

УДК 614.253:34.03:004.056(575.2)
DOI: 10.36979/1694-500X-2026-26-7-42-47

ЭТИЧЕСКИЙ И ПРАВОВОЙ АСПЕКТ МЕДИЦИНЫ В БУДУЩЕМ

У.Ы. Аскаров, П.Т. Жолуева

Аннотация. Медицина развивается в условиях ускоренной цифровизации и биотехнологической революции, что меняет не только клинические протоколы, но и архитектуру ответственности, прав пациентов и охраны персональных данных. Расширение применения искусственного интеллекта (ИИ) в диагностике и принятии решений, развитие геномной инженерии (CRISPR/Cas), внедрение телемедицинских платформ, электронных медицинских карт и биобанков делают этическую повестку центральной для здравоохранения. Цель статьи – системно проанализировать ключевые этические дилеммы и правовые риски медицины будущего и предложить ориентиры регулирования, релевантные для Кыргызской Республики. Методологически работа опирается на сравнительно-правовой анализ международных и национальных актов (включая подходы ВОЗ к этике ИИ, нормы защиты медицинских данных, правила риск-ориентированного регулирования в ЕС и практики отдельных государств), а также на анализ типовых кейсов (ошибки алгоритмов, киберинциденты, генетическое вмешательство, трансграничные телемедицинские услуги). Показано, что устойчивое развитие инноваций возможно только при сочетании: прозрачных правил ответственности, принципов справедливости и недискриминации, процедур информированного согласия, управления данными, человеческого надзора и независимой оценки безопасности. Предложены меры по укреплению нормативной базы и институциональных механизмов этического контроля, включая стандарты качества данных, обязательную оценку рисков ИИ, требования к кибербезопасности и обновление клинико-этических протоколов.

Ключевые слова: медицина будущего; биоэтика; медицинское право; искусственный интеллект; геномная инженерия; телемедицина; электронная медицинская карта; кибербезопасность; конфиденциальность данных; эвтаназия.

КЕЛЕЧЕКТЕГИ МЕДИЦИНАНЫН ЭТИКАЛЫК ЖАНА УКУКТУК АСПЕКТТЕРИ

У.Ы. Аскаров, П.Т. Жолуева

Аннотация. Медицина ылдам санариптешүү жана биотехнологиялык революция шартында өнүгүп жатат, бул өзгөрүүлөр клиникалык протоколдорго гана эмес, жоопкерчиликтин түзүмүнө, бейтаптардын укуктарына жана жеке маалыматтарды коргоо системасына да таасир этүүдө. Диагностикада жана клиникалык чечим кабыл алууда жасалма интеллектти (ЖИ) кеңири колдонуу, гендик инженериянын (CRISPR/Cas) өнүгүшү, телемедицина платформаларынын, электрондук медициналык карталардын жана биобанктардын киргизилиши этикалык жана укуктук маселелерди саламаттык сактоо тармагындагы негизги багыттардын бирине айландырууда. Макаланын максаты – келечектеги медицинанын негизги этикалык дилеммаларын жана укуктук тобокелдиктерин системалуу талдоо жана Кыргыз Республикасы үчүн актуалдуу жөнгө салуу багыттарын сунуштоо болуп саналат. Методологиялык жактан изилдөө эл аралык жана улуттук нормативдик актыларды салыштырма-укуктук талдоого (анын ичинде ДСУнун ЖИ этикасы боюнча ыкмалары, медициналык маалыматтарды коргоо стандарттары, Европа Бирлигиндеги тобокелдикке негизделген жөнгө салуу модели жана айрым мамлекеттердин практикалары) таянат, ошондой эле типтүү учурларды (алгоритмдик каталар, киберинциденттер, генетикалык кийлигишүү, чек аралык телемедициналык кызматтар) талдоону камтыйт. Изилдөөнүн жыйынтыктары медициналык инновациялардын туруктуу өнүгүшү төмөнкү шарттардын айкалышы аркылуу гана мүмкүн экендигин көрсөтөт: жоопкерчиликтин ачык-айкын эрежелери, адилеттүүлүк жана дискриминацияга жол бербөө принциптери, маалымдалган макулдук жол-жоболору, маалыматтарды натыйжалуу башкаруу, адамдык көзөмөл жана коопсуздукту көз карандысыз баалоо. Макалада нормативдик базаны жана этикалык көзөмөлдүн институционалдык механизмдерин бекемдөөгө багытталган чаралар сунушталат, анын ичинде маалымат сапатынын стандарттары, жасалма интеллект үчүн милдеттүү тобокелдик баалоо, киберкоопсуздук талаптары жана клиникалык-этикалык протоколдорду жаңыртуу.

Түйүндүү сөздөр: келечектеги медицина; биоэтика; медициналык укук; жасалма интеллект; гендик инженерия; телемедицина; электрондук медициналык карта; киберкоопсуздук; жеке маалыматтарды корго; эвтаназия.

THE ETHICAL AND LEGAL DIMENSION OF MEDICINE IN THE FUTURE

U.Y. Askarov, P.T. Jolueva

Abstract. Medicine is evolving in the context of accelerated digitalization and a biotechnological revolution, transforming not only clinical protocols but also the architecture of liability, patient rights, and personal data protection. The expanding use of artificial intelligence (AI) in diagnostics and clinical decision-making, the advancement of genetic engineering (CRISPR/Cas), and the implementation of telemedicine platforms, electronic health records, and biobanks place ethical and legal considerations at the core of contemporary healthcare governance. The purpose of this article is to provide a systematic analysis of the key ethical dilemmas and legal risks of future medicine and to propose regulatory orientations relevant to the Kyrgyz Republic. Methodologically, the study relies on a comparative legal analysis of international and national regulatory frameworks (including the WHO approaches to AI ethics, standards for medical data protection, EU risk-based regulatory models, and selected national practices), as well as on the examination of typical case scenarios (algorithmic errors, cybersecurity incidents, genetic interventions, and cross-border telemedicine services). The findings demonstrate that the sustainable development of medical innovation is achievable only through a combination of transparent liability rules, principles of fairness and non-discrimination, robust informed consent procedures, effective data governance, human oversight, and independent safety assessment. The article proposes measures aimed at strengthening the regulatory framework and institutional mechanisms of ethical control, including data quality standards, mandatory AI risk assessment, cybersecurity requirements, and the modernization of clinical-ethical protocols.

Keywords: future medicine; bioethics; medical law; artificial intelligence; genetic engineering; telemedicine; electronic health records; cybersecurity; data privacy; euthanasia.

Введение. В конце XX – начале XXI века медицина вошла в фазу перехода от индустриальной модели здравоохранения к данно-ориентированной (или data-driven) и персонализированной модели. Драйверами стали машинное обучение, биотехнологии, телекоммуникации и экосистемы цифрового здравоохранения. Одновременно инновации повышают сложность нормативных решений: ответственность распределяется между разработчиками алгоритмов, поставщиками платформ, медицинскими организациями, врачами и государственными регуляторами.

Традиционные механизмы медицинского права (лицензирование, сертификация лекарств и медицинских изделий) сталкиваются с динамикой самообновляющихся систем и трансграничностью цифровых услуг. Поэтому этические и правовые рамки должны развиваться синхронно с технологиями, иначе возрастает риск утраты доверия и появления новых форм вреда – от систематической дискриминации до утечек генетической информации.

Цель исследования – определить ключевые узлы этико-правовых рисков медицины будущего и предложить рамочную модель регулирования, которая сочетает поддержку инноваций и защиту фундаментальных прав пациентов.

Материалы и методы исследования. Работа выполнена на основе междисциплинарного

подхода (биоэтика, сравнительное медицинское право, управление рисками). **Методы:** сравнительно-правовой анализ международных и национальных актов; анализ руководств международных организаций; кейс-метод; нормативно-догматический анализ информированного согласия, конфиденциальности, ответственности и надзора.

Использованы: руководства ВОЗ по этике и управлению ИИ в здравоохранении [1–2]; нормы ЕС о высокорисковых ИИ-системах в медицине [3–4]; правила защиты специальных категорий данных (GDPR, ст. 9) [5]; национальные режимы защиты данных (Кыргызская Республика [6], Россия [7], Китай [8], Турция [9], США [10]); документы по управлению рисками ИИ (NIST AI RMF 1.0) [11]; документы в области прав человека и биомедицины (Овьедская конвенция [12]) и глобальные этические стандарты (ЮНЕСКО [13]); немецкие рекомендации по защите медицинских данных и национальное право (BDSG) [14–15]; материалы ВОЗ о телемедицине [16] и материалы о стандартизации телемедицины в Кыргызстане [17].

Актуальность: почему этико-правовая проблематика усиливается. Для медицины будущего характерен одновременный рост возможностей и рисков. Искусственный интеллект (ИИ) способен повышать точность диагностики и ускорять разработку лекарств, геномика

и клеточные технологии обещают лечение ранее неизлечимых болезней, телемедицина расширяет доступ к помощи. Но цена ошибки возрастает: решения принимаются на основе сложных моделей и больших массивов данных.

Актуальность усиливается из-за асимметрии знаний (пациенту трудно понять роль алгоритма), асимметрии власти (данные концентрируются у платформ), и асимметрии ответственности (в цепочке поставки цифровых решений). Эти факторы делают необходимыми прозрачные процедуры информирования, надзор и аудит.

Для Кыргызской Республики проблема значима в связи с развитием цифрового здравоохранения и внедрением государственных медицинских информационных систем, включая цифровую медицинскую карту пациента и экосистему электронного здравоохранения [18–19]. Одновременно действуют Закон «Об информации персонального характера» [6] и отраслевой закон об охране здоровья граждан [20], что требует согласования норм и практик.

Результаты и обсуждение.

1. Искусственный интеллект и алгоритмическая медицина: ответственность, безопасность, справедливость

Практика преподавания медицинского права и правоповедения в высшем медицинском учебном заведении позволяет выявить дополнительные этические и правовые риски, связанные с широким и некритическим использованием искусственного интеллекта. В процессе учебной работы автор статьи неоднократно сталкивался с ситуациями, при которых студенты активно применяют системы искусственного интеллекта для подготовки письменных работ, рефератов и даже научных текстов без осознания правовых последствий таких действий.

Наиболее распространённой проблемой является некорректное заимствование сгенерированных текстов без указания источников, авторства и без соблюдения принципов академической добросовестности. Студенты, зачастую, не рассматривают результаты работы искусственного интеллекта как объект, подпадающий под нормы авторского права и этики цитирования, что формирует искажённое представление о допустимых границах использования

цифровых технологий в научной и профессиональной деятельности.

Данная ситуация демонстрирует, что проблема искусственного интеллекта в медицине и праве не ограничивается клинической практикой, но затрагивает также сферу медицинского образования. Отсутствие чётких институциональных правил и разъяснений относительно допустимого использования ИИ в образовательном процессе повышает риск формирования у будущих медицинских специалистов правового нигилизма и пренебрежительного отношения к вопросам интеллектуальной собственности и ответственности.

В этой связи представляется необходимым включение в образовательные программы медицинских вузов специализированных модулей, посвящённых правовым и этическим аспектам использования искусственного интеллекта, включая вопросы авторского права, академической честности и профессиональной ответственности. Такой подход позволит формировать у студентов не только цифровые навыки, но и правовую культуру, соответствующую требованиям медицины будущего.

ИИ в здравоохранении применяется для анализа изображений, прогнозирования рисков, триажа, поддержки клинических решений, управления потоками пациентов. Основной правовой вопрос – распределение ответственности при негативном исходе: врач, организация, разработчик или поставщик платформы. Международные подходы описывают ИИ как социотехническую систему: риски обусловлены не только моделью, но и контекстом внедрения [11].

Риск-ориентированная модель ЕС выделяет медицинские ИИ-системы как высокорисковые и связывает их допуск с управлением рисками, качеством данных, документацией, прозрачностью и человеческим надзором [3–4]. Это соответствует принципам ВОЗ: предотвращение вреда, инклюзивность, ответственность и ориентированность на общественное благо [1].

Проблема алгоритмической предвзятости требует обязательной проверки данных и качества модели на разных подгруппах пациентов, иначе возникает цифровое неравенство. Остельную осторожность требуют генеративные

модели и большие мультимодальные модели, способные выдавать убедительные, но ложные ответы; ВОЗ подчеркивает необходимость клинической верификации, строгого надзора и управления инцидентами [2].

Минимальный набор правовых условий безопасного внедрения медицинского ИИ включает: определение статуса продукта, правила ответственности, специальные требования к информированному согласию (включая информирование о роли алгоритма), мониторинг и регистрацию инцидентов, независимый аудит.

2. Геномика, CRISPR (Clustered Regularly Interspaced Short Palindromic Repeats – кластерные регулярно расположенные короткие палиндромные повторы) и персонализированная медицина: границы допустимого и риск дискриминации. Геномика и редактирование генов позволяют выявлять наследственные риски и корректировать отдельные мутации, но повышают этическую цену вмешательства, особенно при потенциальном влиянии на будущие поколения. Международная биомедицинская этика исходит из приоритета достоинства личности над интересами науки; в этом смысле Овьедская конвенция рассматривается как ключевой юридический ориентир для защиты прав человека в биомедицине [12].

Риски включают информированное согласие при неопределенности долгосрочных последствий, справедливость доступа, генетическую дискриминацию и размывание границы между лечением и «улучшением» (enhancement). Правовой ответ предполагает усиленную защиту генетических данных; в ЕС это коррелирует с режимом специальных категорий данных по Общему регламенту по защите данных (GDPR – General Data Protection Regulation) [5].

3. Цифровое здравоохранение и данные: конфиденциальность, кибербезопасность, доверие. Цифровое здравоохранение основано на данных: электронные медицинские карты, лабораторные и эпидемиологические платформы, телемониторинг. Это повышает непрерывность помощи, но усиливает риск утечек и кибератак. Поэтому кибербезопасность становится частью безопасности пациента, а не только ИТ-функцией.

Сравнение правовых режимов показывает, что медицинская информация трактуется как чувствительная и требует специальных гарантий: HIPAA в США защищает PHI [10]; GDPR в ЕС устанавливает режим специальной защиты данных о здоровье и генетических данных [5]; PIPL в Китае регулирует обработку и трансграничную передачу чувствительной информации [8]; KVKK в Турции закрепляет охрану частной жизни при обработке данных [9].

В немецкой практике вопросы защиты медицинских данных детализируются через национальные разъяснения и нормативные акты, дополняющие GDPR: в частности, федеральные рекомендации по защите медицинских данных обращают внимание на необходимость соблюдения Article 9 GDPR и национальных «открывающих» норм [14], а также на роль BDSG как дополнительного уровня регулирования [15].

Для Кыргызской Республики ключевым является согласование норм о цифровом здравоохранении с Законом «О персональной информации» [6] и отраслевыми актами об охране здоровья [20], включая развитие государственной цифровой медицинской карты пациента и связанных систем [18–19]. Практически важно унифицировать режимы доступа и логирования, установить стандарты киберзащиты и реагирования на инциденты, закрепить процедурные права пациента (доступ, исправление ошибок, уведомление об утечках).

4. Телемедицина и трансграничные услуги: качество, юрисдикция, этика коммуникации. Телемедицина преодолевает географические барьеры и особенно важна для сельских и труднодоступных регионов. ВОЗ отмечает, что телемедицина повышает доступность и качество услуг при наличии соответствующей политики и инфраструктуры [16]. В Кыргызстане телемедицина рассматривается как практический инструмент повышения доступности специализированной помощи и требует стандартизации услуг [17]. Правовые сложности при трансграничных консультациях включают определение применимой юрисдикции, правил хранения данных, механизма ответственности, идентификации пациента и врача, а также допустимости дистанционной диагностики. Эти вопросы

требуют гармонизации норм и развития профессиональных стандартов.

Этически важно сохранять качество коммуникации и не допускать «обезличивания» помощи: пациент должен понимать ограничения дистанционного формата, иметь право на очную консультацию при необходимости и на защиту конфиденциальности в цифровых каналах.

5. Роботизированная хирургия, наномедицина, нейротехнологии: новые зоны биоэтики. Роботизированная хирургия расширяет границы возможного, но усложняет ответственность и требования к компетенциям. Наномедицина и регенеративная терапия требуют усиленного пострегистрационного надзора из-за долгосрочных эффектов.

Нейротехнологии поднимают вопросы ментальной приватности и согласия на обработку нейроданных. Международная дискуссия об этических стандартах нейротехнологий показывает необходимость заблаговременного регулирования даже для технологий, которые пока ограниченно доступны в клинике.

Предложения по развитию регулирования и практик для Кыргызской Республики. На основе анализа международных подходов и национальной нормативной базы целесообразно сформировать пакет мер, ориентированный на «ответственное внедрение» технологий:

1) *Регуляторная классификация медицинского ИИ и цифровых продуктов:* определение, какие решения относятся к ПО медицинского назначения; какие подлежат обязательной оценке безопасности; какие допустимы как вспомогательные инструменты.

2) *Модель ответственности:* закрепление принципа распределенной ответственности с четкими зонами – разработчик (качество и документация), интегратор (безопасность внедрения), медорганизация (условия эксплуатации), врач (профессиональное решение и надзор).

3) *Данные и конфиденциальность:* уточнение статуса медицинских и генетических данных как особо чувствительных; введение стандартов доступа, логирования, уведомления об инцидентах и минимизации данных; согласование с Законом «О персональной информации» [6].

4) *Независимая оценка и аудит:* укрепление этических комитетов, внедрение оценок рисков и справедливости (fairness) для ИИ; использование принципов ВОЗ и ЮНЕСКО как ориентиров [1, 13].

5) *Подготовка кадров:* модули по медицинскому праву, этике данных и клиническому применению ИИ; протоколы переподготовки для новых ролей.

Выводы:

1. Медицина будущего усиливает требования к ответственности, справедливости и защите данных в условиях ИИ и геномики.

2. Международные стандарты и риск-ориентированное регулирование (ВОЗ, ЮНЕСКО, ЕС, NIST) формируют основу для управления жизненным циклом технологий [1–5, 11, 13].

3. В Кыргызской Республике необходима синхронизация законодательства о персональных данных и здравоохранении с цифровыми практиками [6, 18–20].

4. Устойчивое внедрение инноваций требует качества данных, информированного согласия, киберустойчивости и независимого аудита.

Поступила: 11.02.2026;

рецензирована: 25.02.2026; принята: 27.02.2026.

Литература

1. Ethics and governance of artificial intelligence for health. Geneva: WHO, 2021. URL: <https://www.who.int/publications/i/item/9789240029200> (дата обращения: 08.02.2026).
2. Ethics and governance of artificial intelligence for health: guidance on large multi-modal models. Geneva: WHO, 2025. URL: <https://www.who.int/publications/i/item/9789240084759> (дата обращения: 08.02.2026).
3. Artificial intelligence in healthcare (AI Act entered into force on 1 August 2024). URL: https://health.ec.europa.eu/ehealth-digital-health-and-care/artificial-intelligence-healthcare_en (дата обращения: 08.02.2026).
4. van Kolschooten H. The EU Artificial Intelligence Act (2024): Implications for healthcare // Hannah van Kolschooten, Janneke van Oirschot // Computer Law & Security Review. 2024. URL: <https://www.sciencedirect.com/science/article/pii/S0168851024001623> (дата обращения: 08.02.2026).

5. Regulation (EU) 2016/679 (GDPR). Article 9: Processing of special categories of personal data. URL: <https://gdpr-info.eu/art-9-gdpr/> (дата обращения: 12.02.2026).
6. Закон Кыргызской Республики от 14 апреля 2008 г. № 58, с изм. «Об информации персонального характера». URL: <https://cbd.minjust.gov.kg/202269/edition/1239270/ru> (дата обращения: 12.02.2026).
7. Федеральный закон «О персональных данных» от 27 июля 2006 года N 152-ФЗ (последняя редакция). URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 12.02.2026).
8. Personal Information Protection Law of the People's Republic of China (PIPL). Effective 1 November 2021. URL: https://en.spp.gov.cn/2021-12/29/c_948419.htm (дата обращения: 14.02.2026).
9. Republic of Türkiye. Personal Data Protection Law No. 6698 (KVKK). URL: <https://www.kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law> (дата обращения: 14.02.2026).
10. U.S. Department of Health & Human Services. Summary of the HIPAA Privacy Rule. Updated 2025. URL: <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html> (дата обращения: 14.02.2026).
11. NIST. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. 2023. URL: <chrome-extension://efaidnbmninnibpcapjpcglclefindmkaj/https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf> (дата обращения: 14.02.2026).
12. Council of Europe. Convention on Human Rights and Biomedicine (Oviedo Convention), 1997. URL: <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168007cf98> (дата обращения: 15.02.2026).
13. UNESCO. Recommendation on the Ethics of Artificial Intelligence. 2021. URL: <https://unesdoc.unesco.org/ark:/48223/pf0000380455> (дата обращения: 15.02.2026).
14. Federal Ministry for Economic Affairs and Climate Action (Germany). Orientierungshilfe zum Gesundheitsdatenschutz (PDF). URL: https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Downloads/M-O/orientierungshilfe-gesundheitsdatenschutz.pdf?__blob=publicationFile (дата обращения: 15.02.2026).
15. Bundesministerium der Justiz (Germany). Bundesdatenschutzgesetz (BDSG). URL: https://www.gesetze-im-internet.de/bdsg_2018/BJNR209710017.html (дата обращения: 20.02.2026).
16. WHO. Global Observatory for eHealth. Telemedicine: opportunities and developments in Member States: report on the second global survey on eHealth. 2010. URL: <https://iris.who.int/items/0365143e-27dc-418e-ad66-ae095df34fda> (дата обращения: 20.02.2026).
17. UNICEF Kyrgyzstan. Standardization of telemedicine services in Kyrgyzstan (PDF). URL: <https://www.unicef.org/kyrgyzstan/media/7381/file/Standardization%20of%20telemedicine%20services%20in%20Kyrgyzstan.pdf> (дата обращения: 20.02.2026).
18. Программа Правительства Кыргызской Республики по охране здоровья населения и развитию системы здравоохранения на 2019–2030 годы «Здоровый человек – процветающая страна». URL: <https://cbd.minjust.gov.kg/12976/edition/929710/ru> (дата обращения: 15.02.2026).
19. Положение о единой экосистеме цифрового здравоохранения Кыргызской Республики. URL: <https://cbd.minjust.gov.kg/7-34551/edition/20098/ru> (дата обращения: 15.02.2026).
20. Закон Кыргызской Республики от 12 января 2024 года № 14 «Об охране здоровья граждан в Кыргызской Республике» (в ред. Закона КР от 7 августа 2024 года № 163). URL: <https://cbd.minjust.gov.kg/4-5260/edition/1939/ru> (дата обращения: 15.02.2026).