

## ПРАВОВЫЕ ПРОБЛЕМЫ ЗАЩИТЫ И ПЕРЕНОСИМОСТИ ДАННЫХ ПАЦИЕНТОВ В МЕДИЦИНСКИХ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИХ СИСТЕМАХ\*

Д. А. Лебедева

*Национальный исследовательский университет «Высшая школа экономики»*

## LEGAL ISSUES OF PROTECTION AND PORTABILITY OF PATIENT DATA IN MEDICAL INFORMATION AND ANALYTICAL SYSTEMS

D. A. Lebedeva

*National Research University «Higher School of Economics»*

**Аннотация:** статья посвящена исследованию проблем в области обеспечения защиты и переносимости данных пациентов в медицинских информационно-аналитических системах (далее – МИАС). Цель исследования – комплексный анализ правового регулирования МИАС субъектов Российской Федерации. Были выявлены следующие недостатки защиты медицинских данных пациентов: отсутствие единообразных требований к защите медицинской информации в МИАС разных субъектов Российской Федерации, проблема переносимости медицинской информации из МИАС одного субъекта Российской Федерации в другой, финансовые и технические проблемы создания федеральной единой государственной информационной системы здравоохранения Российской Федерации (далее – ЕГИСЗ РФ). Основным практическим ограничением исследования является отсутствие доступной информации об уровне цифровизации в сфере здравоохранения и о зарегистрированных утечках данных пациентов в отдаленных регионах России. Методологическим ограничением исследования является несовпадение подходов законодателя и ученых-правоведов, касающихся уровня доступа государства к данным пациентов и способам хранения медицинской информации в учреждениях здравоохранения. Необходимость перехода всех субъектов Российской Федерации к ЕГИСЗ РФ будет способствовать решению проблемы переносимости медицинской информации при переезде пациента из одного субъекта Российской Федерации в другой субъект путем автоматической выгрузки его медицинских данных с согласия пациента. Автор предлагает создать единые стандарты для взаимодействия МИАС всех субъектов Российской Федерации, усилить меры информационной безопасности путем усиления ответственности в законодательстве о персональных данных за нарушение правил защиты медицинских данных пациентов.

**Ключевые слова:** медицинские информационно-аналитические системы, единая государственная информационная система здравоохранения, защита медицинских данных, переносимость медицинских данных.

**Abstract:** the article is devoted to the study of problems in the field of ensuring the protection and portability of patient data in medical information and analytical systems (hereinafter – MIAS). The purpose of the study is a comprehensive analysis of the legal regulation of the MIAS of the constituent entities of the Russian Federation. The study identified the following disadvantages of protecting patients' medical data were identified: the lack of uniform requirements for the protection of medical information in the MIAS of different subjects of the Russian Federation, the problem of the portability of medical information from the MIAS of one subject of the Russian Federation to another, financial

---

\* Исследование выполнено за счет гранта Российского научного фонда № 25-18-00698, <https://rscf.ru/project/25-18-00698/>

© Лебедева Д. А., 2026

and technical problems of creating the federal unified state health information system of the Russian Federation (hereinafter – the EGISZ of the Russian Federation). The main practical limitation is the lack of accessible information on the level of digitalization in healthcare and on registered leaks of patient data in remote regions of Russia. The methodological limitation is the discrepancy between the approaches of the legislator and legal scholars regarding the level of government access to patient data and the methods of storing medical information in healthcare institutions. The need for all subjects of the Russian Federation to switch to the Unified State Register of Medical Sciences of the Russian Federation, which will contribute to solving the problem of the portability of medical information when a patient moves from one subject of the Russian Federation to another subject by automatically uploading his medical data with the consent of the patient. The author also proposes to create uniform standards for the interaction of MIAS of all subjects of the Russian Federation, to strengthen information security measures by strengthening responsibility in the legislation on personal data for violation of the rules for the protection of medical data of patients.

**Key words:** medical information and analytical systems, unified state health information system, protection of medical data, portability of medical data.

В условиях цифровизации в современном здравоохранении медицинские информационно-аналитические системы приобрели значимую роль, предоставляя возможность оперативного сбора, обработки и анализа медицинских данных для повышения качества медицинской помощи и оптимизации ресурсов здравоохранения. Эти системы объединяют множество процессов, в том числе хранения электронных медицинских карт, диагностирования, планирования лечения, управления ресурсами медицинских учреждений. В связи с этим МИАС становятся ключевым инструментом как для врачей, так и для пациентов и ученого сообщества.

В доктрине существуют широкое и узкое понимание медицинской информационной системы. Так, в узком смысле Р. Хаукс под медицинской информационной системой понимает систему, которая используется медицинскими учреждениями для обработки персональных и медицинских данных в сфере здравоохранения<sup>1</sup>.

В широком смысле, по мнению М. В. Ашпетоной, медицинской информационной системой считается программное обеспечение, предназначенное для автоматизации задач медицинских организаций, в том числе для ведения персонализированного учета медицинских услуг пациента на основе единой электронной медицинской карты<sup>2</sup>.

<sup>1</sup> См.: Reinhold Haux *Medical informatics : past, present, future* // International journal of medical informatics. 2010. No. 79. P. 599–610.

<sup>2</sup> См.: Ашпетоной М. В. Особенности цифровизации МИС как инструмента повышения качества работы лечебных учреждений // Татищевские чтения : актуальные проблемы науки и практики. Тольятти : Волж. ун-т им. В. Н. Татищева (Ин-т), 2021. Т. 1. С. 155.

Кроме того, под медицинской информационной системой подразумевается совокупность программно-технических средств, баз данных и знаний, предназначенных для автоматизации различных процессов, протекающих в лечебно-профилактических учреждениях в системе здравоохранения<sup>3</sup>.

Целью исследования является комплексный анализ правового регулирования МИАС субъектов Российской Федерации. Задачами исследования выступают необходимость выявления недостатков системы защиты медицинских данных пациентов, находящихся в МИАС субъектов Российской Федерации, анализ устройства и правового регулирования зарубежных МИАС, выявление их преимуществ и недостатков, а также разработка предложений по совершенствованию отечественного законодательства в части защиты и переноса медицинских данных на примере зарубежных МИАС.

В рамках исследования были использованы общенаучные методы: анализ и синтез, дедукция и индукция, прогнозирование, моделирование, а также специальные методы: технико-юридический и сравнительно-правовой. Автором проведен анализ российского законодательства в сфере требований к обработке и охране персональных данных пациентов в МИАС, а также изучено законодательство зарубежных стран (США, Австралия и ЕС). Всего было проанализировано 65 источников из общедоступных и открытых баз данных, однако в работу вошли всего 27, так

<sup>3</sup> См.: Назаренко Г. И., Гулиев Я. И., Ермаков Д. Е. *Медицинские информационные системы : теория и практика* / под ред. Г. И. Назаренко, Г. С. Осипова. М. : Физматлит, 2005. С. 120.

как их содержание способствовало решению поставленных задач и отражало цели работы.

В настоящее время в Российской Федерации ведутся работы по созданию и введению в эксплуатацию единой государственной информационной системы здравоохранения Российской Федерации. К концу 2024 г. все медицинские учреждения должны были интегрировать медицинские данные пациентов в данную систему. В 2025 г. не все медицинские учреждения были интегрированы в единую государственную информационную систему здравоохранения Российской Федерации, официальных данных в настоящее время не представлено.

В целом основу правового регулирования МИАС в Российской Федерации составляют несколько ключевых законов, которые охватывают защиту персональных данных, обеспечение безопасности информации и организацию взаимодействия медицинских учреждений в цифровой среде, а именно:

1. Федеральный закон № 152-ФЗ<sup>4</sup> – основополагающий нормативный правовой акт, устанавливающий правовое регулирование обработки и защиты персональных данных. Закон регулирует также обработку и защиту медицинских данных, поэтому его положения применяются и к деятельности МИАС. Согласно ст. 19 указанного федерального закона оператор, обрабатывающий персональные данные, обязан принять необходимые правовые, организационные и технические средства защиты или гарантировать их принятие, чтобы обезопасить персональные данные от несанкционированного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения или иных неправомерных действий. Основные обязанности операторов обработки персональных данных включают следующее: определение потенциальных угроз безопасности персональных данных при их обработке в информационных системах, использование процедур оценки соответствия средств защиты информации, оценку эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных, учет машинными носителями персональных данных, и т. д.

<sup>4</sup> См.: О персональных данных : федер. закон от 27 июля 2006 г. № 152-ФЗ // Собр. законодательства Рос. Федерации. 2006. № 31 (1 ч.). Ст. 3451.

2. Федеральный закон № 323-ФЗ<sup>5</sup>, устанавливающий правовое регулирование системы здравоохранения и определяющий цифровизацию в этой сфере. В соответствии со ст. 13 закона врачебная тайна включает в себя информацию о фактическом обращении пациента за медицинской помощью, его состоянии здоровья и диагнозе, а также иные сведения, полученные пациентом во время его медицинского обследования и лечения. Однако законодательно не установлена специальная правовая норма, определяющая меры ответственности за разглашение врачебной тайны. Ответственность в этом случае наступает согласно ст. 13.14 КоАП РФ<sup>6</sup> или ст. 137 УК РФ<sup>7</sup>. Более того, ч. 4 ст. 13 указанного федерального закона ограничивает право пациента на врачебную тайну в определенных случаях. Например, с целью проведения медицинского обследования и лечения пациента, который не способен выразить свою волю по причине состояния здоровья, а также при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений. При этом стоит отметить, что в российском законодательстве, в отличие от зарубежных стран, не предусмотрено уведомление пациентов об ограничении врачебной тайны. Например, в Королевстве Дании установлены меры достаточно незамедлительного уведомления пациента об игнорировании (ограничении) его права на врачебную тайну<sup>8</sup>. Основы использования информационных технологий в сфере здравоохранения, включая создание и использование электронных медицинских карт, а также обеспечение безопасности медицинских данных, раскрываются в ст. 91 Федерального закона № 323-ФЗ. Указанный нормативный правовой акт был дополнен ст. 91.1,

<sup>5</sup> См.: Об основах охраны здоровья граждан в Российской Федерации : федер. закон от 21 ноября 2011 г. № 323-ФЗ // Собр. законодательства Рос. Федерации. 2011. № 48. Ст. 6724.

<sup>6</sup> См.: Кодекс Российской Федерации об административных правонарушениях : федер. закон от 30 декабря 2001 г. № 196-ФЗ // Собр. законодательства Рос. Федерации. 2002. № 1 (ч. 1). Ст. 1.

<sup>7</sup> См.: Уголовный кодекс Российской Федерации : федер. закон от 13 июня 1996 г. № 63-ФЗ // Собр. законодательства Рос. Федерации. 1996. № 25. Ст. 2954.

<sup>8</sup> См.: Павлов А. В. Правовое регулирование общественных отношений по поводу врачебной тайны в Королевстве Дания и в Российской Федерации : сравнительный анализ // Журнал зарубежного законодательства и сравнительного правоведения. 2017. № 4. С. 77.

регламентирующей развитие и эксплуатацию единой государственной информационной системы в сфере здравоохранения и установившей основания для введения в действие единой государственной информационной системы в сфере здравоохранения, раскрывая основные положения о ее работе.

3. Постановление правительства № 140<sup>9</sup>, в котором содержатся основные положения о порядке доступа к медицинской информации между участниками цифрового взаимодействия в рамках единой государственной системы здравоохранения. Данный нормативно-правовой акт регламентирует структуру и порядок ведения единой системы здравоохранения, а также устанавливает требования к программно-техническому обеспечению участников ЕГИСЗ и содержит перечень рекомендованных информационных систем. В структуру единой системы здравоохранения входит 9 федеральных регистров, реестров и подсистем, которые отвечают за защиту и обмен информацией между различными государственными органами (Минздрав, Росздравнадзор, ФМБА РФ, СФР, Минцифры). Непосредственно с медицинской информацией пациента работают 3 подсистемы: а) федеральная электронная регистратура обеспечивает доступ граждан к медицинским услугам посредством МИАС; б) федеральная интегрированная электронная медицинская карта формирует базы данных с обезличенной информацией пациентов и обеспечивает доступ медицинских работников к ним; в) федеральный реестр электронных медицинских документов осуществляет получение, проверку, обработку и хранение медицинской документации пациентов в электронном виде.

В условиях продолжающегося развития технологий и увеличения объемов данных актуальное законодательство не всегда успевает адаптироваться к современным условиям, что создает правовые пробелы, а также сложности в обеспечении необходимой защиты информации в МИАС.

Сейчас в отдельных субъектах РФ (Московская область, Республика Татарстан, Краснодарский край, Свердловская область, Ростовская область и др.) наблюдается использование нескольких

МИАС одновременно. Каждое медицинское учреждение имеет свои особенности документооборота, требования к формированию медицинской карты и исследований, что затрудняет возможность быстрого и унифицированного перехода на единую информационную систему. Более того, каждый субъект в настоящее время самостоятельно определяет разработчика МИАС (IT-платформу), на которой размещаются данные всех пациентов. При этом внутреннее наполнение МИАС в некоторых случаях существенно отличается в зависимости от регионов, что вызывает логичные вопросы к реальности объединения в единую федеральную МИАС. Такой переход должен сопровождаться выбором единственного подрядчика, способного единым образом настроить во всех 89 субъектах РФ МИАС и учесть все недостатки IT-платформ, на которых в настоящее время содержатся медицинские данные пациентов.

Кроме того, в субъектах РФ наблюдается разный уровень цифровой грамотности среди медицинских работников, что также является одним из барьеров для цифровизации исследуемой отрасли<sup>10</sup>.

Тем не менее переход на ЕГИСЗ РФ способствует обеспечению унифицированного взаимодействия между медицинскими учреждениями из разных субъектов РФ. При этом не стоит исключать вероятность утечки медицинских данных пациентов в процессе их передачи в ЕГИСЗ РФ, поскольку до настоящего времени на законодательном уровне не разработан единый механизм переноса данных из региональных МИАС в ЕГИСЗ РФ, который будет конфиденциально обеспечивать передачу данных пациентов без каких-либо утечек информации.

Рост объемов обрабатываемых данных в МИАС обуславливает потребность в обеспечении их безопасности и конфиденциальности. Изначально основная задача МИАС заключалась в сборе и хранении аналитической и статистической информации, а именно сборе и обработке статистической отчетности. Однако позже структурно и функционально первоочередной задачей стало обеспечение функциони-

<sup>9</sup> См.: О единой государственной информационной системе в сфере здравоохранения : постановление Правительства РФ от 21 февраля 2022 г. № 140 // Собр. законодательства Рос. Федерации. 2022. № 8. Ст. 1152.

<sup>10</sup> См.: Гусев А. В., Владимирский А. В., Голубев Н. А., Зарубина Т. В. Информатизация здравоохранения Российской Федерации : история и результаты развития // Национальное здравоохранение. 2021. № 2 (3). С. 16.

рования информационных систем<sup>11</sup>. При этом особенностью медицинских информационных ресурсов является наличие в их составе объединенной информации, сбор, обработка и хранение которой регулируются различными нормативными правовыми актами<sup>12</sup>. Например, после внедрения Единой медицинской информационно-аналитической системы в г. Москве возникла проблема обеспечения конфиденциальности информации, составляющей врачебную тайну, ввиду наличия у любого сотрудника из числа административного персонала прав доступа к информационной системе и отсутствия согласия на обработку данных о состоянии здоровья третьими лицами<sup>13</sup>. В этом случае неправомерно раскрываются сведения, относящиеся к медицинской тайне, а также информация, которая одновременно может составлять профессиональную тайну и тайну частной жизни.

Кроме того, получение согласия на обработку персональных данных от субъекта в настоящее время стало более формальным и часто не отражает фактической воли человека<sup>14</sup>. Согласно А. И. Савельеву, иной проблемой обработки персональных данных является сложность определения перечня персональных данных и их способы обработки и цели ввиду динамичности развития медицинских информационных систем<sup>15</sup>.

<sup>11</sup> См.: Позднякова М. А., Коновалов А. А. Медицинский информационно-аналитический центр в системе организации информационного обеспечения региональной системы здравоохранения // Профилактическая медицина как научно-практическая основа сохранения и укрепления здоровья населения : сб. науч. трудов / под общ. ред. М. А. Поздняковой. Ниж. Новгород : Ремедиум Приволжье, 2016. Т. 3. С. 182.

<sup>12</sup> См.: Амелин Р. В., Бессонов Л. В. Правовой режим информационных ресурсов медицинских информационных систем // Известия Саратов. ун-та. Новая серия. Сер.: Экономика. Управление. Право. 2019. № 19 (4). С. 428.

<sup>13</sup> См.: Анашкина Е. Д. Единая медицинская информационно-аналитическая система : особенности и перспективы // Математические модели техники, технологий и экономики : материалы Всерос. науч.-практ. студ. конф. (Санкт-Петербург, 14–15 мая 2019 г.). СПб. : ПОЛИТЕХ-ПРЕСС, 2019. С. 76.

<sup>14</sup> См.: Mantovani E., Quinn P. mHealth and data protection – the letter and the spirit of consent legal requirements // International Review of Law, Computers & Technology. 2014. Vol. 28. Issue 2. P. 222.

<sup>15</sup> См.: Савельев А. И. Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) // Право : журнал Высшей школы экономики. 2015. № 1. С. 49.

В связи с этим перед правоприменителями и учеными-правоведами стоят две проблемы, а именно – правовое обеспечение защиты данных, а также их переносимости.

Правовое регулирование защиты информации в МИАС включает требования к конфиденциальности, обеспечению сохранности и безопасности персональных данных. Вопросы защиты медицинской информации приобретают особую значимость в условиях тенденции увеличения количества зарегистрированных преступлений, совершаемых с использованием информационных технологий, а также увеличения количества случаев утечки персональных данных<sup>16</sup>. Например, за январь и февраль 2025 г. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций зафиксировала 19 фактов утечек персональных данных, в результате которых в открытом доступе оказались более 24 млн записей российских пользователей. Самая крупная утечка персональных данных в России произошла в секторе предоставления государственных услуг в начале января 2025 г. В результате совершенного преступления был получен доступ к более чем 2 млрд строк, общим размером около 1 Тб, включая паспортные данные, даты рождения, СНИЛС, ИНН, место жительства и регистрации и пр.

Органы государственной власти, по мнению Н. А. Назарова, обязаны обеспечивать актуальность и достоверность медицинских данных, находящихся в информационных системах<sup>17</sup>. Проблема переносимости медицинских данных возникает в процессе смены места жительства пациента. В связи с тем что законодательством РФ не предусмотрен процесс переноса данных пациента с одной МИАС в другую, то, например, при переезде пациента из одного субъекта в другой пациенту необходимо заводить новую медицинскую карту. При этом какого-либо сохранения данных о прежних медицинских заключениях, сданных анализах пациента автоматически не происходит. Безусловно, пациент имеет возможность сделать дубликат электронной медицинской карты, но вряд ли такой руч-

<sup>16</sup> См.: Статистические сведения о преступлениях за 2023 г. // ФКУ «ГИАЦ МВД России». URL: <https://xn--b1aew.xn--p1ai/folder/101762> (дата обращения: 15.03.2025).

<sup>17</sup> См.: Назаров Н. А. Обеспечение качества данных при автоматизированном принятии решений в государственном управлении // Журнал рос. права. 2024. № 5. С. 148.

ной перенос медицинской информации удобен, например для пожилых пациентов.

Фактически без направления запроса новым лечащим врачом о заболеваниях пациента в прежнее медицинское учреждение данные не могут быть получены. Кроме того, это занимает значительное время из-за бюрократической волокиты. Проблема переносимости медицинских данных влияет на получение качественной медицинской помощи и скорость получения лечения. Для решения данной проблемы предлагается создать автоматический доступ к региональным МИАС при смене места жительства пациентов для лечащих врачей после получения согласия от пациента или его законного представителя. Похожая процедура переноса медицинских данных реализована в США. При переезде в другой штат пациенту необходимо заполнить электронную форму о том, какие данные он хочет перенести и в какую новую медицинскую организацию<sup>18</sup>. Однако такой способ может вызвать ряд проблем, среди которых необходимость выбрать медицинское учреждение до переезда и отсутствие оповещения о необходимости заполнения формы.

Другим решением данной проблемы является подключение всех субъектов с региональной к федеральной ЕГИСЗ РФ. Данный переход способствует упрощению процедуры переноса медицинских данных, автоматически открывая доступ к данным пациента для врачей.

На международном уровне подобные медицинские системы достаточно распространены и стали необходимой поддержкой для специалистов и пациентов, в частности при трансграничных операциях, а их использование предполагает комплексное правовое регулирование (первые медицинские информационные системы появились еще в конце 60-х гг. прошлого столетия и были ориентированы на применение при оказании неотложной помощи)<sup>19</sup>. Например, одной из наиболее развитых международных баз данных является система электронных медицинских записей (Electronic health record, далее – EHR), которая широко используется в странах ЕС и США. В странах Европы действует Общий ре-

гламент по защите данных (General data protection regulation, далее – GDPR), который установил требования в сфере защиты и обеспечения переносимости медицинских данных, создавая основу для функциональной совместимости и соблюдения прав пациентов<sup>20</sup>.

В США существует национальная информационная сеть здравоохранения, способствующая свободному обмену медицинскими данными пациентов между учреждениями разных штатов. Однако в научной литературе выделяется один из «минусов» введения национальной информационной сети в США, который заключается в том, что сотрудники медицинских учреждений стали тратить больше времени на заполнение документации в электронном формате<sup>21</sup>. В Великобритании на территории всей страны действует единый центр здравоохранения и социального обеспечения, который включает в себя свободный обмен информацией между медицинскими учреждениями, доступ пациентов к их истории заболевания, позволяет заказать рецепт на лекарства и записаться к врачу<sup>22</sup>.

В Австралии действует система «Моя медицинская карта», созданная в рамках формирования электронного документооборота медицинских данных, хранящая историю болезней пациентов, результаты анализов, назначенное лечение, список экстренных контактов. Стоит отметить, что человек может самостоятельно удалить данные, хранящиеся в системе. В практике также были случаи неправомерного использования медицинских данных, хранящихся в системе, и их неправомерное завладение, несмотря на принимаемые меры защиты для увеличения уровня защиты медицинской информации<sup>23</sup>. Кроме

<sup>20</sup> См.: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679> (date of access: 15.03.2025).

<sup>21</sup> См.: Momenipur A., Priyadarshini R. Balancing documentation and direct patient care activities : a study of a mature electronic health record system // International journal of industrial ergonomics. 2019. Vol. 72. P. 338–346.

<sup>22</sup> См.: Chapman JR., Wang JC., Wiechert K. Big Spine Data Put to Good Use : the NHS Sets an Example // Global Spine J. 2019. P. 689–691.

<sup>23</sup> См.: Holt M., MacGibbon J., Smith A., Broady TR., Davis MD., Newman CE. Knowledge of Australia's My Health Record and factors associated with opting out : results from a

<sup>18</sup> См.: Summary of the HIPAA Security Rule. URL: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9977020/> (date of access: 19.01.2025).

<sup>19</sup> См.: Кулаков А. А., Серегин С. С. История развития медицинских информационных систем // Стоматология. 2015. № 94 (6). С. 51.

того, в настоящее время в Австралии пациенту приходит уведомление при использовании его медицинской карты сотрудником медицинского учреждения.

Нормативное регулирование данной сферы общественных отношений в зарубежных странах продолжает развиваться. Так, в 2019 г. были опубликованы новая редакция рекомендаций и приложение к ней, в которых установлены принципы, составляющие основу работы ЕНР:

а) «защита и конфиденциальность данных», т. е. полное соблюдение правил конфиденциальности и законодательства о защите данных, начиная со стадии разработки;

б) «согласие или другое законное основание», т. е. наличие юридического основания для обработки данных;

в) «безопасность», т. е. внедрение соответствующих технических и организационных мер для защиты систем ЕНР от любых рисков<sup>24</sup>.

А. Е. Демкина полагает, что зарубежный опыт иллюстрирует длительность и дороговизну цифровой трансформации системы здравоохранения<sup>25</sup>. По мнению А. В. Гусева, одной из проблем на пути цифровизации здравоохранения в России является ее дороговизна, в частности отсутствие финансирования отрасли и ожидание отдельных субъектов получения медицинской информационной системы бесплатно и в императивном порядке<sup>26</sup>. Кроме того, уровень развития ИТ-технологий в государстве влияет на то, насколько много инноваций внедряется на практике. Тем не менее государствам необходимо идти по пути цифровизации, так как

national survey of the Australian general population and communities affected by HIV and sexually transmissible infections. PLOS Digit Health. 2023. URL: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9977020/> (date of access: 19.09.2025).

<sup>24</sup> См.: *Bincoletto G.* Data protection issues in cross-border interoperability of Electronic Health Record systems within the European Union. *Data & Policy*. 2020. P. 3–4. URL: [https://www.researchgate.net/publication/340274165\\_Data\\_protection\\_issues\\_in\\_crossborder\\_interoperability\\_of\\_Electronic\\_Health\\_Record\\_systems\\_within\\_the\\_European\\_Union](https://www.researchgate.net/publication/340274165_Data_protection_issues_in_crossborder_interoperability_of_Electronic_Health_Record_systems_within_the_European_Union) (date of access: 08.09.2025).

<sup>25</sup> См.: *Демкина А. Е.* Эволюция цифровой медицины. Мировой и отечественный опыт // *Вестник Моск. унта. Сер. 21, Управление (государство и общество)*. 2023. Т. 20, № 2. С. 17.

<sup>26</sup> См.: *Гусев А. В.* Медицинские информационные системы : состояние, уровень использования и тенденции // *Врач и информационные технологии*. 2011. № 3. С. 13.

данное способствует увеличению скорости оказываемой медицинской помощи и повышению ее доступности.

В то же время необходимо развивать интероперабельность (способ взаимодействия субъектов здравоохранения с помощью технологий) информационных систем для решения проблемы переносимости данных. Переносимость медицинских данных означает возможность перемещать и повторно использовать данные между приложениями и информационными системами, чтобы облегчить обмен данными и не допустить «застревания» информации в автономных, изолированных системах<sup>27</sup>. Учитывая ее тесную связь с защитой прав потребителей, экономической свободой, защитой конкуренции и другими правовыми институтами, представляется, что по мере дальнейшего роста цифровых платформ право на переносимость данных будет поддерживаться и расширяться в законах многих стран.

Помимо этого, рекомендуется использовать зарубежную практику цифровизации в сфере здравоохранения, в частности для защиты персональных данных пациентов и обеспечения их безопасности необходимо настроить систему мобильных уведомлений при использовании медицинской карты сотрудником медицинского учреждения. В таком случае пациент будет уведомлен об использовании его данных и обеспечивается его информированность.

Настоящее исследование выполнено на основе открытых источников, включая 20 публикаций в периодических изданиях, научных сборниках и 7 нормативных актов. Основным практическим ограничением является отсутствие доступной информации об уровне цифровизации в сфере здравоохранения и о зарегистрированных утечках данных пациентов в отдаленных регионах России. Методологическим ограничением является несоответствие подходов законодателя и ученых-правоведов, касающихся уровня доступа государства к данным пациентов и способам хранения медицинской информации в учреждениях здравоохранения. В рамках государственного подхода обширный доступ к информации о здоровье граждан оправдывается необходимостью обеспечения национальной безопасности и защиты общественных ин-

<sup>27</sup> См.: *Журавлев М. С.* Интероперабельность как фактор развития права в сфере электронного здравоохранения. // *Право : журнал Высшей школы экономики*. 2019. № 3. С. 103.

тересов. Исходя из подхода ученых-правоведов, аккумуляция значительных массивов информации пациентов в МИАС неизбежно порождает повышенные риски утечек. В России уже были случаи утечки медицинской информации пациентов из-за недобросовестной работы администраторов и хакерских атак на базы данных и сервера, таким образом, обеспечение высокой степени защиты больших медицинских данных является критически важной задачей для государства. Для преодоления методологического ограничения и обеспечения достоверности выводов исследования были дополнительно проанализированы акты «мягкого права», т. е. рекомендации, не имеющие обязательный характер, в частности пояснительные записки, комментарии к нормативно-правовым актам и методические рекомендации.

В Российской Федерации продолжается дискуссия об информатизации различных процессов в системе здравоохранения, в том числе в рамках лечебно-диагностического процесса, а также процесса управления и планирования. В частности, ряд подзаконных актов Правительства РФ предполагает постепенное внедрение мероприятий по информатизации, например, изменения были внесены в государственную программу «Развитие здравоохранения», а также в отдельные соглашения между Министерством здравоохранения РФ и субъектами страны<sup>28</sup>. Кроме того, в рамках Федерального проекта «Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ)» Министерство здравоохранения РФ поручило государственным клиникам разработать план перехода на единую медицинскую информационную систему до конца 2024 г. В настоящее время во всех клиниках был разработан план перехода на единую систему, функционирует централизованная подсистема «Телемедицинские консультации», все медицинские учреждения обеспечивают доступ к электронным медицинским документам посредством личного кабинета пациента «Моё здоровье» на Едином портале государственных и муниципальных услуг.

<sup>28</sup> См.: Коновалов А. А. Актуальные правовые аспекты организации деятельности медицинского информационно-аналитического центра в ходе его функциональной эволюции // Врач и информационные технологии. 2016. № 2. С. 10.

Создание ЕГИСЗ РФ стоит оценивать неоднозначно. Выделим следующие достоинства перехода всех субъектов РФ к ЕГИСЗ РФ:

1) все учреждения здравоохранения будут иметь единый доступ к медицинским данным и свободно обмениваться информацией, что сокращает затраты на проведение первичной консультации и увеличивает качество постановки предварительного диагноза на основе полученных данных из всех учреждений;

2) единый доступ учреждений из разных регионов к медицинским данным способствует решению проблемы их переносимости при смене места жительства пациента. Это обеспечивает сохранность медицинской информации, упрощает доступ к ним для врачей и пациентов и увеличивает скорость постановки медицинского заключения.

В то же время введение единой медицинской информационной системы имеет ряд недостатков:

1) в некоторых медицинских учреждениях наблюдается продолжение практики ведения бумажной документации вместе с электронным документооборотом, удваивающее временные затраты персонала учреждения вместо оказания качественной медицинской помощи и уделения времени и внимания пациенту. В отдельных регионах используются устаревшие оборудование и программное обеспечение, многие сотрудники не приспособлены к ведению документации в электронной форме, поэтому остаются приверженцами проверенных бумажных носителей информации;

2) финансовые затраты на переход всех регионов к ЕГИСЗ РФ, связанные с закупкой нового оборудования, программного обеспечения, проведения обучения среди сотрудников учреждений здравоохранения;

3) при технических сбоях и ошибках в ЕГИСЗ РФ будет затронута деятельность всех учреждений здравоохранения, что способствует увеличению времени приема пациента и большей степени незащищенности его медицинских данных.

Стоит отметить другую проблему. Так, для ряда регионов было затруднительно перейти на медицинскую информационную систему, техническими возможностями для проведения цифровизации учреждений здравоохранения обладают далеко не все субъекты РФ. Например, в Республике Ингушетия переход на единую

информационную систему завершится только в 2024 г. Низкий уровень внедрения информационных технологий в отдельных субъектах РФ влечет необходимость построения системы с чистого листа и дальнейшего присоединения к единой системе, что способствует увеличению финансовых затрат на проведение медицинской цифровизации.

Проведенное исследование позволило нам сделать следующие выводы.

1. Правовое регулирование защиты данных и обеспечение их переносимости в МИАС осложнены рядом проблем, которые затрудняют эффективное функционирование этих систем и защиту данных пациентов, а именно: отсутствуют единые стандарты функциональной совместимости (интероперабельности), наблюдается недостаток единых стандартов для взаимодействия различных МИАС между собой, в результате чего медицинские учреждения вынуждены использовать разные программные продукты, которые не всегда совместимы друг с другом, что затрудняет обмен данными. Отсутствие таких стандартов может привести к фрагментации данных и снижению эффективности системы здравоохранения. Для решения данной проблемы рекомендуется возложить на Министерство здравоохранения обязанность провести проверку существующих стандартов взаимодействия МИАС между собой, выявить неактуальные положения стандартов и объединить их с существующими для устранения дублирующихся стандартов и формирования единого положения для МИАС, регулирующей порядок взаимодействия между МИАС, порядок обмена данными, способы защиты персональных данных и меры, которые организация должна предпринять для защиты медицинских персональных данных. Для защиты персональных данных пациентов и обеспечения их безопасности необходимо настроить систему мобильных уведомлений при использовании медицинской карты сотрудником медицинского учреждения. Предлагается внести изменения в п. 14 постановления Правительства № 140<sup>29</sup>, следовательно, расширить перечень функций федеральной интегрированной электронной медицинской карты, которая является подсистемой ЕГИСЗ и отвечает за доступ меди-

цинских работников к электронной медицинской карте пациентов.

2. Недостаточно регламентированы вопросы обеспечения переносимости данных. Так, в российском законодательстве, в отличие от ЕС, где действует соответствующий регламент GDPR, отсутствует необходимое регулирование прав пациентов на переносимость медицинских данных между различными медицинскими учреждениями. Пациенты не всегда могут легко переместить свои данные из одной системы в другую, что создает препятствия при смене медицинского учреждения или при необходимости получения медицинской помощи в зарубежных странах. Необходимо предусмотреть права пациентов по перенесению медицинских данных между медицинскими учреждениями, установить способы их перенесения, контрольно-надзорные мероприятия, контролирующие уровень переносимости медицинских данных пациентов и ввести меры ответственности для организаций, которые при наличии технических возможностей и ресурсов не переносят медицинские данные по запросу пациентов. Кроме того, предлагается автоматизировать внесение изменений о смене места жительства в полис обязательного медицинского страхования, путем автоматизации смены места жительства персональные данные пациентов будут автоматически отображаться в медицинской организации по месту нового прикрепления полиса. Для реализации данного предложения необходимо внести изменения в п. 16 постановления Правительства № 140<sup>30</sup> и предложенный функционал возложить на федеральный реестр электронных медицинских документов (подсистема ЕГИСЗ), который отвечает за предоставление доступа пациентам к медицинской документации, следит за электронным документооборотом медицинской информации в МИАС.

3. Неудовлетворительный уровень защиты информации. Хотя Федеральный закон № 152-ФЗ «О персональных данных» и устанавливает требования в сфере защиты персональных данных, в действительности уровень защищенности медицинских систем нередко остается несовершенным. МИАС обрабатывают большое количество персональных данных, следовательно, их защита требует усиления мер безопасности, включая использование современных решений

<sup>29</sup> См.: О единой государственной информационной системе в сфере здравоохранения : постановление Правительства РФ от 21 февраля 2022 г. № 140 // Собр. законодательства Рос. Федерации. 2022. № 8. Ст. 1152.

<sup>30</sup> См.: Там же.

и средств контроля доступа. В частности, предлагается увеличить меры ответственности за нарушение использования персональных данных пациентов, ввести для медицинских учреждений обязательную разработку положения о защите персональных данных пациентов и регулярно проводить контроль над его исполнением.

4. Пробелы правового регулирования ответственности за утечку данных. Несмотря на то что нарушения в области эксплуатации МИАС охватываются нормами административного и уголовного законодательства, в настоящее время не предусмотрена специальная норма, устанавливающая ответственность за утечку медицинских данных, тогда как информация о пациентах может быть использована неправомерно, а механизмы возмещения причиненного вреда и привлечения к ответственности недостаточно развиты, что снижает уровень доверия к МИАС. Предлагается в несколько раз увеличить размер штрафов не только для должностного лица, но и для медицинской организации, действия которой привели к утечке данных пациентов. Для реализации данного предложения необходимо внести изменения в ст. 13.11 КоАП РФ<sup>31</sup>, которая предусматривает систему штрафов за нарушение законодательства в сфере персональных данных.

На основании изложенного следует отметить, что правовое регулирование МИАС в России требует дальнейшего совершенствования, что позволит обеспечить более эффективную защиту данных пациентов, стандартизацию медицинских систем и обеспечение переносимости данных. Считаем, что введение единых стандартов для взаимодействия систем, усиление мер информационной безопасности и разработка современных правовых норм по защите прав пациентов могут значительно улучшить работу МИАС в России.

#### Библиографический список

Амелин Р. В., Бессонов Л. В. Правовой режим информационных ресурсов медицинских информационных систем // Известия Саратов. ун-та. Новая серия. Сер.: Экономика. Управление. Право. 2019. № 19 (4). С. 428–435.

<sup>31</sup> См.: Кодекс Российской Федерации об административных правонарушениях : федер. закон от 30 декабря 2001 г. № 196-ФЗ // Собр. законодательства Рос. Федерации. 2002. № 1 (ч. 1). Ст. 13.11.

Анашкина Е. Д. Единая медицинская информационно-аналитическая система : особенности и перспективы // Математические модели техники, технологий и экономики : материалы Всерос. науч.-практ. студ. конф. (Санкт-Петербург, 14–15 мая 2019 г.). СПб. : ПОЛИТЕХ-ПРЕСС, 2019. С. 75–77.

Ашпетова М. В. Особенности цифровизации МИС как инструмента повышения качества работы лечебных учреждений // Татищевские чтения : актуальные проблемы науки и практики. Тольятти : Волж. ун-т им. В. Н. Татищева (Ин-т), 2021. Т. 1. С. 155–157.

Гусев А. В. Медицинские информационные системы : состояние, уровень использования и тенденции // Врач и информационные технологии. 2011. № 3. С. 6–14.

Гусев А. В., Владимирский А. В., Голубев Н. А., Зарубина Т. В. Информатизация здравоохранения Российской Федерации : история и результаты развития // Национальное здравоохранение. 2021. № 2 (3). С. 5–17.

Демкина А. Е. Эволюция цифровой медицины. Мировой и отечественный опыт // Вестник Моск. ун-та. Сер. 21, Управление (государство и общество). 2023. Т. 20, № 2. С. 3–26.

Журавлев М. С. Интероперабельность как фактор развития права в сфере электронного здравоохранения // Право : журнал Высшей школы экономики. 2019. № 3. С. 98–116.

Коновалов А. А. Актуальные правовые аспекты организации деятельности медицинского информационно-аналитического центра в ходе его функциональной эволюции // Врач и информационные технологии. 2016. № 2. С. 6–12.

Кулаков А. А., Серегин С. С. История развития медицинских информационных систем // Стоматология. 2015. № 94 (6). С. 50–53.

Назаренко Г. И., Гулиев Я. И., Ермаков Д. Е. Медицинские информационные системы : теория и практика / под ред. Г. И. Назаренко, Г. С. Осипова. М. : Физматлит, 2005. С. 120.

Назаров Н. А. Обеспечение качества данных при автоматизированном принятии решений в государственном управлении // Журнал рос. права. 2024. № 5. С. 140–155.

Павлов А. В. Правовое регулирование общественных отношений по поводу врачебной тайны в Королевстве Дания и в Российской Федерации : сравнительный анализ // Журнал зарубежного законодательства и сравнительного правоведения. 2017. № 4. С. 74–80.

Позднякова М. А., Коновалов А. А. Медицинский информационно-аналитический центр в системе организации информационного обеспечения региональной системы здравоохранения // Профи-

лактическая медицина как научно-практическая основа сохранения и укрепления здоровья населения : сб. науч. трудов / под общ. ред. М. А. Поздняковой. Ниж. Новгород : Ремедиум Приволжье, 2016. Т. 3. С. 176–186.

Савельев А. И. Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) // Право : журнал Высшей школы экономики. 2015. № 1. С. 43–66.

Bincoletto G. Data protection issues in cross-border interoperability of Electronic Health Record systems within the European Union. *Data & Policy*. 2020. P. 3–4. URL: [https://www.researchgate.net/publication/340274165\\_Data\\_protection\\_issues\\_in\\_crossborder\\_interoperability\\_of\\_Electronic\\_Health\\_Record\\_systems\\_within\\_the\\_European\\_Union](https://www.researchgate.net/publication/340274165_Data_protection_issues_in_crossborder_interoperability_of_Electronic_Health_Record_systems_within_the_European_Union)

Chapman JR., Wang JC., Wiechert K. Big Spine Data Put to Good Use : the NHS Sets an Example // *Global Spine J*. 2019. P. 689–691.

Holt M., MacGibbon J., Smith A., Broady TR., Davis MD., Newman CE. Knowledge of Australia's My Health Record and factors associated with opting out : results from a national survey of the Australian general population and communities affected by HIV and sexually transmissible infections. *PLOS Digit Health*. 2023. URL: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9977020/>

Mantovani E., Quinn P. mHealth and data protection – the letter and the spirit of consent legal requirements // *International Review of Law, Computers & Technology*. 2014. Vol. 28. Issue 2. P. 222.

Momenipur A., Priyadarshini R. Balancing documentation and direct patient care activities : a study of a mature electronic health record system // *International journal of industrial ergonomics*. 2019. Vol. 72. P. 338–346.

Reinhold Haux Medical informatics : past, present, future // *International journal of medical informatics*. 2010. No. 79. P. 599–610.

## References

Amelin R. V., Bessonov L. V. The legal regime of information resources of medical information systems // *Izvestiya of Saratov University. New Series. Series: Economics. Management. Law*. 2019. No. 19(4). P. 428–435.

Anashkina E. D. Unified medical information and analytical system : features and prospects // *Mathematical Models of Engineering, Technology, and Economics : Proceedings of the All-Russian Scientific and Practical Student Conference, Sankt-Peterburg, 14–15 may 2019. Sankt-Peterburg : POLITEX-PRESS, 2019. P. 75–77.*

Ashpetova M. V. Features of the digitalization of MIS as a tool for improving the quality of work in med-

ical institutions // *Tatishchev Readings : Current Issues in Science and Practice. Tolyatti : V. N. Tatishchev Volzhsky University (Institute), 2021. Vol. 1. P. 155–157.*

Gusev A. V. Healthcare Information Systems : Status, Usage, and Trends // *Medical doctor and information technologies*. 2011. No. 3. P. 6–14.

Gusev A. V., Vladzimirskij A. V., Golubev N. A., Zarubina T. V. Informatization of Healthcare in the Russian Federation : History and Results of Development // *National Health Care (Russia)*. 2021. No. 2(3). P. 5–17.

Demkina A. E. The evolution of Digital Medicine. World and Domestic Experience // *Lomonosov Public Administration Journal. Series 21: Management (state and society)*. 2023. Vol. 20, No. 2. P. 3–26.

Zhuravlev M. S. Interoperability as Factor of Law Development in the Digital Economy (eHealth Case) // *Law Journal of the Higher School of Economics*. 2019. No. 3. P. 98–116.

Konovalov A. A. Current Legal Aspects of the Organization of the Regional Medical Information and Analysis Center at its Functional Evolution // *Medical doctor and information technologies*. 2016. No. 2. P. 6–12.

Kulakov A. A., Seregin S. S. The History of Development of Medical Information Systems // *Dentistry*. 2015. No. 94(6). P. 50–53.

Nazarenko G. I., Guliev Ya. I., Ermakov D. E. Medical information systems : theory and practice / ed. by G. I. Nazarenko. Moscow : Fizmatlit, 2005. P. 120.

Nazarov N. A. Ensuring Data Quality in Automated Decision-Making in Public Administration // *Journal of Russian Law*. 2024. No. 5. P. 140–155.

Pavlov A. V. Legal Regulation of Public Relations on the Medical secrecy in the Kingdom of Denmark and in the Russian Federation : A Selective Comparative Analysis // *Journal of Foreign Legislation and Comparative Law*. 2017. No. 4. P. 74–80.

Pozdnyakova M. A., Konovalov A. A. Medical information and analytical center in the system of organizing information support for the regional healthcare system // *Preventive medicine as a scientific and practical basis for maintaining and strengthening public health : Collection of scientific papers. Nizhny Novgorod : Remedium Privolzhye*. 2016. No. 3. P. 176–186.

Savelev A. I. The Issues of Implementing Legislation on Personal Data in the Era of Big Data // *Law Journal of the Higher School of Economics*. 2015. No. 1. P. 43–66.

Bincoletto G. Data protection issues in cross-border interoperability of Electronic Health Record systems within the European Union. *Data & Policy*. 2020. P. 3–4. URL: [https://www.researchgate.net/publication/340274165\\_Data\\_protection\\_issues\\_in\\_crossborder\\_interoperability\\_of\\_Electronic\\_Health\\_Record\\_systems\\_within\\_the\\_European\\_Union](https://www.researchgate.net/publication/340274165_Data_protection_issues_in_crossborder_interoperability_of_Electronic_Health_Record_systems_within_the_European_Union)

der interoperability of Electronic Health Record systems within the European Union

*Chapman JR., Wang JC., Wiechert K.* Big Spine Data Put to Good Use : the NHS Sets an Example // *Global Spine J.* 2019. P. 689–691.

*Holt M., MacGibbon J., Smith A., Broady TR., Davis MD., Newman CE.* Knowledge of Australia's My Health Record and factors associated with opting out : results from a national survey of the Australian general population and communities affected by HIV and sexually transmissible infections. *PLOS Digit Health.* 2023. URL: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9977020/>

*Mantovani E., Quinn P.* mHealth and data protection – the letter and the spirit of consent legal requirements // *International Review of Law, Computers & Technology.* 2014. Vol. 28. Issue 2. P. 222.

*Momenipur A., Priyadarshini R.* Balancing documentation and direct patient care activities : a study of a mature electronic health record system // *International journal of industrial ergonomics.* 2019. Vol. 72. P. 338–346.

Reinhold Haux Medical informatics : past, present, future // *International journal of medical informatics.* 2010. No. 79. P. 599–610.

Национальный исследовательский университет «Высшая школа экономики»

**Лебедева Д. А.**, преподаватель, аспирант, младший научный сотрудник департамента права цифровых технологий и биоправа факультета права  
E-mail: lebedevady@yandex.ru

Поступила в редакцию: 02.02.2025

**Для цитирования:**

*Лебедева Д. А.* Правовые проблемы защиты и переносимости данных пациентов в медицинских информационно-аналитических системах // *Вестник Воронежского государственного университета.* Серия: Право. 2026. № 1 (64). С. 66–77. DOI: <https://doi.org/10.17308/law/1995-5502/2026/1/66-77>

National Research University «Higher School of Economics»

**Lebedeva D. A.**, Lecturer, Post-Graduate Student, Junior Research Fellow at the Department of Digital Technology Law and Biolaw at the Faculty of Law  
E-mail: lebedevady@yandex.ru

Received: 02.02.2025

**For citation:**

*Lebedeva D. A.* Legal issues of protection and portability of patient data in medical information and analytical systems // *Proceedings of Voronezh State University.* Series: Law. 2026. No. 1 (64). P. 66–77. DOI: <https://doi.org/10.17308/law/1995-5502/2026/1/66-77>