам информационно-телекоммуникационных платформ и системам искусственного интеллекта для их обучения, допускается исключительно в изолированных сетях без права выгрузки данных во внешнюю интернет-среду»;
- Изменения в ФЗ-152 «О персональных данных». Ввести запрет на использование телемедицинских данных, полученных с использованием средств ИИ, в рекламных и страховых целях без создания отдельного, специального цифрового согласия через Госуслуги;

- Введение института сертификации ИИ (наподобие SaMD в США). Обязать разработчиков медицинского ИИ проходить сертификацию ФСТЭК России не только на предмет защиты каналов связи, но и на устойчивость ИИ к вышеупомянутым методам обхода ограничений.

Правовое регулирование ИИ в медицине находится в стадии становления, что требует гибкого, но надежного механизма защиты прав участников процесса. Сложная природа технологий диктует необходимость комплексного подхода: жесткие требования к безопасности должны гармонично дополняться нормами биоэтики — этическими кодексами и профессиональными стандартами врачей. Оптимальная модель регулирования призвана стимулировать технологический рост и доступность здравоохранения, одновременно минимизируя потенциальные риски. Формирование такой среды возможно лишь в рамках междисциплинарного диалога между юристами, медиками, разработчиками нейросетей и общественностью, что обеспечит ответственное внедрение инноваций для повышения качества жизни граждан [10].

Список литературы:

- [1] Наумов В.Б., Незнамов А.В., Смирнова К.М. Этико-правовые принципы применения технологий искусственного интеллекта в медицине: международные стандарты и российская перспектива // Вестник Московского университета. Серия 11: Право. 2023. № 2. С. 63-76.
- [2] Федеральный закон «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» от 24.04.2020 N 123-ФЗ (последняя редакция) // СПС КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_351127/ (дата обращения: 04.03.2026).
- [3] World Health Organization. Ethics and governance of artificial intelligence for health: WHO guidance. Geneva: WHO, 2021. 165 p.
- [4] U.S. Food and Drug Administration. Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD). FDA, 2019. 20 p.
- [5] European Commission. Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). COM(2021) 206 final, 2021.

[6] Проект Федерального закона «Об основах государственного регулирования сфер применения технологий искусственного интеллекта в Российской Федерации» // СПС КонсультантПлюс. URL: <https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=PRJ&n=271763&dst=#wYeO6IVsl1QujFJL> (дата обращения: 04.03.2026).

[7] Петрова Н.Г., Савельев А.И. Ответственность за причинение вреда системами искусственного интеллекта в здравоохранении: проблемы и перспективы регулирования // Медицинское право: теория и практика. 2023. Т. 9. № 1. С.45-57.

[8] Лебедев В.А., Иванова А.П. Правовые аспекты защиты персональных данных при использовании систем искусственного интеллекта в медицине // Информационное право. 2022. № 4. С. 32-41.

[9] Атаки на IoT: киберпреступники угрожают пациентам и предприятиям // Infowatch URL: <https://www.infowatch.ru/company/presscenter/news/ataki-na-iot-kiberprestupniki-ugrozhayut-patsiyentam-i-predpriyatiyam> (дата обращения: 04.03.2026).

[10] Карцхия А. А. Искусственный интеллект как средство управления в условиях глобальных рисков // Мониторинг правоприменения. — 2020. — № 1 (34). — С. 45-50.

[11] Морозов С.П., Владимирский А.В., Андрейченко А.Е. Нормативно-правовое регулирование использования искусственного интеллекта в здравоохранении: ключевые аспекты и тенденции // Медицинское право. 2022. № 3. С. 14-22.

[12] Шкарин В.В., Берсенева Е.А., Кураева В.М., Савостина Е.А. Искусственный интеллект в здравоохранении: возможности и проблемы внедрения // Вестник Росздравнадзора. 2021. № 3. С. 31-38.

References:

[1] Naumov V.B., Neznamov A.V., Smirnova K.M. Ethical and legal principles of the application of artificial intelligence technologies in medicine: international standards and Russian perspective // Bulletin of Moscow University. Series 11: Law. 2023. No. 2. P. 63-76.

[2] Federal Law "On Conducting an Experiment to Establish Special Regulation in Order to Create the Necessary Conditions for the Development and Implementation of Artificial Intelligence Technologies in the Subject of the Russian Federation - the City of

Federal Significance Moscow and Amending Articles 6 and 10 of the Federal Law "On Personal Data" dated April 24, 2020 N 123-FZ (latest revision) // SPS ConsultantPlus. URL: https://www.consultant.ru/document/cons_doc_LAW_351127/ (date accessed: March 4, 2026).

[3] World Health Organization. Ethics and governance of artificial intelligence for health: WHO guidance. Geneva: WHO, 2021. 165 p.

[4] U.S. Food and Drug Administration. Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD). FDA, 2019. 20 p.

[5] European Commission. Proposal for a Regulation laying down harmonized rules on artificial intelligence (Artificial Intelligence Act). COM(2021) 206 final, 2021.

[6] Draft Federal Law "On the Fundamentals of State Regulation of the Application of Artificial Intelligence Technologies in the Russian Federation" // SPS ConsultantPlus. URL: <https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=PRJ&n=271763&dst=#wYeO6IVsl1QujFJL> (accessed: 04.03.2026).

[7] Petrova N.G., Savelyev A.I. Liability for harm caused by artificial intelligence systems in healthcare: problems and prospects of regulation // Medical Law: Theory and Practice. 2023. Vol. 9. No. 1. P. 45-57.

[8] Lebedev V.A., Ivanova A.P. Legal aspects of personal data protection when using artificial intelligence systems in medicine // Information law. 2022. No. 4. P. 32-41.

[9] Attacks on the IoT: cybercriminals threaten patients and enterprises // Infowatch URL: <https://www.infowatch.ru/company/presscenter/news/ataki-na-iot-kiberprestupniki-ugrozhayut-patsiyentam-i-predpriyatiyam> (date of access: 04.03.2026).

[10] Kartshiya A.A. Artificial intelligence as a management tool in the context of global risks // Monitoring of law enforcement. - 2020. - No. 1 (34). - P. 45-50.

[11] Morozov S.P., Vladimirsky A.V., Andreychenko A.E. Normative-legal regulation of the use of artificial intelligence in healthcare: key aspects and trends // Medical law. 2022. No. 3. pp. 14-22.

[12] Shkarin V.V., Berseneva E.A., Kuraeva V.M., Savostina E.A. Artificial intelligence in healthcare: opportunities and challenges of implementation // Bulletin of Roszdravnadzor. 2021. No. 3. pp. 31-38.

