УДК 342, 349 DOI: 10.31249/rgpravo/2026.09

СКУРКО Е.В.[1] ПРОБЛЕМЫ БЕЗОПАСНОСТИ В СФЕРЕ ЦИФРОВОГО ЗДРАВООХРАНЕНИЯ И ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В МЕДИЦИНЕ (Обзор)

Аннотация. В обзоре рассматриваются позиции и взгляды зарубежных ученых на вызовы цифровизации в системе здравоохранения, раскрываются особенности и проблемы обеспечения кибербезопасности, гарантии защиты персональных данных при использовании ИИ, оформлении информированного согласия на применение ИИ в процессе оказания медицинской помощи. Особое внимание уделяется вопросам обеспечения соблюдения государственных нормативов, стандартов и рекомендаций, а также внедрению и соблюдению протоколов кибербезопасности в информационных системах сферы медицины и здравоохранения.

Ключевые слова: цифровизация медицины; персональные данные; информированное согласие; конфиденциальность; медицинский ИИ.

SKURKO E.V. Security Issues in Digital Healthcare and the Use of Artificial Intelligence in Medicine (Review)

Abstract. The review examines the positions and views of foreign scientists on the challenges of digitalization in the healthcare system, reveals the features and problems of ensuring cybersecurity, guarantees the protection of personal data when using AI, and the process of obtaining informed consent for the use of AI in the provision of medical care. Special attention is paid to ensuring compliance with government regulations, standards, and recommendations, as well as implementing and adhering to cybersecurity protocols in medical and healthcare information systems.

[1] *Скурко Елена Вячеславовна*, старший научный сотрудник отдела правоведения ИНИОН РАН.

Keywords: digitalization of medicine; personal data; informed consent; confidentiality; medical AI.

Для цитирования: Скурко Е.В. Проблемы безопасности в сфере цифрового здравоохранения и применения искусственного интеллекта в медицине (Обзор) // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4: Государство и право. – 2026. – № 4. – С. 108–120. – DOI: 10.31249/rgpravo/2026.04.09

Введение

Современные технологии, цифровизация, системы искусственного интеллекта (ИИ) стремительно меняют формы и способы оказания медицинской помощи, развитие систем здравоохранения во всем мире. Цифровизация, автоматизация, интеграция ИИ в процессы управления медицинскими учреждениями, здравоохранение в целом позволяют сделать предоставление медицинских услуг более доступным и высококачественным.

Начиная с перевода медицинских записей с бумажных носителей в цифровые формы и их размещение в облачной среде цифровых систем и сетей, обработка данных в системе здравоохранения, в том числе средствами ИИ, в конечном счете призваны не только и не столько оптимизировать деятельность медицинского сообщества, но и, в отношении каждого пациента, через доступ к информации предложить врачам максимально полное представление об истории болезни человека, а следовательно, определить пути профилактики и лечения больных [3, p. 337].

Вместе с тем новые средства и подходы при цифровизации здравоохранения несут новые вызовы и ставят вопросы, требующие в том числе юридических решений, развития правового регулирования цифровизации здравоохранения.

Особенности и проблемы обеспечения информационной безопасности в системе здравоохранения

Цифровые информационные системы – в большей или меньшей степени – представлены и развиваются практически в любом современном медицинском учреждении, повсеместно в мире. Как указывает Сейед Амин Табиш из Института медицинских наук Шер-и-Кашмир (Индия), информационные системы медицинских учреждений (здравоохранения) следует рассматривать как системы, состоящие не только из технических компонентов, но и

«человеческого фактора» (персонала учреждения и пациентов). Информационные системы медицинских учреждений, кроме того, решают не только вопросы оптимизации лечения и ухода за пациентами, но и вопросы администрирования данного учреждения, финансов, оборудования, транспорта и т.п. Информационная система медицинского учреждения, подчеркивает автор, – это система управления данными о медицинском обслуживании, централизованная база данных, в которой накапливается, хранится и обрабатывается информация, относящаяся к пациентам учреждения здравоохранения и их здоровью. Получая доступ к этой базе данных, просматривая информацию о состоянии здоровья пациентов, врачи могут быстрее и точнее поставить диагноз, назначить лечение [3, p. 337].

Кроме того, такие информационные системы содержат информацию и обрабатывают данные, связанные с оперативным управлением медицинским учреждением, т.е. ориентированы на административно-хозяйственные потребности учреждений здравоохранения, обеспечивают поддержку принятия решений финансового и юридического характера [Ibid].

В качестве примеров, получивших наибольшее распространение цифровых решений в системе управления здравоохранением, С.М. Табиш указывает на базы данных электронных медицинских карт; электронную медицинскую документацию по диагностике, выданным врачебным предписаниям, назначениям, рецептам, отчетам о наблюдении; базы данных по оборудованию и распределению транспорта для оказания неотложной помощи и др. Комплексное управление обозначенными и иными функциями, на основании данных информационной системы медицинского учреждения, в существенной степени сегодня также осуществляться средствами специализированного программного обеспечения по работе с соответствующими базами данных и их информационном взаимодействии [3, p. 338].

В современном учреждении здравоохранения информационные системы применяются, начиная с процедуры онлайн-записи пациента на прием к врачу, заканчивая отчетами медсестер по своей смене для передачи этих данных заступающему на дежурство медицинскому персоналу. В случае оказания платных медицинских услуг информационные системы управляют платежными накладными и циклами выставления счетов за оказываемые услуги пациентам. В рамках этих информационных систем получают развитие функции поддержки принятия клинических решений леча-

щим врачом, средства дистанционного мониторинга пациентов и др. [3, p. 338]

Одним из ключевых вопросов в развитии цифровизации учреждений здравоохранения является то, что действующие информационные системы – источник данных по истории болезни пациента, а также его персональных данных, что признается как «чувствительная» информация, и данные такого рода должны обеспечиваться защитой и контролем за тем, кто, на каком основании и в каком объеме может получить к ним доступ [3, p. 350].

Как указывают Алисса Або из Стенфордского центра биодизайна им. Муссалема (США) и Шэннон Лантци из компании «Сильвер спринг» Мэриленд (США), угрозы утечек персональных данных, в том числе медицинских данных пациентов, кибератаки в сфере здравоохранения, как показывает опыт, не только распространены, но идут из различных источников, совершаются субъектами с различными мотивами, начиная от совершения преступных деяний с использованием программ-вымогателей до атак, приводящих к повреждению данных пациентов, что может иметь катастрофические последствия для их жизни и здоровья. Кроме того кибератаки и другие инциденты в информационных системах учреждений медицины и здравоохранения могут иметь последствием сбои и повреждения критически важной инфраструктуры здравоохранения, начиная от цифрового медицинского оборудования, например технических средств обработки изображений, как то в системах компьютерной и магнитно-резонансной томографии, до информационных сбоев в системах хранения и обработки данных, влекущих те или иные нарушения работы медицинских служб, вплоть до сбоев документооборота, расчета заработной платы сотрудников, оформления налоговых отчислений учреждения и др. [1, p. 166].

Соответствующим образом последствия угроз кибербезопасности для информационных систем учреждений медицины и здравоохранения разнообразны, включая сбои и общие нарушения в работе медицинских служб, угрозы жизни и здоровью пациентов, нарушение конфиденциальности медицинских данных и утечек персональных данных, а также увеличение рабочей нагрузки на сотрудников этих учреждений, оказывающихся в ситуации необходимости оказывать медицинскую помощь без цифровых инструментов. Комплексность информационных систем здравоохранения обусловливает дополнительные угрозы и вызовы безопасности данных, в них аккумулируемых, – например, когда

кибератаки предпринимаются через, казалось бы, «периферийные» точки, как то системы расчета заработной платы сотрудников либо оплаты счетов пациентами, имеющими результатом повреждения цифровой части клинической инфраструктуры медицинского учреждения, и т.п.

Как справедливо указывают А. Або и Ш. Лантци, в современных условиях каждый «участник» системы здравоохранения, от врачей и администраторов до непосредственно пациентов, играет важную роль в поддержании кибербезопасности. При этом проблемы информационной безопасности зачастую являются неявными или «скрытыми», и, следовательно, регулирование информационной безопасности медицинских учреждений, как правило, всегда остается недостаточным [1, p. 166].

Авторы приходят к выводу, что обеспечение кибербезопасности в системах здравоохранения является исключительно сложной задачей, особенно в условиях стремительной цифровизации сектора и критического характера предоставляемых услуг. Проблема кибербезопасности в здравоохранении должна решаться системно, на различных уровнях, для которых предусмотрены различные функции и обязанности лиц, обращающихся к информационной системе, – от директивных органов, предписывающих меры по повышению безопасности в масштабах всей отрасли здравоохранения, до повседневных действий медицинских работников и пациентов, передающих свои персональные данные [1, p. 167].

Вызовы информационной и кибербезопасности в здравоохранении, по мнению А. Або и Ш. Лантци, требуют комплексного и системного подхода, заключающего в том, что:

– на государственном уровне, наряду с секторами оборонной и торговой политики, кибербезопасность в сфере здравоохранения должна находиться ряду приоритетов. Это предполагает внедрение жестких стандартов на импорт медицинских изделий и цифрового медицинского оборудования, обеспечение их соответствия нормативным критериям кибербезопасности. Актуально развитие международного сотрудничества в сфере кибербезопасности в здравоохранении, разработка глобальных нормативно-правовых систем и стандартов, направленных на снижение трансграничной уязвимости в информационных системах в медицине и здравоохранении;

– на уровне регулирующих органов в сфере здравоохранения (министерств и ведомств) требуется разработка подзаконных актов, нормативов и стандартов, направленных на обеспечение госу-

дарственной политики и рекомендаций по кибербезопасности в отношении цифровых медицинских технологий. Требуется проводить комплексную оценку безопасности и кибербезопасности перед сертификацией либо внедрением новых цифровых устройств в медицинской практике, периодически пересматривать существующие стандарты и технологии. Важную роль играет надзор со стороны регулирующих органов – в целях гарантировать, что производители и поставщики медицинских услуг следуют «лучшим практикам» в сфере кибербезопасности;

– на уровне производителей цифровых технологий и оборудования для медицины и здравоохранения требуется, чтобы при производстве были обеспечены максимальные технические гарантии кибербезопасности. Производители должны учитывать особенности критической инфраструктуры и социальную роль сферы здравоохранения, в том числе сотрудничать с регулирующими органами и экспертами в сфере медицины и кибербезопасности;

– на уровне учреждений медицины и здравоохранения требуется соблюдение государственных нормативов, стандартов и рекомендаций профильных ведомств, а также внедрение строгих протоколов кибербезопасности в своих информационных системах. Это, в частности, подразумевает регулярную оценку уязвимостей информационных систем, своевременное обновление программного и аппаратного обеспечения, постоянный мониторинг функционирования информационных систем, отслеживание потенциальных нарушений. Важное значение имеет формирование «культуры кибербезопасности» и осведомленности об информационной безопасности всех сотрудников медицинских учреждений;

– на уровне практикующих врачей следует развивать культуру того, что врач – «главный страж» цифрового здравоохранения. Непосредственное взаимодействие врача с цифровыми технологиями в медицине, средствами ИИ, дает ему не только уникальные возможности исполнения своих профессиональных функций и обязанностей, но и позволяет в числе первых выявлять уязвимые места цифровых средств и оборудования, принимать превентивные меры в соответствующих случаях и ситуациях. Действительно, в то время как системные усилия крайне важны и необходимы, практикующие врачи – ключ развитию и обеспечению безопасности цифровых информационных систем в медицине и здравоохранении [1, p. 172–173].

Конфиденциальность и правовые проблемы использования технологий искусственного интеллекта в медицине и здравоохранении

Карен Хаберкосс из Медицинского университета Чикаго (США) в отношении информационно-правовых аспектов применения ИИ в медицине и здравоохранении обращает внимание на то, что эффективное применение средств ИИ в медицине и здравоохранении требует, чтобы ИИ получал доступ к медицинским данным, аккумулирующим информацию о прошлых и нынешних пациентах различных медицинских учреждений, иных потребителях медицинских услуг и услуг в сфере здравоохранения, а в некоторых случаях – биомедицинских исследованиях человека и др. Каждый из этих типов данных, а также цели их использования, права доступа и формы обработки могут регулироваться и контролироваться на основании различных законодательных и иных нормативных правовых актов, правительственных и ведомственных постановлений и руководств, директив, методологий, руководящих принципов, разработанных профессиональными структурами и организациями, а также внутренними нормативными актами каждого конкретного учреждения медицины и здравоохранения [2, p. 149].

Искусственный интеллект в медицине, как и в других областях, работает с «большими данными» для обеспечения качества результатов. Причем, это – технология, которая, как и все другие виды информационных систем и технологий в медицине и здравоохранении, требует обеспечения конфиденциальности, особенно со стороны практикующего врача. Очевидно при этом, что чем больше объем данных, которыми оперирует ИИ, тем больше вероятность нарушения конфиденциальности информации, в том числе по причинам некорректного управления, непреднамеренного использования, а в крайнем случае – злонамеренности, особенно в условиях отсутствия надлежащего надзора.

Так, пациенты и широкая общественность сегодня становятся все более обеспокоены проблемой конфиденциальности медицинских данных. Формируется общественный запрос, чтобы информация в сфере медицины и здравоохранения использовалась в строгом соответствии с законом, требуется большая прозрачность и контроль применения медицинских данных и персональных данных пациентов, ожидается, что граждане будут информироваться о том, как их информация – в сфере медицины и здравоохранения –

передается другим лицам, даже если они используются в медицинских целях медицинскими работниками, а также о технологиях, используемых для их передачи [2, p. 149].

Актуальной становится необходимость, чтобы медицинские учреждения и организации специально анализировали риски, связанные со сбором, использованием и передачей медицинских и иных данных своих информационных систем. Зачастую это сопрягается с получением согласия пациента, начиная с обработки его персональных данных, заканчивая применяемым способом лечения [2, p. 150].

Сферу здравоохранения и медицины и ее работу с информацией, как указывалось ранее, принято считать «чувствительной» по своей природе, поскольку эта информация имеет персональный, индивидуализированный характер [2, p. 154].

Конфиденциальность является важным принципом в медицине и здравоохранении. Так, почти каждый, обращающийся в систему здравоохранения, полагает, что его персональная информация, а также медицинские данные других людей могут быть отнесены к категории конфиденциальной, а профессиональные союзы, ассоциации и организации в сфере медицины и здравоохранения, как минимум на этическом уровне, признают, что соблюдение конфиденциальности – предварительное условие поддержания доверия в отношениях с пациентами. Действительно, люди, обращающиеся за медицинскими услугами, услугами здравоохранения либо участвующие в исследованиях в этих сферах, ожидают, что данные, которыми они делятся во время общения с сотрудниками данных учреждений или которые собираются в ходе исследований, будут охраняться, в том числе с точки зрения конфиденциальности. В отношении отдельных видов медицинских данных может быть нормативно установлена категория особой конфиденциальности, что требует соответствующих режимов обращения, а в результате их нарушения может повлечь дополнительные юридические последствия для поставщиков медицинских услуг, в том числе за использование или разглашение данных за рамками отношений, связанных с лечением. Этот тип информации и допустимые формы работы с ней могут получать особенное законодательное регулирование [2, p. 154].

К категории особо охраняемых медицинских данных, в том числе в случае их использования в работе систем ИИ, как правило на законодательном уровне, относятся такие, как: психическое здоровье и отклонения в развитии, генетика, репродуктивное здо-

ровье и медицина, инфекционные заболевания и заболевания, передающиеся половым путем, а также данные медицинского освидетельствования по фактам насилия, жестокого обращения и насилия в семье и др. Такая информация в случае ненадлежащей охраны несет риски для затронутых лиц, нарушение конфиденциальности их персональных данных – в том числе и в особенности в случаях их использования в системах ИИ, а также при обучении ИИ-моделей. Помимо морального вреда, разглашение особо охраняемой конфиденциальной медицинской информации может иметь последствием причинение вреда жизни и здоровью человека, нести ряд других негативных последствий [2, p. 154].

В информационно-техническом и правовом аспекте особо охраняемые и «высококонфиденциальные» типы данных – в электронных медицинских картах, системах медицинского страхования, базах данных страховых выплат, исследовательских базах данных, которые содержат медицинскую информацию, и т.п. – маркируются как «закрытые», порой «обезличиваются». Формы раскрытия и использования таких данных для целей обработки ИИ – актуальная правовая и техническая проблема, требующая решения.

Кодирование и изоляция «высококонфиденциальных» типов данных призвана обеспечить дополнительную защиту конфиденциальности, с одной стороны. Вместе с тем, с другой стороны, это отчасти ограничивает развитие ИИ-моделей в медицине и здравоохранении, поскольку из обучения ИИ исключаются существенные сведения, что может повлечь искажения результатов его работы впоследствии.

К. Хаберкосс полагает, что при разработке и обучении моделей ИИ либо использовании конфиденциальных данных действующими моделями, содержащими технологии ИИ, должен быть обеспечен уровень конфиденциальности, пропорциональный соответствующему типу обрабатываемых данных, учитывая потенциальный вред, который может быть причинен человеку в случае утечки его персональных данных, вне зависимости от того, насколько это было преднамеренно [2, p. 155].

Еще одним фактором информационно-правовой проблематики обработки медицинских данных, в том числе с применением ИИ, сегодня становится Интернет и средства телемедицины. Действительно, Интернет все шире используется человеком для поиска сведений об оценке своего здоровья, выбора и определения поставщиков медицинских услуг или услуг в сфере здравоохранения. Получают распространение формуляры и приложения с анкетиро-

ванием на различных сайтах различных учреждений, предлагающих оценить свое здоровье, поиск профильных специалистов, онлайн-консультации и др. Ряд данных, которые оставляет человек в таком анкетировании, может относиться к разряду конфиденциальных, однако получение их третьими сторонами, в том числе средствами ИИ, не всегда технически исключено и обеспечено. То есть, информация, оставленная человеком на интернет-сайте, может использоваться в числе прочего в форматах непрерывного обучения моделей ИИ, принадлежащих третьей стороне.

В случаях, если человек делает выбор в пользу вариантов телемедицины, подключаясь через Интернет, как правило, защита конфиденциальности предусматривается и гарантируется поставщиком соответствующих услуг телемедицины. Так, интернет-соединения и сайты, по которым предоставляются услуги телемедицины, должны находиться под техническим контролем и мониторингом поставщика услуг телемедицины с тем, чтобы определить, не был ли подключен ИИ к поступившим от пациента данным и данным консультации, т.е. требуется максимально устранить потенциальную угрозу конфиденциальности такого рода [2, p. 155].

Кроме того, К. Хаберкосс обращает внимание на то, как медицинские учреждения и их сотрудники должны соблюдать правила, направленные на обеспечение охраны конфиденциальной медицинской информации о пациентах – в объеме их компетенции. Это относится, в том числе, к ситуациям, когда врач, консультируя пациента либо проводя онлайн-оплату медицинских услуг и т.п., взаимодействует с технологиями ИИ. В таких случаях медицинское учреждение, по общему правилу, должно гарантировать, что персональные данные пациентов не будут переданы неизвестным источникам, в том числе системам ИИ [ibid].

В большинстве современных государств в том или ином виде сформировалось законодательство о защите персональных данных. Его цель – распределение рисков и ответственности за нарушения в сфере охраны персональных данных между человеком и организацией, которой персональные данные им передаются. Это относится и к сфере медицины и здравоохранения. Кроме того, в системе здравоохранения получает развитие правовой институт «информированного согласия», которое дает человек на проведение в отношении него определенных процедур, лечения, оказания иных видов медицинской помощи или услуг здравоохранения.

Расширение применения ИИ в сфере медицины и здравоохранения ставит вопрос реформирования этих институтов, поскольку в существующем виде они не всегда соответствуют объективным обстоятельствам информационного обмена и принятия решений затронутыми сторонами.

Анна Циммерман из Школы профессиональных исследований Колумбийского университета (США) ставит вопрос развития института «информированного согласия на применение ИИ» в здравоохранении [4].

По мнению А. Циммерман, использование средств ИИ в различных областях медицины и системах здравоохранения, как то – при постановке диагноза, ведении электронных медицинских карт пациентов, разработке и назначении лекарственных средств и препаратов и др. – требует установить допустимые формы и объемы раскрытия информации, обмен которой происходит в соответствующих процессах, в том числе в отношении определенных потребителей медицинских услуг. При этом, как указывает автор, юридически обязывающего права потребителя медицинских услуг знать, применяется ли в отношении него или его персональных данных обработка средствами ИИ, не существует [4, p. VI].

А. Циммерман при этом справедливо подчеркивает различие правового института «согласия на обработку персональных данных», которое зачастую дает человек, обращаясь за медицинской помощью или в другие учреждения системы здравоохранения, и «информированного согласия» пациента, подразумевающего, что человек проинформирован о предполагаемой форме лечения, процедурах и других воздействиях на его организм, а также о вероятных рисках и побочных эффектах соответствующих методов, прежде чем примет решение на них согласиться. Действительно, институт информированного согласия существенно отличается от того, чтобы разрешать или ограничивать распространение персональных данных пациента, что регулируется в основном в рамках законодательства о защите персональных данных, форматах государственной информационной политики и т.п. Тем не менее автор предлагает связать указанные два института при определении применимости ИИ в сфере здравоохранения – в форме «информированного согласия на применение ИИ», которое в числе прочего давал бы человек при обращении в учреждения здравоохранения [4, p. VII].

По мнению А. Циммерман, институт информированного согласия на применение ИИ в здравоохранении стал бы оптимальной

формой интеграции ИИ в медицинскую практику и в систему здравоохранения, с уважением автономии и выбора человека. Автор предлагает, опираясь на правовой институт информированного согласия, оформление информированного согласия на применение ИИ – на различных стадиях обращения человека в учреждения здравоохранения. По мнению исследователя, это не создает принципиально новых этических рисков, но гарантирует человеку выбор – готов ли он принять рекомендации ИИ для своего лечения или иных медицинских процедур – либо откажется от них, предпочтя рекомендации врача без обращения его к ИИ-инструментарию [4, p. 35].

Заключение

Системные решения по регулированию цифровизации медицины и здравоохранения носят многоуровневый характер. На государственном уровне требуется вынести вопросы безопасности в сфере здравоохранения в основные направления политики обеспечения государственной безопасности и торговли, в частности, путем внедрения жестких стандартов на импорт медицинских изделий и цифрового медицинского оборудования, обеспечение их соответствия нормативным критериям кибербезопасности. Важное значение имеет развитие международного сотрудничества в сфере кибербезопасности в здравоохранении. На уровне профильных министерств и ведомств в сфере здравоохранения необходима разработка нормативов и стандартов, направленных на обеспечение государственной политики по кибербезопасности в отношении цифровых медицинских технологий и информационных систем, сертификация, мониторинг, надзор. На всех уровнях учреждений медицины и здравоохранения необходимо обеспечить соблюдение государственных нормативов, стандартов и рекомендаций, а также внедрение и соблюдение протоколов кибербезопасности в информационных системах.

Внедрение технологий ИИ в медицине и здравоохранении, помимо преимуществ в оперативности и качестве оказания медицинских услуг и услуг в сфере здравоохранения, несет новые риски охране персональных данных и медицинских данных. Актуальность приобретает общественный запрос к медицинским учреждениям и организациям обеспечить анализ и противодействие рискам, связанным со сбором, использованием и передачей медицинских и иных данных своих информационных систем. Новую роль и зна-

чение приобретает как правовой институт согласия на обработку персональных данных, так и институт информированного согласия пациента.

Некоторые специалисты предлагают разработать и внедрить в юридическую практику новый институт – информированного согласия на применение ИИ в здравоохранении.

Список литературы

1. Abo A., Lantzy S. Cybersecurity Challenges of Digital Health and AI in Healthcare // Digital Health, AI and Generative AI in Healthcare: A Concise, Practical Guide for Clinicians / Ed. Terry Adirim. – Cham: Springer, 2025. – P. 165–178.
2. Habercoss K. Privacy and Legal Issues in the Use of Artificial Intelligence // Digital Health, AI and Generative AI in Healthcare: A Concise, Practical Guide for Clinicians / Ed. Terry Adirim. – Cham: Springer, 2025. – P. 149–163.
3. Tabish S.M. Health Care Management: Principles and Practice. – Singapore: Springer, 2024. – 760 p.
4. Zimmerman A. Informed Consent for AI and Health Care: Consumer Rights and Industry Obligations. – Cham: Springer, 2026. – 101 p.