УДК 34.09 DOI: 10.31249/iajpravo/2026.01.13

ГРОГОЛЬ А.Г.[1] ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В МЕДИЦИНЕ: ВОПРОСЫ ОБЕСПЕЧЕНИЯ ФУНКЦИОНИРОВАНИЯ НАДЕЖНОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И БЕЗОПАСНОСТИ МЕДИЦИНСКИХ ДАННЫХ В ЕВРОПЕЙСКОМ СОЮЗЕ (Обзор)

Аннотация. Использование искусственного интеллекта (ИИ) в сферах медицины и здравоохранения открывает как новые возможности, так и влечет новые риски, связанные с нарушением прав пациентов и созданием угрозы безопасности медицинских данных. В обзоре анализируется правовой опыт Европейского союза в сфере оказания медицинских услуг, защиты персональных данных пациентов, получение компетентного клинического решения, принятого ИИ-системой. Особое внимание акцентируется на правовых вопросах перехода на алгоритмические решения, принимаемые ИИ в сфере медицины, и необходимости пересмотра существующих механизмов обеспечения прав пациентов и их безопасности при использовании технологий искусственного интеллекта.

Ключевые слова: Европейский союз; правовое регулирование; Регламент ЕС о защите персональных данных; права пациентов; искусственный интеллект; медицинские данные; персональные данные; автоматизированные решения; право на «человеческий надзор».

GROGOL A.G. Legal regulation of the use of AI technologies in medicine: issues of ensuring the functional of reliable AI and security of medical data based on EU counties (Review)

[1] *Гроголь Анастасия Георгиевна*, младший научный сотрудник отдела правоведения ИНИОН РАН.

Abstract. The use of artificial intelligence (AI) in the fields of medicine and healthcare opens up both new opportunities and entails new risks related to the violation of patients' rights and the creation of threats to the security of medical data. The review analyzes the legal experience of the European Union in the field of providing medical services, protecting patients' personal data, and obtaining a competent clinical decision made by an AI system. Particular attention is paid to the legal issues of the transition to algorithmic decisions made by AI in the field of medicine, and the need to review existing mechanisms for ensuring patients' rights and safety when using artificial intelligence technologies.

Keywords: European Union; legal regulation; EU Regulation on Personal Data Protection; patients' rights; artificial intelligence; medical data; personal data; automated solutions; the right to «human supervision».

Для цитирования: Гроголь А.Г. Правовое регулирование использования технологий искусственного интеллекта в медицине: вопросы обеспечения функционирования надежного искусственного интеллекта и безопасности медицинских данных в Европейском союзе (Обзор) // Социальные и гуманитарные науки. Отечественная и зарубежная литература: ИАЖ. Сер. 4: Государство и право. – 2026. – № 1. – С. 199–212. – DOI: 10.31249/iajpravo/2026.01.13

Введение

Стремительное развитие технологий искусственного интеллекта (ИИ) претерпевает множество изменений и оказывает все большее влияние на основные сферы жизни общества, в том числе здравоохранение и медицину. Современные способы оказания медицинских услуг постепенно модернизируются, внедряя алгоритмы ИИ в диагностику, лечение и принятие клинических решений. Одновременно возрастает количество угроз, связанных с сохранением и обеспечением фундаментальных прав пациентов в условиях цифровизации медицины. Использование алгоритмических систем вполне может осложнять реализацию таких основополагающих прав, как осознанное и добровольное изъявление согласия граждан на выбор альтернативных путей диагностики и лечения. Кроме того, переход на автоматизированные клинические процессы ставит под угрозу автономность пациента, так как прозрачность принятия клинического решения ИИ не всегда поддается отслеживанию ввиду несовершенства механизмов правового и регулятивного

характера. В связи с этим возникает необходимость вводить новые гарантии защиты персональных медицинских данных (конфиденциальности информации о состоянии здоровья пациента).

В обзоре рассматриваются особые направления цифровой трансформации в различных сферах медицины и здравоохранения в условиях применения технологий ИИ в Европейском союзе: институт защиты персональных медицинских данных, дача информированного согласия на обработку данных ИИ-системами, право на отказ от участия в автоматизированных процессах, непосредственное участие пациента в принятии клинических решений, обеспечение доступа к цифровым медицинским данным и свобода выбора альтернативных способов лечения.

Правовое регулирование искусственного интеллекта в медицинской сфере в Европейском союзе

Общий регламент о защите персональных данных

Искусственный интеллект в медицине, по мнению Софии Палмиери, научного сотрудника Университета в Генте (Бельгия), является одной из наиболее обсуждаемых повесток в рамках правового поля ЕС; это подтверждает активное расширение нормативно-правовой базы и научных исследований. Основополагающим правовым актом признается Общий регламент ЕС по защите данных 2016 г.[1] (далее – Регламент, GDPR). Данный Регламент С. Палмиери характеризует как многоаспектный, комплексный документ, образующий правовую основу в виде правил сбора, обработки, хранения и распространения персональных данных, принципов, подлежащих применению независимо от контекста, в котором обрабатываются персональные данные. По мнению автора, GDPR вполне применим в регулировании медицинского ИИ в случаях, когда данные системы участвуют в обработке персональных данных [3, p. 1–6].

На изучении положений GDPR также сосредоточивают свое внимание Леандро Пеккья, профессор-ассистент в области биомедицинской инженерии Уоринского университета (Великобритания), и Алессия Маккаро, доктор в области биоэтики, научный со-

[1] The Regulation on the Protection of Natural Persons with Regard to the Processing of Personal Data. – URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng (дата обращения: 15.10.2025).

трудник этого же Университета, и другие исследователи. Среди наиболее важных положений Регламента авторы выделяют регулируемые этим актом права физических лиц в эпоху цифровых технологий, обязанности лиц, участвующих в обработке данных (сбор, хранение, анализ), способы и методы обеспечения соблюдения медицинскими работниками и пациентами законодательства, а также меры ответственности за нарушение установленных правовых норм. Ученые отмечают, что GDPR напрямую не регулирует применение медицинского ИИ, но содержит общие положения, указывающие на необходимость руководствоваться принципом справедливости в управлении данными при принятии доступного и понятного решения, принятого ИИ (ст. 22 GDPR) [1, p. 665–667].

Регламент о медицинском оборудовании

Анализируемый автором Регламент о медицинском оборудовании, принятый Европейским парламентом и Советом ЕС в 2017 г. (далее – MDR)[1], является специализированным правовым актом, регулирующим порядок реализации устройств медицинского назначения на территории ЕС, размещения таких товаров на рынке и процесс проведения медицинских исследований, учитывая отдельные вопросы применения ИИ в медицинском секторе. Данный правовой акт характеризует медицинский ИИ в качестве специализированного программного обеспечения, а также устанавливает строгие требования соблюдения безопасности и сохранения эффективности оказания медицинских услуг для медицинских учреждений, которые применяют технологии ИИ в своей деятельности; обеспечивает надежность данных, которые получаются в результате клинических исследований, сохраняя при этом безопасность участников исследовательских программ. MDR также предусматривает необходимость установления ответственного лица, удовлетворяющего минимальным квалификационным требованиям, которое выступает гарантом качества и безопасности медицинского оборудования на всех этапах его реализации – от производства до послепродажного контроля и мониторинга (ст. 34 Регламент о медицинском оборудовании).

[1] The Regulation on Medical Devices: сайт. – URL: https://eur-lex.europa.eu/eli/reg/2017/745/oj/eng (дата обращения: 11.08.25).

Регламент об установлении гармонизированных правил в области искусственного интеллекта

В своем исследовании С. Палмиери сосредоточивает особое внимание на Законе ЕС об установлении гармонизированных правил в области ИИ 2024 г.[1] (далее – Закон ЕС об ИИ). Этот Закон является ключевым в вопросах применения ИИ в различных сферах жизнедеятельности (кроме военной), в том числе в здравоохранении и медицине, состоит из 13 глав и содержит положения о безопасности и прозрачности медицинских ИИ-систем, запрещенных практиках использования ИИ-моделей, категорирование рисков, связанных с применением различных технологий ИИ, в том числе в медицинской сфере. По мнению С. Палмиери, только во взаимодействии всех трех актов – Регламент о защите персональных данных, Регламент о медицинском оборудовании и Закона ЕС об ИИ – можно говорить о создании в Евросоюзе сильной правовой основы регулирования применения ИИ в рассматриваемой области.

Риск-ориентированный подход применительно к медицинскому искусственному интеллекту

Один из вопросов, рассматриваемый С. Палмиери, – применение риск-ориентированного подхода при классификации ИИ. Такой подход позволяет расширить или ограничить применение технологий ИИ, воспринимать эти технологии как определенный продукт, категорировать его в зависимости от риска, снизить сомнения пользователей, связанные с развитием, функционированием и использованием ИИ путем соблюдения требований безопасности, установленных в Законе ЕС об ИИ [3, p. 3–8].

Исходя из положений Закона ЕС об ИИ, автор выделяет три класса риска:

- 1-й класс – неприемлемые риски (unacceptable risks), ставящие под угрозу фундаментальные основы безопасности, здоровья, благополучия и основные права человека. Виды и типы ИИ-систем, попадающие под данную категорию, подробным образом изложены в разделе II ст. 5 рассматриваемого Закона.

[1] Regulation Laying down Harmonized Rules on Artificial Intelligence (the EU Artificial Intelligence Act). – URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (дата обращения:19.10.2025).

• 2-й класс – высокая степень рисков (high risk considered). Для данной категории установлен институт двойного соотношения (double ratio). С одной стороны, данные системы и соответствующие продукты должны отвечать требованиям безопасности, которые в законе подробно не описаны; достаточно лишь указать, что конечная цель использования таких технологий – соблюдение безопасности. С другой стороны, ИИ-системы с высокой степенью риска помимо вышеуказанного требования должны предусматривать определенные меры предосторожности, которые уже регламентированы и перечислены в ст. 6.2 указанного Закона.

• 3-й класс – ограниченные и минимальные риски (limited and minimal risks) применяются для поддержания баланса между безопасностью и инновациями. Ограниченными, согласно рассматриваемого Закона, считаются ИИ-системы, генерирующие ложные сведения (deep fakes) через аудио- или видеоконтент, а минимальными рисками принято считать ИИ-системы вышеупомянутых категорий, которые не имеют повышенную степень опасности [4, p. 9].

Углубленный анализ Закона ЕС об ИИ, регулирующего вопросы проведения оценок рисков и уязвимостей ИИ-систем, постмаркетингового надзора, внедрения принципов обеспечения безопасности, а также создания надежных и прозрачных ИИ-систем предприняли также авторы статьи «Нормативная экосистема ЕС для этичного искусственного интеллекта» [2] – Вайос Болгурос, доктор в области кибербезопасности из Пирейского университета (Италия), Апостолис Заррас, профессор кафедры цифровых систем этого же университета, Кристиан Лека, профессор факультета науки Университета Лучиана Благи в Сибиу (Румыния). С их точки зрения, именно критерий прозрачности выполняет главную роль, так как обязывает ИИ-разработчиков детально прописывать системные ограничения и возможные риски, предоставлять их в общедоступном формате, чтобы пользователи могли самостоятельно прийти к решению о согласии применения технологий ИИ в личных медицинских целях. Однако, несмотря на широкую сферу действия Закона ЕС об ИИ, авторы сходятся во мнении, что данный правовой акт не уделяет существенного внимания функциональным требованиям к операционным особенностям ИИ-систем [2, p. 5067–5068].

Право пациента на информированное согласие и отказ в использовании медицинских и персональных данных при работе с технологиями искусственного интеллекта

В своем исследовании ученые из Туринского университета (Италия) – Маринелла Кваранта, профессор факультета компьютерных наук, Марко Гроссо, доктор наук в области общественного здравоохранения и Илария Анжела Амантеа, отмечая сложность в объяснении работы ИИ-систем пациентам, ставят под вопрос осознанность получения согласия на анализ медицинских данных с использованием ИИ-систем. По их мнению, в настоящее время большинство технологий ИИ не отвечают критерию прозрачности, доступности, понятности, так как алгоритмы вычисления и обработки информации многих ИИ-систем крайне трудно отследить и тем более объяснить лицам (пользователям), не владеющим специализированным набором знаний. Такая проблема ставит под угрозу индивидуальные и коллективные права пользователей, и если результаты ИИ-операций недоступны для понимания простым гражданам, то риск возникновения более сложных и серьезных юридических претензий будет возрастать. Именно поэтому в работе с медицинскими данными пациентов с применением ИИ-технологий обработки информации крайне важно предоставить пользователям понятную и доступную информацию о функционально-операционных деталях используемой ИИ-технологии, чтобы дать пациенту возможность самостоятельно принять решение об информированном согласии или отказе от ИИ-услуги. Авторы подчеркивают, что в современном правовом поле отсутствует прямо выраженное и закрепленное право на отказ от применения ИИ-технологии, в том числе в сфере медицины и здравоохранения. Именно поэтому необходима правовая конкретизация применения медицинского ИИ на уровне национального законодательства [4, p. 275–276].

На ограниченные условия участия пациента в выборе и отказе от применения технологиий ИИ также указывает С. Палмиери. Она считает, что институт раскрытия информации об использовании той или иной технологии особенно со все большим переходом на автоматизированные решения является преимуществом для пациентов, которым не была предоставлена возможность выбрать соответствующую ИИ-систему в обработке медицинских данных или принятии клинических решений, также как и отказаться от данной технологии. Содержание ст. 13–15 GDPR позволяет

С. Палмиери утверждать о существовании косвенного правового механизма, содержащего требование раскрытия информации о существовании автоматизированного процесса принятия решений. Несмотря на споры в научной литературе, автор убеждена, что применение института раскрытия информации в юридической практике оказало бы значительное влияние на регулирование медицинского ИИ без необходимости применения положений специального Закона ЕС об ИИ [3, p. 4–9].

Право на «человеческий надзор» (right to human oversight) при принятии решений на основе ИИ-систем

В ходе изучения требований безопасности по использованию и эксплуатации ИИ-систем В. Болгурос, А. Заррас и К. Лека обратили внимание на многоуровневый, комплексный подход в их регулировании. По мнению ученых, рассматриваемые ИИ-платформы могут быть эффективными лишь в некоторых областях. При коллективном применении таких платформ, как правило, создается полноценная целостная система безопасности, учитывающая технические, этические и ориентированные на пользователя нюансы. Так, устранение выявленных пробелов в данной цепочке через повышение их функциональной совместимости, систематическое внедрение принципов «человеческого надзора» и справедливости способствуют этическому и безопасному процессу применения медицинских систем на основе технологий ИИ. По мнению авторов, такой комплексный механизм обеспечит защиту медицинских пользователей, повысит доверие и впоследствии станет новой стратегией-ориентиром для других стран [2, p. 5069–5070].

Внедрение механизма «человеческого надзора» за развитием технологий ИИ в медицинском секторе имеет, по мнению названных авторов, множество преимуществ, так как сохраняется приоритетная роль человеческого суждения в программах с применением ИИ, особенно в ситуациях, связанных с принятием наиболее важных медицинских решений (постановка диагноза, обработка медицинских анализов, выбор способа лечения и т.д.). Такой инструмент позволяет снизить риск как ошибочного автоматизированного решения, так и человеческого фактора (врачебной ошибки) [2, p. 5067–5068].

Тема сохранения ключевой роли человека в автоматизированном процессе в медицинской деятельности рассматривается в статье «Европейская ответственность за качеством продукции для

систем поддержки клинических решений на основе искусственного интеллекта» [5] Яна Штальдуинена, исследователя вопросов медицинской ответственности в сфере применения технологий ИИ в Институте частного права Лейденского университета (Нидерланды). Автор полагает, что врач является своего рода «переводчиком» автоматизированных медицинских решений ИИ, и именно поэтому он должен нести юридическую ответственность независимо от объема применения ИИ-технологии в данном решении. Такая позиция позволяет ему сделать вывод о высокой доли человеческого фактора в эпоху автоматизированных решений.

Я. Штальдуинен подробно анализирует концепцию внедрения систем поддержки принятия клинических решений (Clinic Decision Support System) (далее – CDSS), разработанную Робертом Хейвордом, сотрудником Центра доказательной медицины при Оксфордском университете и являющуюся передовым достижением в области машинного обучения. В таких системах программируются правила и механизмы вывода наиболее точных решений для клинической диагностики на основе ранее встроенных кейсов, опыта и т.п. Это позволяет более гибко решать проблему возможной врачебной ошибки. По мнению автора, вспомогательная роль алгоритмов и технологий ИИ делает CDSS наиболее подходящей автоматизированной системой в медицинской сфере. В то же время нельзя отрицать недостаток критерия прозрачности в CDSS-системах на базе ИИ. В случаях сбоя или какой-либо непредвиденной ошибки в виде некорректной рекомендации о клиническом решении, препарата, ошибка ИИ-системы может отразиться на ответственности доктора. В отношении CDSS указанные риски являются наиболее серьезными, так как реализуются через посредника (медицинского работника) и могут охватывать более широкий спектр негативного воздействия в системе здравоохранения. На данном основании Я. Штальдуинен предлагает учитывать такие ошибки, как халатность медицинского работника, который, получив сомнительный результат или рекомендацию CDSS, не принял во внимание и не учел негативные последствия такого клинического решения. Однако для этой новой формы ответственности, возникающей на основании некорректного функционирования CDSS, по мнению автора, необходимо принять специализированный правовой акт. На данный момент реальность такова, что клиницисты далеко не всегда несут полную юридическую ответственность за используемые ими технологии и алгоритмические устройства [5, p. 15–18].

По мере того, как CDSS находит все большее распространение на европейском пространстве, стандарты халатности в правовом регулировании будут также расширяться. Несмотря на первоначальную выгоду в использовании CDSS, Я. Штальдуинен приходит к выводу о том, что внедрение данных систем на основе ИИ может лишить потенциально пострадавшую сторону (пациента) средств правовой защиты [5, p. 15–18].

М. Кваранта, Марко Гроссо и Илария Анжела Амантеа в дополнение позиции Я. Штальдуинена резюмируют, что автоматизация медицинских решений на базе ИИ неминуемо приведет к двум крайне опасным последствиям: потенциальной потере врачебного контроля и снижению качества персонализированного подхода. В связи с этим, подчеркивают исследователи, важно сохранять баланс между машинным и человеческим вмешательством в медицинские операции [4, p. 276–278].

Механизмы обеспечения конфиденциальности и защиты медицинских (персональных) данных в европейском законодательстве

Европейский союз и страны – члены ЕС в парадигме своего развития продвинулись далеко от «индустриальной экономики» (industrial economy) к «экономике знаний» (knowledge economy), что, по мнению Л. Пеккья и А. Маккаро, было вызвано процессами цифровизации и массовым распространением технологий ИИ. Данные в современных реалиях стали новой главной ценностью в медицине. Однако, чтобы необработанные данные (raw data) приобрели набор ценностных характеристик, необходимо создание определенных механизмов, дабы эти данные превратились в интеллектуальный капитал, инновации, информацию и стали стимулом разработки новых технологий. В связи с этим авторы справедливо утверждают, что в Общем регламенте (GDPR) недостаточно принципов, установленных для полноценного эффективного обеспечения защиты данных, особенно персонализированных данных, касающихся отдельных пользователей, в том числе и в медицинском секторе. Исходя из этих положений, Л. Пеккья и А. Маккаро приводят подробный анализ системы европейских данных о состоянии здоровья (European Health Data Space, EHDS). Пандемия COVID-19 позволила повысить осведомленность государств во взаимосвязи и взаимовлиянии между поддержанием устойчивых механизмов обмена медицинскими данными и конкурентоспособ-

ностью, о лидерстве в сфере медицинского сектора (проведения медицинских исследований, производства лекарственных препаратов и др.). В 2020 г. распространившаяся эпидемия с точки зрения прогрессивного роста послужила позитивным стимулом к активному внедрению цифровых технологий в рамках создания единой платформы-пространства медицинских данных (EHDS). Данная экосистема для управления медицинскими данными и их обмена оказала благоприятный эффект на качество результатов медицинского обслуживания, стимулирование медицинских исследований, способствовала выработке стандартизированного и безопасного подхода в обмене медицинскими данными среди государств – участников ЕС. Л. Пеккья и А. Маккаро уточняют, что основным элементом системы EHDS является различие между первичным использованием (primary use), заключающемся в непосредственном предоставлении клинической помощи (clinical care), и вторичным использованием (secondary use), в форме различных исследований, разработки политики и т.д. [1, p. 665–668].

В рамках первичного использования была специально создана добровольная платформа-инфраструктура «MyHealth@EU», которая функционирует на наднациональном уровне и представляет собой эффективный банк медицинских данных, позволяющий упростить доступ среди всех стран ЕС. Данная система также позволяет обеспечить требование GDPR о безопасном обмене информацией для целей первичного использования.

В рамках вторичного использования были установлены общие правила и стандарты в отношении порядка предоставления разрешений и гарантий для исследовательских и политических целей. По мнению авторов, такой дуальный подход раскрывает потенциал экономии данных (data economy protection) в медицинском секторе и сфере здравоохранения, преимущественно посредством разработки политики и нормотворческой деятельности, реализации политики, основанной на фактических данных [ibid.].

Таким образом, авторы сходятся во мнении и убеждены, что платформа EHDS является основным фундаментом в продвижении Европейской стратегии здравоохранения, принятой Еврокомиссией 30 ноября 2022 г. (The EU Global Health Strategy to improve global health security and delivery better health for all)[1], целью кото-

[1] The EU Global Health Strategy to Improve Global Health Security and Delivery Detter Health for All. – URL: https://ec.europa.eu/commission/presscorner/detail/en/ip22153 (дата обращения:19.08.2025).

рой является преодоление существующей фрагментации правовых норм и создание эффективной многоуровневой системы управления оборотом медицинских и персонализированных медицинских данных. Авторы подчеркивают, что стабилизация и стимуляция использования данной платформы увеличивают быстроту реагирования в случае форс-мажора или чрезвычайной ситуации, как это произошло в период пандемии COVID-19. Однако следует учитывать, что даже EHDS имеет ряд свойственных ограничений, в частности в отношении трансграничной защиты конфиденциальности данных в форме информации, функциональной совместимости и стандартизации данных (data interoperability and standardization). Например, ограничения могут возникнуть в различных системах и практиках лиц, предоставляющих медицинские услуги. Сложности заключаются в беспрепятственном обмене и использовании медицинских данных ввиду различий национального законодательства [1, p. 669].

Функциональные требования законодательства Европейского союза к эффективному обращению с медицинскими данными при использовании технологий искусственного интеллекта и иных алгоритмических технологий

Рассмотренные ранее регуляционные требования, а также нормы в отношении безопасности данных не могут в полной мере обеспечить оборот медицинских данных. С точки зрения греческих ученых – В. Болгуроса, А. Зарраса и К. Леки, занимающихся изучением вопросов этического использования технологий ИИ, такую дуальную систему регулирования следовало бы дополнить функциональными требованиями, так как значительные институциональные различия препятствуют нормальному использованию систем обработки медицинских данных на базе ИИ.

В. Болгурос и А. Заррас и К. Лека предлагают выявить и дополнить набор существующих функциональных требований к ИИ-системам, содержащих этические принципы и операционную надежность. Основополагающим критерием-требованием здесь может выступать оценка соответствия (conformity assessment requirement, CAR) этическим и функциональным параметрам. Согласно ст. 43–51 разд. 5 гл. III Закона ЕС об ИИ, поставщики технологий с использованием ИИ обязаны соблюдать CAR для систем ИИ с высоким уровнем риска и получить сертификат соответствия, выданный уполномоченным органом на срок не более пяти

лет. При несоответствии требованиям, установленным в разд. 2 Закона об ИИ, ранее полученный сертификат соответствия может быть приостановлен до устранения нарушений. Раздел 2 Закона об ИИ предусматривает, что ИИ-системы с высокой степенью риска должны проходить обязательную проверку на соответствие требованиям, установленным в технической документации, процедурам управлениям качества (quality management procedures), стратегиям послепродажного маркетинга (post-market monitoring strategies), при этом данная процедура проходит как на этапе внедрения ИИ-технологии, так и в рамках ее последующего эксплуатирования. Такой подход позволяет свести к минимуму потенциальные ошибки в функционировании ИИ-систем и моделей, что повышает эффективность предоставляемых медицинских услуг. Регламент GDPR дополняет положения Закона ЕС об ИИ и в ст. 32 содержит положения о безопасности и устойчивости ИИ, о необходимости интеграции таких механизмов на протяжении всего жизненного цикла ИИ-системы. По мнению авторов, симбиоз данных требований способствует выработке упреждающих мер против киберугроз, гарантирует надежность и эффективность ИИ-системы при принятии клинических решений [2, p. 5069–580].

Заключение

Представленный обзор показывает, что развитие и внедрение технологий ИИ в медицинской сфере позволяет открыть качественно новые подходы в диагностике заболеваний, принятии клинических решений, разграничении юридической ответственности за медицинские ошибки, сохранении конфиденциальности медицинских и персональных данных. Именно поэтому крайне важно, чтобы трансформация традиционной модели оказания медицинских услуг, основанная на ИИ-системах и алгоритмических технологиях, подлежала детальной правовой оценке, так как обеспечение баланса между инновациями и этическими нормами позволит грамотно и качественно внедрить такие достижения без потерь и угроз. Европейские регламенты – GDPR, MDR, Закон об ИИ – демонстрируют комплексный подход в регулировании ИИ-систем и медицинских данных, обеспечивая прозрачность, безопасность и соблюдение общепринятых норм. Ключевыми приоритетами развития правового регулирования в ЕС сегодня стали вопросы обеспечения информированного согласия пациента на применение ИИ-систем при предоставлении медицинских ус-

луг, института «человеческого надзора», защиты персональных медицинских данных и расширения требований к медицинским ИИ-системам.

Список литературы

1. Artificial Intelligence, Data Protection and Medical Device Regulations: Squaring the Circle with a Historical Perspective in Europe / L. Pecchia, A. Macarro, M.A.G. Marrese, F. Folkvord, G. Fico // Health and Technology. – 2024. – Vol. 14. – P. 663–670. – URL: https://link.springer.com/article/10.1007/s12553-024-00789-9 (дата обращения: 22.10.2025).
2. EU Regulatory Ecosystem for Ethical AI / V. Bolgouras, A. Zarra, C. Leka, I. Stylianou, A. Farao, C. Xenakis // AI and Ethics. – 2025. – Vol. 5. – P. 5063–5080. – URL: https://link.springer.com/article/10.1007/s43681-025-00370-6 (дата обращения: 22.10.2025).
3. Palmieri S. The Renewed EU Legal Framework for Medical AI // European Journal of Law and Technology. – 2024. – Vol. 15, N 3. – P. 1–23. – URL: https://ejlt.org/index.php/ejlt/article/view/957 (дата обращения: 24.10.2025).
4. Quaranta M., Amantea I.A., Grosso M. Obligation for AI Systems in Healthcare: Prepare for Trouble and Make it Double? // The Review of Socionetwork Strategies. – 2023. – Vol. 17. – P. 1–20. – URL: https://link.springer.com/article/10.1007/s12626-023-00145-z (дата обращения: 24.10.2025).
5. Staalduinen J.H. van (Jan) European Product Liability for AI Based Clinical Decision Support Systems // Digital Governance. – 2025. – Vol. 39. – P. 15–40. – URL: https://link.springer.com/chapter/10.1007/978-3-031-47834-2_8 (дата обращения: 24.10.2025).